JOURNAL

OF THE KANSAS TRIAL LAWYERS ASSOCIATION

VOL. L | NO. 2 | NOVEMBER 2026

CELEBRATING 1951 75 2026 YEARS OF KTLA

KANSAS TRIAL LAWYERS ASSOCIATION

20 26

ANNUAL MEETING & CLE SEMINAR

DECEMBER 10-12

KANSAS CITY MARRIOTT
COUNTRY CLUB PLAZA
KANSAS CITY, MO

SEE PAGE 19 FOR MORE INFORMATION

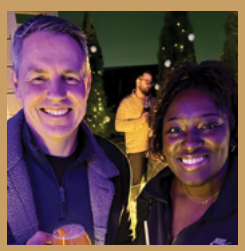
IN THIS ISSUE:

How Common Law Marriage Impacts Kansas Personal Injury Claims (And What to Do If It Fails)

Who Speaks for the Public? Municipal Litigation Authority, the Limits of Attorney General Intervention, and Kansas's New Statutory Gatekeeping Regime

Chatrie v. *United States*: SCOTUS Continues to Restrain Government Access to the Virtual Panopticon in Criminal Investigations





WWW.KTLA.ORG/ANNUALMEETING

Chatrie v. *United States*: SCOTUS Continues to Restrain Government Access to the Virtual Panopticon in Criminal Investigations



DANIEL E. MONNAT

Daniel E. Monnat of Monnat & Spurrier, Chtd., has been a practicing criminal-defense lawyer for the past 47 years in his hometown of Wichita, Kan. Mr. Monnat defends criminal and white-collar criminal cases throughout the state of Kansas and elsewhere. Mr. Monnat is a past two-term president of the Kansas Association of Criminal-Defense Lawyers, a former member of the Board of Directors of the National Association of Criminal Defense Lawyers, an Advocate Eagle member of KTLA and on its Journal Editorial Board, and a Fellow of the American College of Trial Lawyers, the International Academy of Trial Lawyers, and the American Board of Criminal Defense Lawyers.



GINA L. WEHBY

Gina L. Wehby, of Monnat & Spurrier, Chtd., holds a keen interest and enjoyment in legal research and writing. Ms. Wehby graduated from the University of Kansas with a Bachelor's in Political Science and a minor in global and international studies. She also has completed courses in law and master's level courses in public health, health management, and health policy at Saint Louis University. Ms. Wehby returned to her hometown of Wichita where she has collaborated with Mr. Monnat in his criminal defense practice as his paralegal for the past six years.

"[T]he government . . . possesses [access to] a virtual panopticon with which to scrutinize its citizens' activities." ***Chatrie v. United States***, 609 U.S. ----, 146 S. Ct. 2193, 2210 (2026).

Our constant use of digital devices, as well as mass surveillance by the government and private companies (e.g., Flock), produces stored digital data for billions of people that can be accessed by individuals, private companies, or law enforcement. One catch-all term for this digital treasure trove is the "virtual panopticon."[1] By accessing this mother lode through the third-party private actors who often hold this data (e.g., Google), law enforcement can effectively "travel back in time"[2] "with just the click of a button"[3] to attempt to find a new investigative lead or solve an impossible case.[4] Such searches may cull through the data of hundreds or even billions of innocent people[5] without the particularity or probable cause required by the Fourth Amendment to support a traditional search warrant. Essentially, users are reduced from people with Constitutional rights to data points.[6] Recognizing the untold potential for intrusion by the government into the property and privacy interests of all technology users,[7] the U.S. Supreme Court continues to restrain the government's access to this digital gold mine in *Chatrie v. United States*.



***Chatrie's* invocation of a "virtual panopticon" deserves some historical context.** This virtual panopticon is unprecedented, but its historical roots run deep. From the dawn of time, humanity has chronicled narratives of omniscient watchers, both benign[8] and

malevolent.[9] In Greek mythology, the primordial giant Argus Panoptes ("all-seeing") was a warrior and warden endowed with one hundred eternally watchful eyes.[10] In the Industrial Age, humanity sought this omniscience for itself. Through constant, unverifiable surveillance, overseers could exert maximum social control over large groups of workers, patients, students, and prisoners, all at minimal cost.[11] Blueprints for panoptical prisons were particularly prevalent;[12] namely, largely circular buildings wherein a centrally located, invisible overseer (the watcher) could at any time randomly observe any prisoner (the watched), but the prisoner would never know when they were being watched.[13] As an industrial safeguard to this quasi-one-way mirror, visitors (public oversight) were permitted drop-in inspections.[14]



Today, the "virtual panopticon" has clawed its way into recent judicial rhetoric[15] as an Orwellian metaphor for the manner in which now ubiquitous technology watches and preserves the actions and locations of every human being.

The virtual panopticon shatters the quasi-one-way mirror and creates the opportunity for unprecedented government intrusion. In the virtual panopticon, billions of users are completely aware that their digital data is being collected[16] but have become desensitized to the breach of privacy as the "automatic price"[17] of using digital devices and often have not read the lengthy legalese detailing what data is being collected, how often that data is being collected, or how that data will be used.[18] Most of that data is internally analyzed by the companies who collect it to improve app performance or advertising efforts.[19] While the companies hold the data, they do not use it to inspect the users in a traditional watchers' capacity. Instead, they essentially abdicate that role to law enforcement, who seeks to leverage the virtual panopticon in a "newfound tracking capacity."[20] Law enforcement either uses public online databases as if they were a member of the general public (e.g., some investigative genetic genealogy searches)[21] or presents private data holders with search warrants.[22] With the latter, private companies, acting as government agents,[23] search the data of hundreds or even billions of users.[24] Ideally, the detached magistrates authorizing the warrants for those digital searches would assume the panoptical role of public oversight by ensuring that the warrants were sufficiently particularized and supported by probable cause.[25] Yet compliance with those Fourth Amendment requirements is difficult to ascertain, especially in the context of multi-step reverse search warrants.[26] The first steps of these warrants often resemble the general warrants[27] reviled by the Founding Fathers.[28] Subsequent steps risk granting law enforcement a "roving commission"[29] to "conduct[] key portions of the search outside the supervision of a 'neutral and detached magistrate.'"[30]

