

LITIGATING THE 4TH AMENDMENT IN THE SURVEILLANCE STATE

*MSPD Contract Defender
Training*

March 24, 2022



OBJECTIVES

Review current state of Fourth Amendment law in Missouri

Learn about emerging technologies, accompanying police tactics, and how to challenge them under extant SCOTUS jurisprudence.



WHY THIS FIGHT MATTERS

We Want to Win Cases

The Fourth Amendment needs our victories to remain relevant

- “Internet users generate enormous quantities of data, much of it stored by their online service providers. The Fourth Amendment would provide little meaningful protection given modern technology if we retain no reasonable expectation of privacy in what we give to others.” Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search by Stephen E. Henderson

“Ultimately, saying that you don't care about privacy because you have nothing to hide is no different from saying you don't care about freedom of speech because you have nothing to say.” Edward Snowden

“My take is, privacy is precious. I think privacy is the last true luxury. To be able to live your life as you choose without having everyone comment on it or know about.” Valerie Plame



THE DEMISE OF PRIVACY

Modern technology & individual choice



“The Government and people generally do not care about your privacy. Average citizens should not fear government surveillance unless they have top secret information to hide.”

- Elon Musk.



An abstract, textured background featuring a mix of vibrant colors including red, orange, yellow, green, blue, and purple. The texture resembles cracked paint or marbled paper. The text 'FIRST PRINCIPLES' is overlaid in a bold, white, sans-serif font.

FIRST PRINCIPLES

COMPARISON

Federal v. State Constitutions

U.S. Const. amend. IV

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

Mo. Const. art. I, § 15

COMPARISON

Federal v. State Constitutions

U.S. Const. amend. IV

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

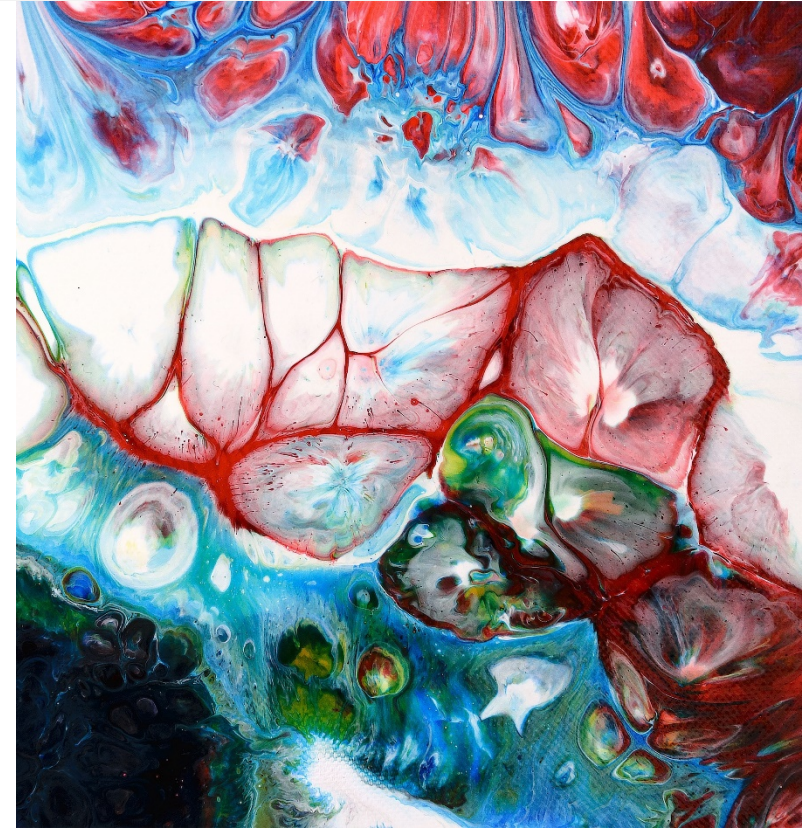
Mo. Const. art. I, § 15

“That the people shall be secure in their persons, papers, homes, effects, **and electronic communications and data**, from unreasonable searches and seizures; and no warrant to search any place, or seize any person or thing, **or access electronic data or communication**, shall issue without describing the place to be searched, or the persons or thing to be seized, **or the data or communication accessed**, as nearly as may be; nor without probable cause, supported by written oath or affirmation.”

