Negative: Geofence Warrants – not a problem

By “Coach Vance” Trefethen

***Resolved: The United States federal government substantially reform the use of Artificial Intelligence technology***

Case Summary: The AFF plan stops GEOFENCE warrants. These are search warrants obtained by the police, as required by the 4th Amendment, to obtain data regarding the location of any device that was in a specified area during a certain time range. Police are following the court rulings and getting warrants. But AFF’s problem with this is that it scoops up a lot of data from innocent bystanders in addition to the suspects law enforcement was trying to catch. Plan also bans “keyword warrants.” These are warrants obtained by the government that demand information from Google regarding all the search terms used by people in a particular area during a certain time range.

Negative: Geofence Warrants – not a problem 3

TOPICALITY 3

1. Where’s the AI? Part 1: Geofence 3

Geofence warrants don’t depend on (and may not even use) artificial intelligence. 3

Violation: “Analyzing data” isn’t AI. The machine has to be learning on its own, and that doesn’t happen in Geofence 3

Impact: No one affirming the resolution means Negative ballot 3

2. Where’s the AI – Part 2: Keyword warrants 3

Cross-apply all the same arguments from Geofence. 3

And cross-apply the same impacts – Negative ballot 3

INHERENCY 4

1. Cell phone tracking already requires a warrant 4

Supreme Court *Carpenter v. U.S.* decision in 2018 requires warrants for cell phone location data 4

2. Federal courts are banning geofence warrants 4

Two federal court cases have already ruled the way AFF wants 4

MINOR REPAIR – Recommended by attorneys for Google 4

Don’t ban geofence, just ensure that they are supervised by a judge and only allowed with probable cause 4

HARMS / SIGNIFICANCE 5

1. A/T “4th Amendment harms” – Response #1. Handing over records as evidence has nothing to do with 4thA 5

Government demands to produce records have nothing to do with the 4th Amendment because they’re not a search 5

Handing over documents has nothing to do with the 4th Amendment when no government search occurs 5

Founding Fathers would disagree with AFF: Handing over evidence in your possession is embedded in Anglo-American legal traditions 5

2. A/T “4th Amendment harms” – Response #2. Twisting the 4th A to create a privacy claim on someone else’s property 6

Data in the AFF plan (Google data) belongs to someone else. Claiming privacy over someone else’s property radically departs from the meaning of the 4th Amendment 6

3. Users disclose data voluntarily 6

Users opt in to location disclosure, and they can delete it any time they want 6

Users opt in to sharing their location data with Google - that voluntary information is what Geofence gets 6

4. Privacy is dead and nobody attended the funeral 7

Most people don’t care about privacy as much as they claim to 7

What people value is “security,” not privacy. Strong belief in data privacy is dead 7

Naïve to expect privacy any more, and people’s behavior proves they don’t really care 7

There’s nothing anyone can do about data privacy 7

SOLVENCY 8

1. No change in Geofence post-plan 8

No AI involved, so no “Geofence warrants using AI” are stopped by the AFF plan. This is how Geofence warrants work: 8

No AFF evidence that blocking AI would stop geofence warrants 8

2. No change in keyword warrants post-plan 8

Cross-apply the same arguments from geofence. 8

DISADVANTAGES 8

1. Unsolved crimes & Justice denied 8

Someday it could be you: Here’s someone who’s extremely glad geofence warrants exist 8

Negative: Geofence Warrants – not a problem

TOPICALITY

1. Where’s the AI? Part 1: Geofence

Geofence warrants don’t depend on (and may not even use) artificial intelligence.