In the last decade, law enforcement has often sought access to the virtual panopticon through reverse search warrants. Law enforcement has an alleged crime but no viable suspect and no leads; their case may go cold. What do they do? Traditional search warrants "seek information on a particular suspect"[31] or target. No target; no search warrant. Now what? Law enforcement turns to the virtual panopticon for answers. To access this glittery cache of data, they essentially reverse engineer a traditional search warrant by working backward from a "potentially incriminating piece of evidence"[32] and looking for user information "implicated by that evidence."[33] Reverse search warrants have been used to solve previously hard-to-solve crimes[34] by helping to identify previously unidentifiable victims, apprehend alleged criminals, and provide leads in cold cases.[35] The three most prominent forms are investigative genetic genealogy,[36] keyword warrants, and – this year's headline – geofence warrants.[37] Let's begin with the form of warrant at issue in *Chatrie*.

Geofence warrants seek access to user Location History stored in the virtual panopticon. These warrants begin with a physical location,[38] usually a crime scene or disposal site. From that point, law enforcement draws a geofence; that's a virtual fence or perimeter that can take the form of a circle, a polygon, or even a straight line.[39]

In *Chatrie*, the starting point was a credit union that had been the site of an armed robbery.[40] From witness accounts and surveillance recordings, law enforcement could see that the bank robber appeared to be talking on his cellphone near the credit union around the time of the robbery, but they still had no suspects and no additional leads three weeks later.[41] Their solution: obtain a geofence warrant from a local magistrate for cellphone Location History stored with Google to help identify the bank robber, possible accomplices, and additional witnesses.[42] That was not an anomalous request. Since 2016, Google alone has received over 11,000 geofence warrants;[43] other recipients include Apple, Lyft, SnapChat, and Uber.[44] Because of the exponential influx of these warrants, Google worked with law enforcement to develop the process for a three-step geofence warrant.[45] The geofence warrant issued in the credit union robbery ultimately led to the arrest of Okello Chatrie.[46]

So, what is Location History? We have all gotten that annoying popup box on our cell phones asking us if we want to enable or continue allowing an app to use our location.[47] Usually there is an in-app warning that the app will not be able to do "X" without permitting the app to access our location.[48] What we are

enabling is often Location History. It is a time stamp recorded nearly every two minutes[49] that contains a cell phone's latitude and longitude within 20 meters (about 65 feet),[50] its elevation (i.e., what floor of a building the cell phone is on),[51] whether that information was gathered from Bluetooth, cell sites, GPS, IP addresses, or Wi-Fi,[52] and the estimated accuracy of that information.[53] By enabling Location History, cell phone users essentially have access to a personal journal,[54] diary, or map[55] of their movements that they can consult, edit,[56] and receive recommendations from.[57] In short, it's "the most sweeping, granular, and comprehensive tool" existing today for collecting and storing location data on a smartphone.[58] And, like with most "accepted" End User License Agreements that go unread today, most cell phone users who enable Location History do not know how frequently it is tracked, how precise it is, that it might be handed over to the government,[59] or that deleting the app that uses it does not turn Location History off.[60]

In *Chatrie,* law enforcement obtained a geofence warrant that compelled Google to produce Location History near the credit union during a specific period of time[61] with the following three-step process:

Step 1. Law enforcement drew a geofence circle with a radius of 150 meters[62] (about 164 yards[63]) and requested that Google produce anonymized Location History for all cellphones within the geofence 30 minutes before to 30 minutes after the robbery (1 hour total).[64]

Step 2. Law enforcement "attempt[ed]"[65] to narrow down the list of cellphones and then requested that Google produce a second anonymized list for those cellphones that included Locations History both inside and outside the geofence over an even longer period of time (2 hours total).[66]

Step 3. Law enforcement again attempted to narrow down the list of remaining cellphones and then requested that Google produce a list of identifying information for the remaining cell phone users including their account numbers, usernames, email addresses, phone numbers, names, and dates of birth.[67]

Based on the results of that geofence warrant, Okello Chatrie was identified and charged in the bank robbery.[68] As part of his defense, he attempted to suppress this multi-step geofence warrant as an unreasonable Fourth Amendment search of his Location History held by Google.[69] The *Chatrie* majority reframed this question as "whether the police conducted a Fourth Amendment 'search' when they acquired the cell phone [Location History] leading to Chatrie's arrest and, if so, whether that search was reasonable given the features of the [multi-step] warrant"[70] – meaning that each of its steps was properly described with particularity and found to be supported by probable cause."[71] The U.S. Supreme Court elected to grant cert to the first part of this question[72] and left the questions of reasonableness and application of the good faith exception up to the Fourth Circuit.[73] The Court then reviewed its Fourth Amendment precedent.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[74] The "basic purpose" of the Fourth Amendment is "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[75] Historically, a Fourth Amendment search occurred when the government obtained information by intruding on an individual's physical property[76] or into an individual's reasonable expectation of privacy.[77]

However, in this brave new world that more closely resembles the setting of a dystopian novel,[78] "[i]nnovations in surveillance tools"[79] have "enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes."[80] "What in the past was 'unknowable' suddenly bec[ame] open to view, presenting formerly unimaginable 'privacy concerns.'"[81] Accordingly, the U.S. Supreme Court has attempted to "assure[] preservation of th[e] degree of privacy against government that existed when the Fourth Amendment was adopted"[82] because "[a] new technology should not transform what individuals had reasonably thought they could withhold from the government."[83]