STANDING

Is there a reasonable expectation of privacy?

- Subjective: actual expectation of privacy
- Objective: expectation is “one that society is prepared to recognize as reasonable”
- Δ has burden of proof to establish



WARRANTS

Probable cause > reasonable suspicion

- “where the facts and circumstances within the officers’ knowledge, and of which they have reasonably trustworthy information, are sufficient in themselves to warrant a belief by a man of reasonable caution that a crime is being committed.” *Brinegar v. United States*, 338 U.S. 160 (1949).

Particularity

- “The fourth amendment requires that the government describe the items to be seized with as much specificity as the government’s knowledge and circumstances allow, and warrants are conclusively invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics of the goods to be seized.” *State v. Douglass*, 544 S.W.3d 182, 192 (Mo. banc 2018).
- THERE IS NO GOOD FAITH DEFENSE TO A PLAINLY UNPARTICULARIZED WARRANT! *Groh v. Ramirez*, 540 U.S. 551 (2004).



MOTION TO SUPPRESS

Evidence

- Mo. Const. art. I, § 15
- § 542.296 RSMo
 - “A person aggrieved by an unlawful seizure made by an officer and against whom there is pending criminal proceeding growing out of the subject matter of the seizure...” = STANDING
 - **in writing**
 - **before trial** → unless Δ unaware of grounds or had no opportunity to file pretrial
 - notice up for hearing
- Rule 24.05

IN THE CIRCUIT COURT OF BOONE COUNTY
STATE OF MISSOURI

STATE OF MISSOURI,) Cause No. 16BA-CR00037-01
Plaintiff)
) Division No. 2
v.)
)
DAVID L REED,)
Defendant)

MOTION TO SUPPRESS EVIDENCE

COMES NOW David Reed and moves this Court to suppress the evidence obtained in this matter, to wit, all items in the "Search Inventory List" pertinent to this matter, for the reason that said items were obtained in violation of Mr. Reed's right against unreasonable search and seizure protected by the Fourth and Fourteenth Amendments to the United States Constitution as well as by Art. I., Sec. 15, of Missouri's Constitution. This unreasonable seizure also violated Mr. Reed's statutory right regarding lawful application for, and procedure of, executing search warrants as mandated by RSMo Secs. 542.261, 542.266, and 542.271.

The seizure of all items listed in the Inventory Return List pertinent to this cause should be suppressed pursuant to RSMo 542.296.5(2)(3) and (4) for the following reasons:

HEARING MECHANICS

π has the burden:

- “At a hearing on a motion to suppress, the **state** bears both the **burden of producing evidence** and the **risk of nonpersuasion** to show by a **preponderance of the evidence** that the motion to suppress should be overruled.” *State v. Carrawell*, 481 S.W.3d 833, 837 (Mo. banc 2016).
- review of overruled MTS → Ct. App. “considers evidence presented at **both** the suppression hearing and at trial to determine whether sufficient evidence exists in the record to support the trial court’s ruling.” *Id.*



PRESERVATION

DO NOT TAKE YOUR MOTION “WITH THE CASE”

Object to contested evidence as it's offered:

- “When a motion to suppress evidence is denied, and the evidence is offered, **the defendant must object at the trial to preserve his contentions for appellate review.**” *State v. Brown*, 438 S.W.3d 500, 508 (Mo. App. 2014), citing *State v. Powers*, 613 S.W.2d 955, 959 (Mo. App. 1981). This is because the trial judge “should be given an opportunity to reconsider his prior ruling against the backdrop of the evidence actually adduced at trial.” *State v. Fields*, 636 S.W.2d 76, 79 (Mo. App. 1982), citing *State v. Yowell*, 513 S.W.2d 397, 403 (Mo. banc 1974). This also allows the defendant to control whether the objection is maintained or withdrawn.