**Listen to this description of how Geofence warrants work and see if you can find any AI in it:**

Maura Arnold 2021 (JD candidate at Suffolk Univ. Law School) Geofence Warrants: Useful Crime Solving Tool or Invasive Surveillance Tactic? JOURNAL OF HIGH TECHNOLOGY LAW <https://sites.suffolk.edu/jhtl/2021/03/10/geofence-warrants-useful-crime-solving-tool-or-invasive-surveillance-tactic/> (accessed 22 Jan 2022)

[Geofence warrants](https://perma.cc/N6S8-6AQ7), also known as “reverse-location warrants,” are a new concept to the world of criminal justice. At its core, geofencing is when a virtual border is drawn around a predefined geographical area where data can be gathered on those who enter the area. Outside of a criminal law context, geofencing is used for marketers who are trying to target specific audiences for ads.  First utilized in [2016 by federal law enforcement](https://perma.cc/9Q3B-W3KY), geofence warrants allow law enforcement officers to collect anonymized information from Google from any kind of device that was in a specific geographic area in a specific period of time. Law enforcement officers then ask Google for specific user information from any device they may decide could belong to a suspect.

Violation: “Analyzing data” isn’t AI. The machine has to be learning on its own, and that doesn’t happen in Geofence

*Brad Eck 2018* (Strategic Alliances Program Owner – Americas, Milestone Systems, a global industry leader in open platform IP video management software) 15 Nov 2018 “Clearing up Confusion: Misconceptions About AI” <https://news.milestonesys.com/clearing-up-confusion-misconceptions-about-ai/> (accessed 8 Aug 2021)

* AI (artificial intelligence) at its most basic is the ability for a machine to learn on its own;
* Machine learning typically references how the AI is being applied (shallow/deep evaluation of data at different levels); and
* Analytics are typically a catch-all word for the results that are presented back to the user (and this is also used with non-AI related analytics).
The most basic definition of AI is the ability for a machine to learn on its own. The expectations are that it would provide actionable results and potentially even take intelligent action based on those results.

Impact: No one affirming the resolution means Negative ballot

The Affirmative had dozens of possible cases they could run that involve the actual use of AI. Instead, they chose something that doesn't use it. Since they failed to affirm the resolution, and we deny the resolution, there is effectively no Affirmative team in this round. No matter who wins, you should vote Negative.

2. Where’s the AI – Part 2: Keyword warrants

Cross-apply all the same arguments from Geofence.

A keyword search by Google is simply a search. There’s no machine learning AI involved.

And cross-apply the same impacts – Negative ballot

Not affirming the resolution means 2 Negative teams in the round, so the only possible ballot is Negative.

INHERENCY

1. Cell phone tracking already requires a warrant

Supreme Court *Carpenter v. U.S.* decision in 2018 requires warrants for cell phone location data

Andrew Crocker & Jennifer Lynch 2018. (Crocker - senior staff attorney on the Electronic Frontier Foundation’s civil liberties team. Lynch –attorney, Surveillance Litigation Director at EFF) 22 June 2018 “Victory! Supreme Court Says Fourth Amendment Applies to Cell Phone Tracking” <https://www.eff.org/deeplinks/2018/06/victory-supreme-court-says-fourth-amendment-applies-cell-phone-tracking> (accessed 21 Jan 2022)

The Supreme Court handed down a landmark [opinion](https://www.eff.org/document/carpenter-v-united-states-supreme-court-opinion) today in Carpenter v. United States, ruling 5-4 that the Fourth Amendment protects cell phone location information. In an opinion by Chief Justice Roberts, the Court recognized that location information, collected by cell providers like Sprint, AT&T, and Verizon, creates a “detailed chronicle of a person’s physical presence compiled every day, every moment over years.” As a result, police must now get a warrant before obtaining this data.