For example, modern cell phones have become so "pervasive"[84] that the U.S. Supreme Court has likened them to "an important feature of human anatomy."[85] Our cell phones contain "vast quantities of personal information,"[86] and we "compulsively carry"[87] them around with us to the point that each cell phone "tracks nearly exactly the movements of its owner"[88] through "public thoroughfares into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[89]

In 2018, the U.S. Supreme Court in *Carpenter v. United States* held "individuals have a reasonable expectation of privacy in the whole of their physical movements."[90] Then, it was addressing Cell-Site Location Information (CSLI), which is logged an average of 101 times per day[91] and can place the cell phone user within a sector ranging from 1/8 to 4 square miles.[92] In contrast, the Location History addressed in *Chatrie* logs the user's location every 2 minutes, can pinpoint the user's location within 20 meters, and even estimates the user's elevation.[93] The CSLI addressed in *Carpenter* provides a "detailed" and "encyclopedic" portrait of a person's whereabouts that are only accessible by the cell service provider.[94] The Location History addressed in *Chatrie* is much more; the Court likens it to emails, documents, photographs, or calendars because the data essentially serves as a personal journal of the user's movements that the user can consult and edit.[95] The *Chatrie* court made the following declaration about the resemblances between these two forms of location data: "Everything *Carpenter* relied on to find that law enforcement officers conducted a Fourth Amendment search when they accessed wireless carriers' CSLI records applies as well or better to the police's accessing of Google's Location History data."[96] Thus *Chatrie* squarely held, "An individual has a legitimate expectation of privacy in his cell-phone location data."[97]

An individual's legitimate expectation of privacy in their cell-phone location data is not relinquished just because they share private data with third-party private actors as the "automatic price of conventional cell-phone usage."[98] Location History, like other new forms of property,[99] may be in the possession of the user and/or the private company that facilitates the apps that store such data.[100] Enabling Location History is in no meaningful sense of the word voluntarily "sharing" data with a third party.[101] Therefore, "the police conducted a search when they gained access to Location History data."

Therefore, "an individual has a reasonable expectation of privacy in records about his cellphone's location, and the police intrude on that constitutionally protected interest when they demand information—even though for only a limited time, and from a third-party tech company."[102] In his concurring opinion, Justice Gorsuch asked the question we would all like an answer to: Did the *Chatrie* majority mean to give the third-party doctrine "a quiet burial" by that reasoning?[103]

Now, you and the *Chatrie* dissent might ask, aren't the majority's holding and geofence warrants "obsolete"[104] now that Google no longer stores Location History on its servers?[105] By no means. While on remand the Fourth Circuit may ultimately determine that the geofence warrant was an unreasonable series of Fourth Amendment searches but still valid because of the good faith exception, future similar search warrants will not have that cushion. *Chatrie* puts police, prosecutors, judges, and defense lawyers on notice.[106] Geofence warrants (and similar search warrants) are Fourth Amendment searches, and they must be sufficiently particularized and supported by probable cause to pass constitutional muster.

Further, *Chatrie* has potential implications for other forms of reverse search warrants and for other warrants for access to data that feeds into the virtual panopticon. Remember, geofence warrants are only one type of reverse search warrant being used by law enforcement. They have also begun pursuing investigative genetic genealogy and keyword warrants in attempts to access the virtual panopticon. Deprived of geofence warrants, law enforcement has also sought location history through tower dumps (all cellphones linked to one tower),[107] "frankenwarrants" (all towers within a geofence),[108] and even cell-site simulators (prompt all cell phones within a certain area to send a signal with their locations).[109]

The virtual panopticon also contains a shimmering hoard of genetic data. In his dissenting opinion in *Maryland v. King***,** Justice Antonin Scalia, joined by Justice Elena Kagan (the author of *Chatrie)*, vehemently opposed permitting the warrantless collection of DNA from all persons arrested for "serious offenses"[110] because it contributed to a "genetic panopticon."[111] With the advent of private genetic genealogy databases, that "genetic panopticon" has become a component of the broader virtual panopticon. And, like with Location History, the government has developed a way to access the genetic database component of the virtual panopticon.

Investigative genetic genealogy warrants seek access to private genetic information stored in the virtual panopticon. Investigative genetic genealogy (IGG) begins with genetic material taken from a crime scene.[112] Law enforcement submits genetic material to publicly available commercial genealogy databases in hopes of a match or a familial match.[113] Even if the person has never submitted their DNA to one of these databases, they may have a relative or relative by six degrees of separation who has.[114] It's estimated that more than 1,000 cases have been solved by IGG[115] with some of the best-known uses found in the investigations of the Golden State Killer,[116] Idaho Student Murders,[117] and Nancy Guthrie disappearance.[118] But, like other reverse warrants, IGG warrants have received resistance from both the companies and databases who hold the genetic information[119] and Fourth Amendment advocates.[120] And like the lower courts in Okello Chatrie's case, many trial and appellate courts have agreed with the government[121] that IGG is not a Fourth Amendment search.[122] Reasons vary: the genetic material has been voluntarily given to a third-party database[123]; the defendant has no property or privacy interest in genetic material they share in common with a distant relative who voluntarily gave their own DNA to a private database[124]; the IGG is merely a "tool" for law enforcement to use to narrow their focus or find possible leads.[125] Consider: Are future challenges to IGG likely to succeed after *Chatrie v. United States*?