State v. Hughes, 563 S.W.3d 119, 124 (Mo. banc 2018)

- Renew objections as necessary

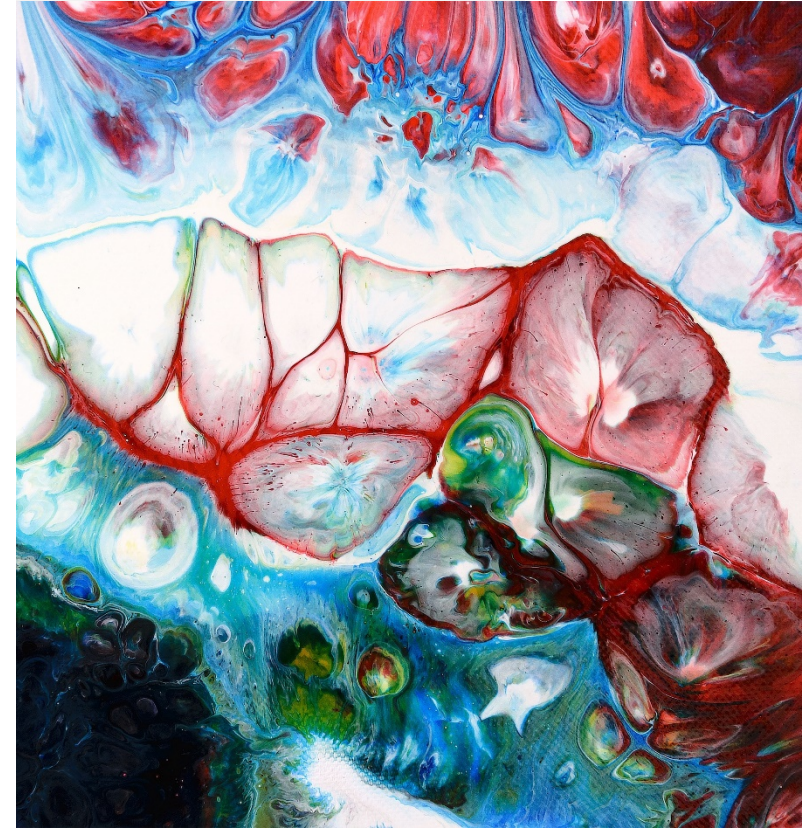
Motion for new trial → claim TC error in both: 1) overruling MTS; and 2) admitting contested evidence



CASUAL ENCOUNTERS

Not a seizure

- Police officer approaches, asks questions, person free to leave. No seizure. *California v. Hodari D.*, 499 U.S. 621 (1991).
- Request for identification doesn't implicate 4th Am. *INS v. Delgado*, 466 U.S. 210 (1984).
- Driving alongside a person who is running in order to conduct further investigation does not constitute a seizure. *Michigan v. Chesternut*, 486 U.S. 567 (1988).
- The mere fact that the police-citizen encounter takes place in a public transportation setting, such as on a bus, does not turn the encounter into a seizure. *Florida v. Bostick*, 501 U.S. 429 (1991).
- If surrounding conditions are so intimidating as to demonstrate that a reasonable person would have believed he was not free to leave if he had not responded, then a seizure occurs. *Florida v. Royer*, 460 U.S. 491 (1983).
- Different factors must be considered when an individual is already stationary, or "when an individual's submission to a show of governmental authority takes the form of passive acquiescence." *Brendlin v. California*, 551 U.S. 249, 255 (2007).