2. Federal courts are banning geofence warrants

Two federal court cases have already ruled the way AFF wants

Jennifer Lynch and Nathaniel Sobel 2020. (Lynch – attorney; Surveillance Litigation Director at Electronic Frontier Foundation (EFF). Sobel – writer for EFF) 31 Aug 2020 “New Federal Court Rulings Find Geofence Warrants Unconstitutional” <https://perma.cc/Z772-7UHF> <https://perma.cc/Z772-7UHF> (accessed 22 Jan 2022)

Two federal magistrate judges in three [separate](https://wr.perma-archives.org/public/z772-7uhf/20210222030634mp_/https%3A/www.eff.org/document/re-search-information-stored-premises-controlled-google-no-20-m-297-de-4-nd-ill-july-8-2020) [opinions](https://wr.perma-archives.org/public/z772-7uhf/20210222030634mp_/https%3A/www.eff.org/document/re-search-info-stored-premises-controlled-google-no-20-m-392-2020-us-dist-lexis-152712-nd) have ruled that a geofence warrant violates the Fourth Amendment’s probable cause and particularity requirements. Two of these rulings, from the federal district court in Chicago, were recently unsealed and provide a detailed constitutional analysis that closely aligns with arguments [EFF](https://wr.perma-archives.org/public/z772-7uhf/20210222030634mp_/https%3A/www.eff.org/deeplinks/2019/04/googles-sensorvault-can-tell-police-where-youve-been) and [others](https://wr.perma-archives.org/public/z772-7uhf/20210222030634mp_/https%3A/www.nacdl.org/Content/United-States-v-Chatrie%2C-No-3-19-cr-130-%28E-D-Va-%29) have been making against geofence warrants for the last couple years.

MINOR REPAIR – Recommended by attorneys for Google

Don’t ban geofence, just ensure that they are supervised by a judge and only allowed with probable cause

Brittany Amadi, Cahterine Carroll and Alex Hemmer 2019 (attorneys for Google) US v. Chatrie 20 Dec 2019 BRIEF OF AMICUS CURIAE GOOGLE LLC IN SUPPORT OF NEITHER PARTY CONCERNING DEFENDANT’S MOTION TO SUPPRESS EVIDENCE FROM A “GEOFENCE” GENERAL WARRANT (ECF NO. 29) <https://www.nacdl.org/getattachment/723adf0b-90b1-4254-ab82-e5693c48e951/191220-chatrie-google-amicus-brief.pdf> (accessed 22 Jan 2022) (brackets added)

Google takes no position on whether the warrant in this case satisfies the requirements of probable cause and particularity or, if it does not, whether suppression is appropriate. But in resolving those questions, the Court should take into account the complete factual and legal context, and it should hold that both the SCA and the Fourth Amendment require the government to obtain a warrant to compel Google to search LH information via a geofence search. That result is compelled by the statute and the Constitution and the cases applying them. It is also the only result that takes appropriate account of the singularly broad and intrusive nature of a geofence search and the granularity of the intimate detail it produces. Given the capacity of geofence searches to intrude on personal privacy, their use should be supervised by a neutral magistrate and restricted to cases in which the government can establish probable cause.

HARMS / SIGNIFICANCE

1. A/T “4th Amendment harms” – Response #1. Handing over records as evidence has nothing to do with 4thA

Government demands to produce records have nothing to do with the 4th Amendment because they’re not a search

Supreme Court Justice Samuel Alito 2018. Dissenting opinion in the case of Carpenter v. U.S. 22 June 2018 <https://supreme.justia.com/cases/federal/us/585/16-402/#tab-opinion-3919268> (accessed 22 Jan 2022) (in context, the Carpenter case was about cell phone location tracking)

The Court’s reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely. First, the Court ignores the basic distinction between an actual search (dispatching law enforcement officers to enter private premises and root through private papers and effects) and an order merely requiring a party to look through its own records and produce specified documents. The former, which intrudes on personal privacy far more deeply, requires probable cause; the latter does not. Treating an order to produce like an actual search, as today’s decision does, is revolutionary. It violates both the original understanding of the Fourth Amendment and more than a century of Supreme Court precedent.