Keyword warrants seek access to user online searches stored in the virtual panopticon. Our tendency to Google every thought, worry, question, and secret[126] also contributes to the virtual panopticon, and law enforcement has begun accessing those searches using keyword warrants. Keyword searches begin with just that—a keyword entered into an online search engine. Reverse keyword warrants require companies or databases to produce information for every single person who searched a specific set of keywords over a specific period of time, which can encompass hundreds or even billions of users.[127] Law enforcement then works backward from that data to find the next investigative lead or suspect.[128] Like geofence warrants, keyword warrants produce data about completely innocent people who have absolutely nothing to do with the crime being investigated.[129] At least one Colorado court has held that reverse keyword searches intrude on the defendant's constitutionally protected "possessory interest" under the Fourth Amendment.[130] That same court found that a keyword warrant to Google for the IP addresses of all users who searched a specific address over a 15-day period was sufficiently particularized. Yet that court held the warrant was insufficiently supported by individualized probable cause. But, as we have seen time and time again, they determined that any constitutional deficiencies were cured by the good faith exception.[131] Opponents of keyword warrants claim this type of reverse warrant "is a 21st century variety of the general warrants that the Fourth Amendment was designed to guard against."[132] They opine that Google searches are "some of the most private data that exists."[133] That is probably equally true for AI queries. Arguably, Google searches and queries are even

more private than the Location History data at the heart of *Chatrie v. United States*. Some opponents even go beyond the Fourth Amendment to the First. They suggest keyword warrants have the potential to stop or caution users against entering private data into online search engines, thereby chilling free speech.[134]

In the months following the *Chatrie* decision, there has been immediate and significant backlash against law enforcement access to the virtual panopticon. For example, surveillance networks created by coast-to-coast Flock cameras and automated license plate readers have been subject to public condemnation in the form of nationwide protests,[135] petitions for removal,[136] civil rights litigation,[137] and even physical acts like obscuring the cameras or cutting them down.[138] The fervor has only increased with investigations into law enforcement misuse and abuse of the cameras for personal agendas.[139] In response, the government has been cutting off its own access to this component of the virtual panopticon by terminating its contracts with Flock and similar companies.[140]

There are other components of the virtual panopticon that law enforcement has been accessing with impunity.



For years, police have been requesting, and judges have been issuing, search warrants for full extractions of smartphones, desktops, laptops, tablets, Apple accounts, Yahoo accounts, and, yes, Google accounts. But the contents of those devices and accounts are very rarely limited to that one device being searched. And extraction software and physical analyzers such as Cellebrite and GrayKey now permit access not only data on the physical device being searched but also to related cloud accounts.[141] Email and cloud accounts might have data from the inception of the user's account. Digital devices might have data from not only that phone or that computer but the accumulation of data from every single smartphone or every single computer that the user has had in the recent past. How many of us make sure we copy files from an old computer to a new one to avoid losing vital data? How many of us permit Verizon, AT&T, or T-Mobile to facilitate a cloud transfer of all of the data from our old smartphone to our new iPhone or Android? A full extraction of one's smartphone can often contain a lifetime of data well beyond what is relevant to the crime being investigated.

How can we help limit government intrusion into private data held in the virtual panopticon? It may be time for lawyers – criminal defense attorneys, prosecutors, and judges alike – to reexamine the constitutionality of these blanket search warrants for full-device extractions and other digital data dumps.[142]

The Fourth Amendment protection against unreasonable searches and seizures does not wait for a violation to occur before protecting Americans from unreasonable intrusions by the government,[143] and it isn't dependent on the quality of data law enforcement is able to acquire.[144]

Prevention of Fourth Amendment violations starts with law enforcement and prosecutors drawing up the search warrants with sufficient particularity and support for probable cause. It is easy to draft a search warrant to download the entire contents of a smartphone, laptop, or cloud account. Law enforcement and prosecutors should be urged to ask for only the time period or expected data within those downloads that are relevant to the crime they are investigating.

Should zeal to solve a crime cloud the Fourth Amendment lens of law enforcement or prosecutors, judges are the gatekeepers. Judges must review reverse search warrants and warrants for full extractions of digital devices and cloud accounts, paying special attention to the particularity of the warrant and whether law enforcement or the prosecutor has sufficient probable cause to support a reverse search warrant or a full extraction of the digital device or cloud account in question.

And when all else fails, criminal defense lawyers must stand at the ready to review reverse warrants and search warrants for device extractions with a fine-toothed comb. We are the last bastion between the accused and a violation of their Fourth Amendment rights by intrusions into their expectations of privacy or personal effects. Criminal defense attorneys shine a light on deficient warrants and bring them to the attention of trial and appellate courts for review and, if appropriate, suppression of unreasonable searches of digital data gained through reverse warrants and full-device extractions.

The *Chatrie* court, especially Justice Gorsuch, reminds all lawyers that despite recent Fourth Amendment jurisprudence, there are two vehicles for challenging reverse search warrants and other digital data warrants: constitutionally protected interests in an expectation of privacy and in personal effects. Lawyers holding reverse warrants and digital data warrants up to the Fourth Amendment should not shy from availing themselves of both.

1 ***Chatrie v. United States***, 609 U.S. ----, 146 S. Ct. 2193, 2210 (2026); *id*. at 2218 (Jackson & Sotomayor, JJ., concurring).

2 ***Carpenter v. United States***, 585 U.S. 296, 297 (2018).

3 ***Chatrie***, 146 S. Ct. at 2207 (quoting ***Carpenter***, 585 U.S. at 311).

4 *Compare id.* at 2201.

5 For example, hundreds of millions of Google users have enabled location history. *Id.* at 2199.

6 Just a month before the U.S. Supreme Court decided ***Chatrie***, another headline hit the news. The first American Pope in his very first encyclical addressed the ethical considerations of AI and other advanced digital technologies, including the dangers of dehumanizing people into data points or digital language. Pope Leo XIV, *Magnifica Humanitas* [Encyclical Letter], ¶10, ¶92, ¶94, ¶180, ¶182 (2026), Vatican, https://www.vatican.va/content/leo-xiv/en/encyclicals/documents/20260515-magnifica-humanitas.html (last visited Sept. 29, 2026).

7 ***Chatrie***, 146 S. Ct. at 2207 (citing ***Carpenter***, 585 U.S. at 311–12).

8 *See, e.g.*, Biblical living creatures and cherubim. Ezekiel 1:17–18, 10:12; Revelation 4:9.