TERRY STOP

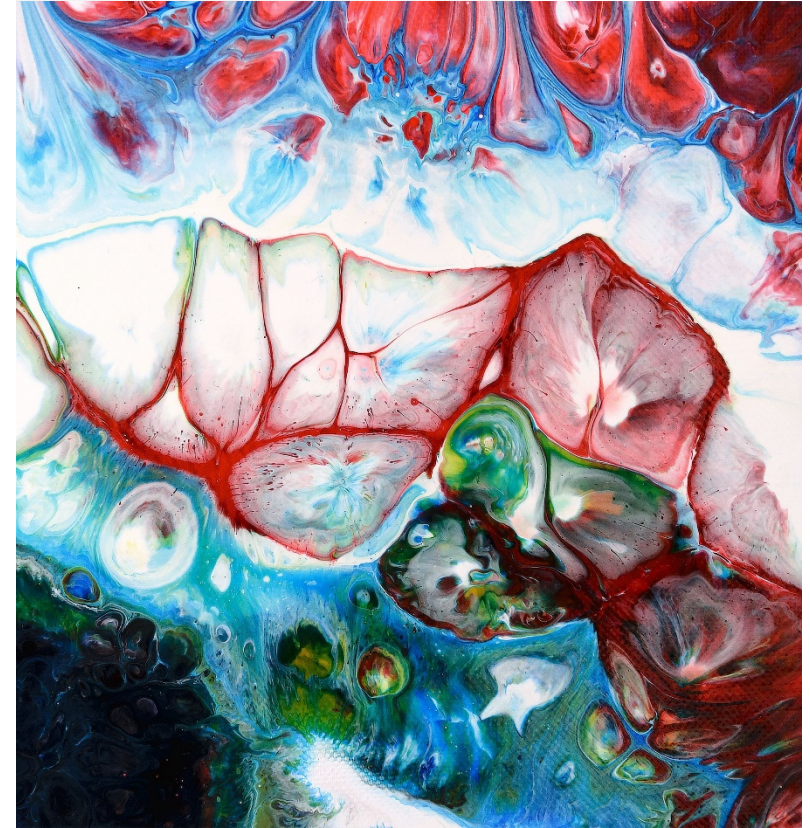
Seizure

Must be supported by **reasonable suspicion**

- Personal observations of the officer
- Information from other officers or dispatch
- Information from witnesses
- Running from officers after approach
- High crime area
- Nervous behavior when combined with inconsistent answers
- Anonymous tips if corroborated

NOT reasonable suspicion:

- Failure to consent to search
- Presence in high crime area late at night
- Anonymous tip standing alone
- Flight that precedes the seizure – see *Hodari D*

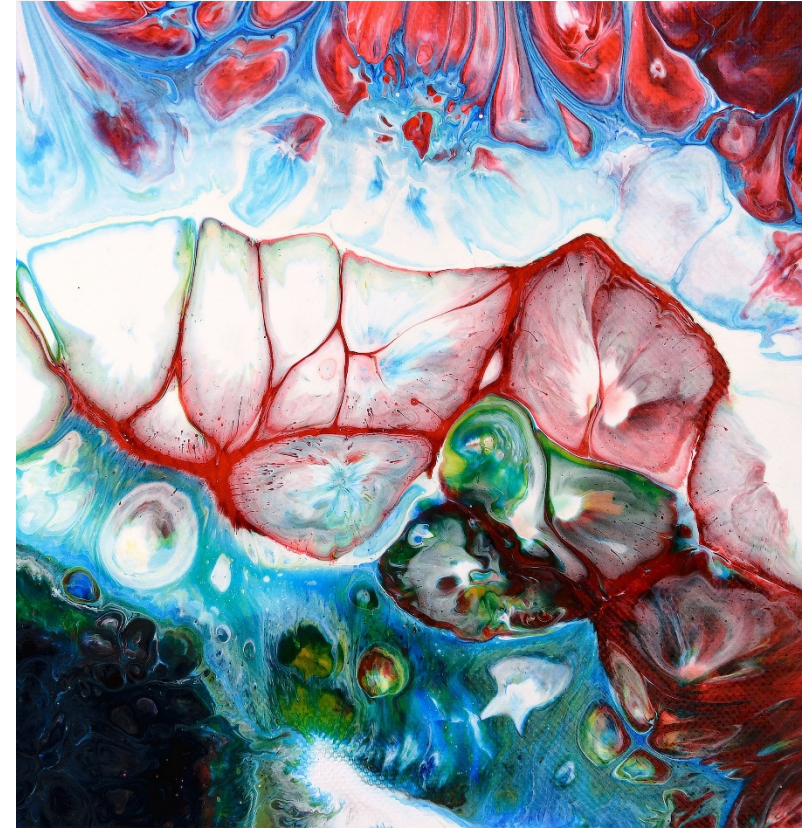


TERRY FRISK

- Limited pat-down for weapons when the officer is justified in the belief that a suspect may be armed and dangerous to the officer or others. *Terry v. Ohio*, 392 U.S. 1, 30-31 (1968)
- Officer must be able to give specific and articulable facts that the officer reasonably believes the person is armed and dangerous

Floyd, et al. v. City of New York, et al., 959 F.Supp. 2d 540 (E.D.N.Y. 2013).