Handing over documents has nothing to do with the 4th Amendment when no government search occurs

Supreme Court Justice Samuel Alito 2018. Dissenting opinion in the case of Carpenter v. U.S. 22 June 2018 <https://supreme.justia.com/cases/federal/us/585/16-402/#tab-opinion-3919268> (accessed 22 Jan 2022) (in context, the Carpenter case was about cell phone location tracking) (brackets and ellipses in original)

The Fourth Amendment does not regulate all methods by which the Government obtains documents. Rather, it prohibits only those “searches and seizures” of “persons, houses, papers, and effects” that are “unreasonable.” Consistent with that language, “at least until the latter half of the 20th century” “our Fourth Amendment jurisprudence was tied to common-law trespass.” United States v. Jones, 565 U. S. 400, 405 (2012). So by its terms, the Fourth Amendment does not apply to the compulsory production of documents, a practice that involves neither any physical intrusion into private space nor any taking of property by agents of the state.

Founding Fathers would disagree with AFF: Handing over evidence in your possession is embedded in Anglo-American legal traditions

Supreme Court Justice Samuel Alito 2018. Dissenting opinion in the case of Carpenter v. U.S. 22 June 2018 <https://supreme.justia.com/cases/federal/us/585/16-402/#tab-opinion-3919268> (accessed 22 Jan 2022) (in context, the Carpenter case was about cell phone location tracking) (brackets and ellipses in original)

Compulsory process was also familiar to the founding generation in part because it reflected “the ancient proposition of law” that “ ‘ “the public . . . has a right to every man’s evidence.” ’ ” *United States* v. *Nixon*, 418 U. S. 683, 709 (1974); see also *ante*, at 10 (Kennedy, J., dissenting). As early as 1612, “Lord Bacon is reported to have declared that ‘all subjects, without distinction of degrees, owe to the King tribute and service, not only of their deed and hand, but of their knowledge and discovery.’ ” *Blair*, *supra*, at 279–280. That duty could be “onerous at times,” yet the Founders considered it “necessary to the administration of justice according to the forms and modes established in our system of government.” *Id.,* at 281; see also *Calandra*, *supra*, at 345.
B
Talk of kings and common-law writs may seem out of place in a case about cell-site records and the protections afforded by the Fourth Amendment in the modern age. But this history matters, not least because it tells us what was on the minds of those who ratified the Fourth Amendment and how they understood its scope. That history makes it abundantly clear that the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all.

2. A/T “4th Amendment harms” – Response #2. Twisting the 4th A to create a privacy claim on someone else’s property

Data in the AFF plan (Google data) belongs to someone else. Claiming privacy over someone else’s property radically departs from the meaning of the 4th Amendment

Supreme Court Justice Samuel Alito 2018. Dissenting opinion in the case of Carpenter v. U.S. 22 June 2018 <https://supreme.justia.com/cases/federal/us/585/16-402/#tab-opinion-3919268> (accessed 22 Jan 2022) (brackets in original) (in context, the Carpenter case was about cell phone location tracking)

Second, the Court allows a defendant to object to the search of a third party’s property. This also is revolutionary. The Fourth Amendment protects “[t]he right of the people to be secure in *their*persons, houses, papers, and effects” (emphasis added), not the persons, houses, papers, and effects of others. Until today, we have been careful to heed this fundamental feature of the Amendment’s text. This was true when the Fourth Amendment was tied to property law, and it remained true after *Katz* v. *United States*, 389 U. S. 347 (1967), broadened the Amendment’s reach. By departing dramatically from these fundamental principles, the Court destabilizes long-established Fourth Amendment doctrine. We will be making repairs—or picking up the pieces—for a long time to come.

3. Users disclose data voluntarily

Users opt in to location disclosure, and they can delete it any time they want

Wendy Davis 2020. (journalist) 1 Dec 2020 “Law enforcement is using location tracking on mobile devices to identify suspects, but is it unconstitutional?” <https://www.abajournal.com/magazine/article/law-enforcement-is-using-location-tracking-on-mobile-devices-to-identify-suspects-geofence> (accessed 22 Jan 2022)

Four months later, the U.S. Department of Justice indicted 24-year-old Okello Chatrie for the robbery. Authorities arrested Chatrie after presenting Google with a “reverse location”—or geofence—warrant for information on account holders whose mobile devices were near the scene of the crime. Google can gather location data from people who use Google Maps and other services on their mobile devices. The company says it stores this data only for account holders who have opted into the “location history” feature. But people who have opted in can manually delete this data. In June, Google said it would automatically delete location history data after 18 months.