9 For example, the Fallen Watchers found in the apocryphal Book of Enoch rebelled and devolved into agents of chaos and destruction. *See* 1 Enoch 1-36. In Greek Mythology, the three Fates (Moirai) were known for being ruthless and inflexible regardless of whether fate spelled tragedy. *See, e.g.*, *The Fates: The Destiny Goddesses*, GreekMythology.com, https://www.greekmythology.com/Other_Gods/The_Fates/the_fates.html#google_vignette (last visited Sept. 28, 2026).

10 *See, e.g.*, *Argus Panoptes: The Hundred-Eyed Giant*, GreekMythology.com, https://www.greekmythology.com/Myths/Creatures/Argus_Panoptes/argus_panoptes.html#google_vignette (last visited Sept. 28, 2026); Argus Panoptes in Greek Mythology, GreekLegendsAndMyths.com, https://www.greeklegendsandmyths.com/argus-panoptes.html (last visited Sept. 28, 2026).

11 *See, e.g.*, Phillip Steadman, *Samuel Bentham's Panopticon*, 14 J. of Bentham Stud. 1 (2012), https://journals.uclpress.co.uk/jbs/article/id/608/ [https://doi.org/10.14324/111.2045-757x.044] (citing letter from Jeremy Bentham to his friend, Charles Brown, 1786); Simon Werrett, *Potemkin and the Panopticon: Samuel Bentham and the Architecture of Absolutism in Eighteenth Century Russia*, 2 J. of Bentham Stud. 1 (1999), https://journals.uclpress.co.uk/jbs/article/id/104/ [https://doi.org/10.14324/111.2045-757x.010] (citing Michel Foucault, *Power/Knowledge: Selected Interviews and Other Writings*, at 104 (1980)).

12 Jeremy Bentham worked with his younger brother Samuel Bentham and architect Revelry Wiley to blueprint the original designs for a panoptical penitentiary. *See, e.g.*, *Panopticon Illustrations*, Univ. Coll. of London, https://ucl.primo.exlibrisgroup.com/discovery/collectionDiscovery?vid=44UCL_INST:UCL_VU2&inst=44UCL_INST&collectionId=81406653080004761. While Bentham's panopticon was ultimately stonewalled by bureaucracy, panoptical prisons were erected worldwide in the 19th and 20th centuries. *See* Phillip Steadman, *The Contradictions of Jeremy Bentham's Panopticon Penitentiary* 1, 9 J. of Bentham Stud. 1 (2007), https://journals.uclpress.co.uk/jbs/article/id/740/ [https://doi.org/10.14324/111.2045-757x.030]. As part of his master's thesis in Architecture in Urban Studies, Myles Zhang worked with Cambridge University and University College of London to create a manipulatable computer model of Bentham's panoptical penitentiary. Myles Zhang, *Virtual Reality Computer Model of Jeremy Bentham's Panopticon* (Nov. 2019), https://mylesszhang.org/2019/11/11/jeremy-bentham-panopticon-animation/. The University College of London even created a game called "Panopticon Pandemonium," which gives the user the opportunity to "bring to life the complexities and ambiguities of Bentham's prison scheme." *Panopticon Pandemonium: bringing to life Bentham's unrealized prison*, Univ. Coll. of London, https://www.ucl.ac.uk/laws/panopticon-pandemonium-bringing-life-benthams-unrealised-prison.

13 *See* Werrett, *supra* note 11.

14 *See Id.*

15 ***Chatrie***, 146 S. Ct. at 2210; *id.* at 2218 (Jackson & Sotomayor, JJ., concurring).

16 *See id.* at 2199.

17 *See id.* at 2213.

18 *Id*.

19 *See id.* at 2209; *id.* at 2229 (Alito & Barrett, JJ., dissenting).

20 *Id.* at 2207 (quoting ***Carpenter***, 585 U.S. at 312).

21 Also known as forensic genetic genealogy and forensic investigative genetic genealogy. *See, e.g.*, *Investigative Genomics*, NIH: Nat'l Human Genome Rsch. Inst. (May 19, 2021), https://www.genome.gov/about-genomics/policy-issues/Investigative-Genomics.

22 *See generally*, ***Chatrie***, 146 S. Ct. 2193 (2026).

23 *See id.* at 2222 (Gorsuch, J., concurring).

24 *See id*. at 2199.

25 *Id.* at 2217 (Jackson & Sotomayor, JJ., concurring).

26 *Id.* at 2215.

27 *Id.* at 2216 (citing *Brief for Chatrie*, at 12). In fact, the Fifth Circuit has called geofence warrants "modern-day general warrants." ***United States v. Smith***, 110 F.4th 817, 840 (2024).

28 ***Riley v. California***, 573 U.S. 373, 403 (2014) (citing ***Boyd v. United States***, 116 U.S. 616, 625 (1886)).

29 ***Chatrie***, 146 S. Ct. at 2218 (Jackson & Sotomayor, JJ., concurring) (quoting ***Berger v. New York***, 388 U.S. 41, 59 (1967)).

30 *Id.* at 2217 (Jackson & Sotomayor, JJ., concurring) (quoting ***Johnson v. United States***, 333 U.S. 10, 14 (1948)); *contrast* ***Lo-Ji Sales Inc. v. New York***, 442 U.S. 319, 327 (1979) (Town Justice acted as an "adjunct law enforcement officer" and not "a neutral and detached magistrate when he participated in the search).

31 ***In re Search of Info. That is Stored at the Premises Controlled by Google LLC***, 579 F. Supp.3d 62, 84 n.19 (D.D.C. 2021).

32 Peter G. Berris & Clay Wild, *Geofence and Keyword Searches: Reverse Warrants and the Fourth Amendment*, Cong. Rsch. Serv. Rep. No. R48852 (2026), https://www.congress.gov/crs-product/R48852#ifn5 (citing ***People v. Seymour***, 536 P.3d 1260, 1268 n.1 (Colo. 2023)).