Users opt in to sharing their location data with Google - that voluntary information is what Geofence gets

Brittany Amadi, Cahterine Carroll and Alex Hemmer 2019 (attorneys for Google) US v. Chatrie 20 Dec 2019 BRIEF OF AMICUS CURIAE GOOGLE LLC IN SUPPORT OF NEITHER PARTY CONCERNING DEFENDANT’S MOTION TO SUPPRESS EVIDENCE FROM A “GEOFENCE” GENERAL WARRANT (ECF NO. 29) <https://www.nacdl.org/getattachment/723adf0b-90b1-4254-ab82-e5693c48e951/191220-chatrie-google-amicus-brief.pdf> (accessed 22 Jan 2022) (brackets added)

As set forth below, the LH [Location History] information at issue in geofence requests such as the one in this case differs in significant respects from the cell site location information (“CSLI”) at issue in Carpenter v. United States, 138 S. Ct. 2206 (2018), and other types of data that courts have considered in Fourth Amendment cases. For example, rather than a record created and stored by Google as an automatic result of using a Google service, Google LH information is created, edited, and stored by and for the benefit of Google users who opt into the service and choose to communicate their location information to Google for storage and processing.

4. Privacy is dead and nobody attended the funeral

Most people don’t care about privacy as much as they claim to

Prof. Neil Sahota 2020 ( IBM Master Inventor, United Nations Artificial Intelligence Advisor, Professor at UC Irvine) 14 Oct 2020 “Privacy Is Dead And Most People Really Don’t Care” https://www.forbes.com/sites/neilsahota/2020/10/14/privacy-is-dead-and-most-people-really-dont-care/?sh=5fc1aa97b733

Have you read the terms and conditions to use Facebook? Your smart phone? [Most people have not](https://www.npr.org/2014/09/01/345044359/why-do-we-blindly-sign-terms-of-service-agreements), and probably with good reason. They’re hundreds, if not, thousands of pages long. In fact, even contract lawyers with thirty years of experience have struggled in trying to understand these agreements. Deep down, though, each of us knows that we’re signing away our privacy rights to use these platforms and devices. So why do we do it? We don’t truly value privacy as much as we like to believe we do.

What people value is “security,” not privacy. Strong belief in data privacy is dead

Prof. Neil Sahota 2020 ( IBM Master Inventor, United Nations Artificial Intelligence Advisor, Professor at UC Irvine) 14 Oct 2020 “Privacy Is Dead And Most People Really Don’t Care” https://www.forbes.com/sites/neilsahota/2020/10/14/privacy-is-dead-and-most-people-really-dont-care/?sh=5fc1aa97b733

We already live in a world where people are used to sharing everything online. You know those phone phishing scams like the fraudsters pretending to be the IRS? [Young millennials and Generation Z fall victim](https://www.vice.com/en/article/pkedxy/millennials-and-gen-z-get-scammed-more-than-their-grandparents-sorry) to them the most of any generation because they’re used to giving information away. People get important value from these platforms and devices and accept the trade offs for it. Data security is still paramount, but the strong belief for data privacy is pretty much dead.

Naïve to expect privacy any more, and people’s behavior proves they don’t really care

Identity Management Institute 2019 (global certification organization dedicated to identity governance, risk management, and compliance) (article is undated but mentions events in Sept 2019) “6 REASONS WHY DATA PRIVACY IS DEAD” <https://identitymanagementinstitute.org/6-reasons-why-data-privacy-is-dead/> (accessed 27 Nov 2021)

Decreasing difference between private and identifiable data is recognized at the governmental level, which proves that expecting privacy is naïve. In its report published years ago, the Federal Trade Commission raised concerns about “the diminishing distinction” between de-identified and personally identifiable information. Therefore, the “death of privacy” goes far beyond conspiracy theories. Based on our observations of the latest incidents and trends, consumer privacy appears dead no matter how much consumers expect it or organizations, industry experts, and regulators try to ensure the confidentiality of personal information and reassure consumers that all their personal data is in good hands. As we observe the latest trends and news, we have a hard time reconciling consumer expectation of privacy with consumer behavior as they post so many personal information on social media.

There’s nothing anyone can do about data privacy

WALL STREET JOURNAL 2018 (Christopher Mims, technology columnist) 6 May 2018 “Privacy Is Dead. Here’s What Comes Next” <https://www.wsj.com/articles/privacy-is-dead-heres-what-comes-next-1525608001> (accessed 27 Nov 2021)

Short of living in a remote hut while forsaking cellphones, the internet and credit cards, there is no longer any way that you, as an individual, can prevent marketers, governments or malicious actors from gathering and using comprehensive, personally identifying information about you.

SOLVENCY

1. No change in Geofence post-plan

No AI involved, so no “Geofence warrants using AI” are stopped by the AFF plan. This is how Geofence warrants work:

Jennifer Lynch and Nathaniel Sobel 2020. (Lynch – attorney; Surveillance Litigation Director at Electronic Frontier Foundation (EFF). Sobel – writer for EFF) 31 Aug 2020 “New Federal Court Rulings Find Geofence Warrants Unconstitutional” <https://perma.cc/Z772-7UHF> <https://perma.cc/Z772-7UHF> (accessed 22 Jan 2022)

As we’ve seen with other geofence warrants, the government’s original application proposed a three-step protocol to obtain the information. At the first step, Google would produce detailed and anonymized location data for devices that reported their location within the geofences for three forty-five minute periods. After that, the government would review that information and produce a list of devices for which it desired additional information. Then at the last step, Google would be required to produce information identifying the Google accounts for the requested devices.

No AFF evidence that blocking AI would stop geofence warrants

They have to prove that Geofence warrants depend on AI and wouldn’t be done without it. Until they prove that, there’s no solvency.

2. No change in keyword warrants post-plan

Cross-apply the same arguments from geofence.

AFF must prove that keyword warrants only work if AI is used. If not, then nothing changes post-plan.

DISADVANTAGES

1. Unsolved crimes & Justice denied

Someday it could be you: Here’s someone who’s extremely glad geofence warrants exist

Doug Austin 2021. (cybersecurity expert and lecturer) 8 Jan 2021 “Geofence Warrants Can Identify Crime Suspects, But Are There Data Privacy Concerns?: Data Privacy Trends” <https://ediscoverytoday.com/2021/01/08/geofence-warrants-can-identify-crime-suspects-but-are-there-data-privacy-concerns-data-privacy-trends/> (accessed 22 Jan 2022)

Armed with a box cutter and hammer, he made her drive off with him, then forced her to pull over and get into a dark-colored pickup truck, where he sexually assaulted her while an accomplice drove. Then they left her at the side of the road. While that might seem like a random crime with slim odds of being solved (her basic description of the rapist and his truck wasn’t enough to narrow the search and her phone was taken, but it was turned off), she did recall that there was a Samsung Galaxy phone in the car that was running Google Maps as they drove past General Mitchell International Airport.  That led Milwaukee Detective Eric Draeger to seek a “geofence warrant”, which is a “digital data hunt that has since soared in popularity among police seeking help in all sorts of unsolved cases, from burglaries to murders.”
**END QUOTE. HE GOES ON LATER IN THE ARTICLE TO CONCLUDE QUOTE:**
The accomplice pled guilty to kidnapping and was sentenced to 25 years in prison.  The accused rapist went to trial, the jury convicted him of all seven charges related to the attack, and a judge sentenced him to more than 100 years in prison. When asked how the investigation would have gone without the location data from Google, Draeger said, “Without that information from Google, we were toast. They came through with information that gave justice to a woman who needed it.”