33 Berris & Wild, *supra* note 29.

34 ***Chatrie***, 146 S. Ct. at 2201.

35 *Reverse Search Warrants*, Nat'l Ass'n of Crim. Def. Law. (NACDL) Fourth Amend. Ctr., https://www.nacdl.org/Landing/Reverse-Search-Warrants (last visited Sept. 29, 2026).

36 *Investigative Genomics, supra* note 21.

37 *Id*.; *Reverse Search Warrants*, *supra* note 32.

38 ***Chatrie***, 146 S. Ct. at 2199.

39 *What is geofencing?* Verizon, https://www.verizonconnect.com/glossary/what-is-a-geofence/ (last visited Sept. 29, 2026); *See also* ***Chatrie***, 146 S. Ct. at 2199.

40 ***Chatrie***, 146 S. Ct. at 2202.

41 *Id*.

42 *Id*.

43 *Id*. at 2201–2202.

44 *Id*. at 2201 n.3.

45 *Id*. at 2201–2202.

46 *Id*. at 2199.

47 *Id*. at 2200.

48 *See, e.g.*, *id*. at 2200. In fact, by conducting a small experiment one of the authors learned that by turning off Location History, the author's vehicle infotainment center no longer worked at full capacity.

49 *Id*. at 2199, 2208.

50 *Id*. at 2200, 2208.

51 *Id*.

52 *Id*. at 2200, 2202.

53 *Id*. at 2199–2200.

54 *Id*. at 2209.

55 *Id*. at 2220 (Jackson & Sotomayor, JJ., concurring).

56 *Id*. at 2209.

57 *Id*. at 2201.

58 *Id*. at 2200 (quoting ***United States v. Chatrie***, 590 F.Supp.3d 901, 907 (E.D. Va. 2022)).

59 *Id.* at 2213.

60 *Id*. at 2200.

61 *Id*. at 2199.

62 *Id*. at 2202.

63 If a visual is helpful, that's approximately 1.4 regulation NFL football fields including the end zones.

64 ***Chatrie***, 146 S. Ct. at 2202.

65 *Id.* Notably, the warrant did not outline how law enforcement might make this "attempt." In fact, law enforcement initially made no "attempt" at all. *Id*. at 2217 (Jackson & Sotomayor, JJ., concurring). It was only at the urging of Google that law enforcement narrowed the list of cell phone users. *Id*. at 2218 (Jackson & Sotomayor, JJ., concurring).

66 *Id.* at 2202–03.

67 *Id*. at 2203; *id*. at *2217 (Jackson & Sotomayor, JJ., concurring).

68 *Id.* at 2199.

69 *Id.* at 2199, 2203.

70 *Id*. at 2200.

71 *Id*. at 2200-01.

72 *Id*. at 2200.

73 *Id*. at 2204.

74 *Id*. (quoting U.S. Const. amend IV).

75 *Id.* at 2204 (quoting ***Carpenter***, 585 U.S. at 303).

76 *Id.* at 2204 (citing ***United States v. Jones***, 565 U.S. 400, 406-07 n.3 (2012)); *See also id.* at 2218–22 (Gorsuch, J., concurring).

77 *Id.* at 2204–05.

78 George Orwell terrified millions with his dystopian world controlled by Telescreens and Thought Police in *Nineteen Eighty-Four* (1949). In popular culture, panopticons abound. Examples include Batman's surveillance network in *The Dark Knight* (2008); the Machine (empathetic) and Samaritan (authoritarian), warring AI superintelligences, in *Person of Interest* (starring Jim Caviezel); the Kyln (interstellar prison) that held the heroes of *Guardians of the Galaxy* (2014); and the Narkina 5 Imperial Prison Complex in *Star Wars: Andor* (2022).

79 ***Chatrie***, 146 S. Ct. at 2205 (quoting ***Carpenter***, 585 U.S. at 305).

80 *Id.*

81 *Id.* at 2207 (quoting ***Carpenter***, 585 U.S. at 311–12).

82 *Id.* at 2205 (quoting ***Kyllo v. United States***, 533 U.S. 27, 34 (2001)).

83 *Id.* at 2207.

84 *Id.* at 2213 (quoting ***Carpenter***, 585 U.S. at 315).

85 *Id*. at 2200 (quoting ***Riley***, 573 U.S. at 385).

86 *Id.* at 2206 (quoting ***Riley***, 573 U.S. at 386).

87 *Id.* at 2207 (quoting ***Carpenter***, 585 U.S. at 311).

88 *Id*.

89 *Id*.

90 *Id.* at 2206 (quoting ***Carpenter***, 585 U.S. at 310).

91 *Id.* at 2208 (quoting ***Carpenter***, 585 U.S. at 302).

92 *Id.* (quoting ***Carpenter***, 585 U.S. at 312).

93 *Id.*

94 *Id*. (quoting ***Carpenter***, 585 U.S. at 309).

95 *Id.* at 2201, 2209.

96 *Id*. at 2208.

97 *Id*. at 2204.

98 *Id.* at 2213.

99 *Magnifica Humanitas*, ¶67; *See also* examinations of whether Location History is property in the context of the Fourth Amendment. ***Chatrie***, 146 S. Ct. at 2220–22 (Gorsuch, J., concurring) ("Mr. Chatrie's Location History data qualifies as his personal property."); Contrast *Id.* at 2226–28 (Alito, J., dissenting).

100 ***Chatrie***, 146 S. Ct. at 2201 (citing ***Riley***, 573 U.S. at 397).

101 *Id.* at 2213 (quoting ***Carpenter***, 585 U.S. at 315); *compare id.* at 2221–22 (Gorsuch, J., concurring); *contrast id.* at 2228–29 (Alito & Barrett, JJ. dissenting); *contrast id.* at 2234 (Barrett, J., dissenting). As NACDL's Michael Price put it during a recent webinar, Google "demonstrated by deed" that Location History belongs to the user.

102 *Id.* at 2199.

103 *Id.* at 2219–20 (2026)(Gorsuch, J., concurring).

104 *Id.* at 2223 (Alito, J., dissenting).

105 *Id.* at 2201 n.2.

106 *Contrast id.* at 2225 (Alito, J., dissenting).

107 *See, e.g., In re: Four Applications for Search Warrants Seeking Information Associated with Particular Cellular Towers A/K/A Tower-Dump Warrants;* No. 3:25-cr-00038-CWR-ASH, 2026 WL 2260371 (S.D. Miss. Aug. 5, 2026) (Tower dumps are unconstitutional general warrants.).

108 Also known as area dumps or area searches. *See, e.g.,* Jake Laperruque & Justin Hendrix, *What's at Stake in Chatrie v. United States*, Tech Pol'y Press (May 17, 2026), https://www.techpolicy.press/whats-at-stake-in-chatrie-v-united-states/ (interviewing litigation director for the NACDL Fourth Amendment Center and attorney for Okello Chatrie: Michael Price).

109 *See, e.g.*, Ian Round, *Police need warrant for cell-site simulators, 4th Circuit rules*, Maryland Daily Rec. (Sept. 28, 2026), https://thedailyrecord.com/2026/09/28/cell-site-simulators-warrant-4th-circuit/.

110 ***Maryland v. King***, 569 U.S. 435, 439 (2013).

111 *Id.* at 482 (Scalia, J., joined by Ginsburg, Sotomayor & Kagan, JJ., dissenting).

112 *Investigative Genomics*, *supra* note 21.

113 *See, e.g.*, Mengge Wange, et al., *Forensic investigative genetic genealogy: expanding pedigree tracing and genetic inquiry in the genomic era*, 52 J. of Genetics and Genomics 4 (2025), https://www.sciencedirect.com/science/article/pii/S1673852724001589 [https://doi.org/10.1016/j.jgg.2024.06.016].

114 *See, e.g.*, Daniel Kling, et al., *Investigative genetic genealogy: Current methods, knowledge and practice,* 52 Forensic Sci. Int'l: Genetics (Jan. 30, 2021), https://www.fsigenetics.com/article/S1872-4973(21)00013-2/fulltext [https://doi.org/10.1016/j.fsigen.2021.102474].

115 David Guerney, *Investigative genetic genealogy is a revolutionary tool for justice*, 42 Cell Press: Trends in Genetics 5:393-95 (May 4, 2026), https://www.sciencedirect.com/science/article/abs/pii/S0168952525002884 [https://doi.org/10.1016/j.tig.2025.11.006].

116 JV Charmary, *How Genetic Genealogy Helped Catch the Golden State Killer*, Forbes (Jun. 20, 2020, at 8:11 p.m. EDT), https://www.forbes.com/sites/jvcharmary/2020/06/30/genetic-genealogy-golden-state-killer.

117 *Order on Defendant's Motion to Suppress re: Genetic Information*, ***Idaho v. Kohberger***, No. CR01-24-31665 (Ada Co. Feb. 19, 2025), https://meshbasestorage.blob.core.windows.net/dnacontainer/021925-Order-Defendants-Motion-Suppress-Genetic-Information.pdf.

118 Michael Ruiz & Julia Bonavita, *Genetic genealogy that caught notorious killers now used in Nancy Guthrie case*, Fox News (Feb. 17, 2026, at 7:05 p.m. EST), https://www.foxnews.com/us/genetic-genealogy-caught-notorious-killers-now-used-nancy-guthrie-case?msockid=2073b66aad536db51240a766ca3.

119 *Ancestry Terms and Conditions, 1.3 Use of the Services*, Ancestry (May 12, 2026), https://www.ancestry.com/c/legal/termsandconditions?ranMID=50138&ranEAID=3829940&ranSiteID=_jZHTpnCvx8-gsySrdp0asUTbPf4Ei1vfg&o_xid=0003829940&o_lid=0003829940&o_sch=Affiliate%20External (prohibiting use "in connection with law enforcement investigation or criminal judicial proceeding"); *23andMe Guide for Law Enforcement: Requests for 23andMe User Information,* 23andMe Rsch. Inst. (2026), https://www.23andme.org/trust-center/guide-for-law-enforcement/ (last visited Sept. 29, 2026) ("23andMe chooses to use all practical legal and administrative resources to resist requests from law enforcement . . . .").

120 *See, e.g.*, *Order on Motion for Discovery*, ***People v. Waller***, No. 18FE018342 (Cal. Super. Ct. Sacramento Cnty. Oct. 7, 2019), https://meshbasestorage.blob.core.windows.net/dnacontainer/Waller-Court-Ruling.pdf; *Ruling on Motion to Compel Production of Discovery*, ***In re Green***, No. PDL202020007 (Cal. Super. Ct. El Dorado Cnty. Oct. 5, 2020), https://meshbasestorage.blob.core.windows.net/dnacontainer/Green.pdf; ***State v. Bortree***, 2021-Ohio-2873 (3d Dist. 2021), https://meshbasestorage.blob.core.windows.net/dnacontainer/State%20v.%20Bortree.pdf; *Findings of Fact, Conclusions of Law, and Order,* ***State v. Carbo***, No. 69HI-CR-20-549 (St. Louis Cnty Minn. Distr. Ct. Nov. 10, 2021), https://meshbasestorage.blob.core.windows.net/nodomaincontainer/carbo-omnibus-order.pdf; *Order Denying Motion to Suppress Familial DNA Search and Fruit Thereof*, ***People v. Phillips***, 2021 CR 15 (Colo. Distr. Ct. Park Cnty. Jan. 5, 2022), https://meshbasestorage.blob.core.windows.net/nodomaincontainer/phillips-order-denying-motion-to-suppress-igg-search-and-fruit-thereof.pdf; ***People v. Lepere***, No. G061393 (Cal. Ct. App. 4th Dist. May 16, 2023), https://meshbasestorage.blob.core.windows.net/dnacontainer/People%20v.%20Lepere.pdf; *See also Order on Defendant's Motion to Suppress re: Genetic Information*, *supra* note 114.

121 *Investigative Genomics*, *supra* note 21.

122 *See, e.g.*, *Order on Motion for Discovery*, *supra* note 115; *Findings of Fact, Conclusions of Law, and Order*, *supra* note 115, at *11–13; *Order Denying Motion to Suppress Familial DNA Search and Fruit thereof*, *supra* note 115, at 2-7; ***Bortree***, 2021-Ohio-2873, *supra* note 115, at ¶96.

123 *See e.g.*, *Investigative Genomics*, *supra* note 21.

124 *See, e.g.*, *Order on Motion for Discovery*, *supra* note 115; *Findings of Fact, Conclusions of Law, and Order*, *supra* note 115, at *11–13; *Order Denying Motion to Suppress Familial DNA Search and Fruit thereof*, *supra* note 115, at 2-7.

125 *See, e.g.*, ***Bortree***, 2021-Ohio-2873, *supra* note 115, at ¶96.

126 *Motion to Suppress Evidence from a Keyword Warrant & Request for a Veracity Hearing*, ***People v. Seymour***, 2021CR20001, at *1, ¶4 (Colo. Dist. Ct. Denver Cnty. Jun. 30, 2022), https://www.nacdl.org/getattachment/9ae907b9-5bcb-4f86-925a-13fed77f5d18/seymour-motion-to-suppress.pdf. Or as Michael Price put it during a recent NACDL webinar, "People treat that [search] box like a confessional."

127 *Id.* at *1, ¶1.

128 *Reverse Search Warrants*, *supra* note 32.

129 *Id.*

130 ***People v. Seymour***, 546 P.3d 1260, 1267 (Colo. 2023).

131 *Id.* at 1268.

132 *Motion to Suppress Evidence from a Keyword Warrant & Request for a Veracity Hearing*, *supra* note 122, at *1, ¶3.

133 *Id.* at 1, ¶4.

134 Abigail Aislis, *Reverse Keyword Search Warrants and the Threat to Online Privacy*, Tech Pol'y Press (Apr. 29, 2025), https://www.techpolicy.press/regulating-tracking-of-online-search-queries-and-histories-the-advent-of-the-reverse-keyword-search-warrant/.

135 *See, e.g.*, Aniyah Robinson, *Wichita protesters raise privacy concerns over Flock cameras,* KSN (Sept. 18, 2026, at 8:22 a.m. CDT), https://www.ksn.com/news/wichita-protesters-raise-privacy-concerns-over-flock-cameras/.

136 *See, e.g.*, *Get the Flock Out*, ACLU (Sept. 25, 2026), https://www.aclu.org/campaigns-initiatives/get-the-flock-out.

137 *See, e.g.*, *Petition for Declaratory Judgment*, No. SG-2026-CV-002760 (Kan. Dist. Ct. Sedgwick Cnty. Jul. 29, 2026), https://kansasjusticeinstitute.org/wp-content/uploads/2026/07/1-Petition.pdf; Ana Valdez, *City of Wichita seeks to dismiss lawsuit over Flock cameras*, KWCH (Sept. 28, 2026, at 9:56 p.m. CDT), https://www.kwch.com/2026/09/29/city-wichita-seeks-dismiss-lawsuit-over-flock-cameras/.

138 Physical acts include holding signs in front of the cameras, spraying them with expanding foam, and cutting them down. *See, e.g.*, Meg Anderson, *Amid intense backlash, people are vandalizing Flock surveillance cameras*, KSN (Aug. 21, 2026, at 4:58 p.m. ET), https://www.npr.org/2026/08/21/nx-s1-5931849/amid-intense-backlash-people-are-vandalizing-flock-surveillance-cameras; Cale Chapman, *As concerns grow over ethics of Flock cameras, police stress vandalism is not the answer*, KWCH (Sept. 22, 2026, at 5:27 p.m. CDT), https://www.kwch.com/2026/09/22/concerns-grow-over-ethics-flock-cameras-police-stress-vandalism-is-not-answer/.

139 *See, e.g.*, *Get the Flock Out, supra* note 136; Christopher Ingraham, *The IJ Database of ALPR Abuse*, Inst. for Justice (Aug. 12, 2026), https://ij.org/the-ij-database-of-alpr-abuse/.

140 At least 214 cities and counties have terminated their contracts with Flock since 2021. Of those 214, 90 cancellations were in August 2026. Cyrus, Farivar, *Cities terminate Flock contracts at record pace in August*, Ars Technica (Aug. 28, 2026, 4:33 p.m.), https://arstechnica.com/tech-policy/2026/08/cities-terminate-flock-contracts-at-record-pace-in-august/.

141 *See, e.g.,* Heather Mahalik, *How to Use Cellebrite Physical Analyzer's New Cloud Feature*, Cellebrite (Nov. 9, 2020), https://cellebrite.com/en/ask-the-expert/how-to-use-cellebrite-physical-analyzers-new-cloud-feature/.

142 For a discussion of how Kansas federal courts previously addressed this issue see: ***In re Nextel Cellular Telephone***, No. 14-MJ-8005-DJW, 2014 WL 2898262 at *9–14 (D. Kan. Jun. 26, 2014), *declined to follow,* ***United States v. Beasley***, No. 13-10112-01, 03, 04, 05, 06, 07, 08, 10, 11, 12-JTM, 2016 WL 502023, at *8–9 (D. Kan. Feb. 8, 2016).

143 ***Chatrie***, 146 S. Ct. at 2210 (quoting ***Pennsylvania Coal Co. v. Mahon***, 260 U.S. 393, 415 (1922)).

144 *Id.* (quoting ***Kyllo***, 533 U.S. at 37).