- NYC liable for violating plaintiffs' 4A + 5A rights in departmental practice of suspicion-less stops + frisks of African-American + Latino suspects





WARRANTLESS EXCEPTIONS

or what I like to call...

WARRANTLESS SEARCHES

Permissible when

- Incident to lawful arrest
- Plain view
- Stop and frisk
- Automobile exception
- Hot pursuit
- Exigent circumstances
- Consensual
- Inventory
- “Community caretaking” exception

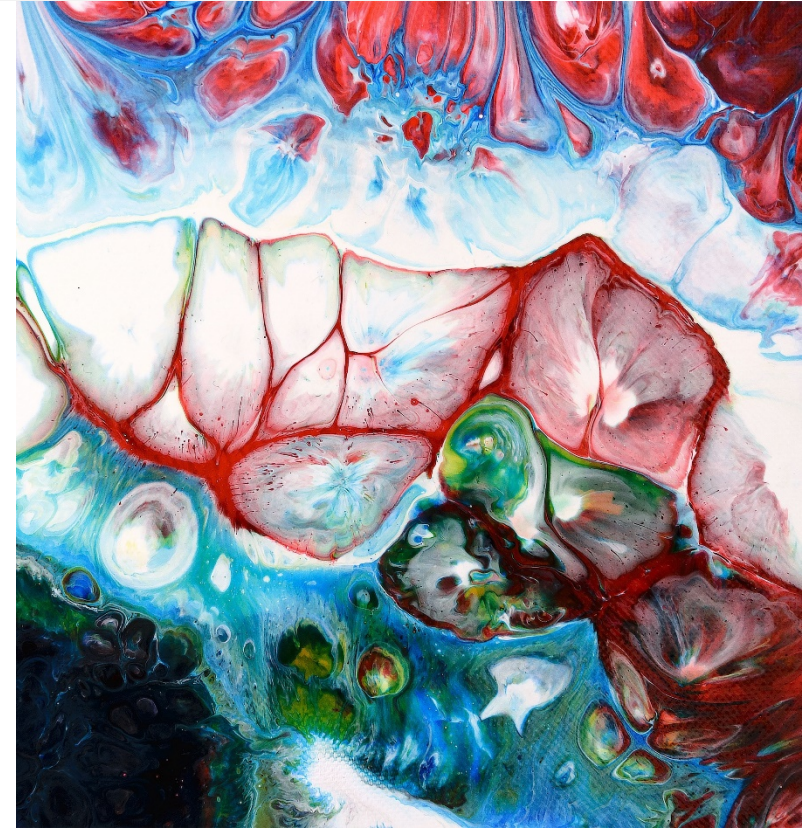


CURTILAGE

Included in the private area of home for which warrant is required

Collins v. Virginia, 138 S.Ct. 1663 (2018).

- Automobile exception does not include the home or curtilage
- Vehicles stored within the home's curtilage cannot be searched without warrant



A SETBACK

Utah v. Strieff, 136 S.Ct. 2056 (2016).

Discovery of pre-existing arrest warrant purged officer's unconstitutional investigatory stop, despite officer's ignorance of the warrant.

SCOTUS emphasized lack of “**flagrant** police misconduct” + no “indication that stop was part of any **systematic or recurrent** police misconduct.”

This means discovery of warrant is *per se* “critical intervening circumstance” breaking chain of causation with illegality + **dissipating its taint**

Reifies notion that exclusion is “**last resort**” and not “first impulse”

Practice tip: make a **showing of misconduct** at suppression hearing



FORCIBLE BLOOD DRAW

Dissipation of alcohol in the bloodstream \neq exigency justifying forcible blood draw: “In these drunk-driving investigations where police officers can reasonably obtain a warrant before a blood sample can be drawn without significantly undermining the efficacy of the search, the Fourth Amendment mandates that they do so.”

Missouri v. McNeely, 569 U.S. 141 (2013).

Breath test \neq substantial intrusion on a defendant, but blood draw does. States can criminalize breath test refusal without a warrant, but cannot criminalize refusal of blood draw absent a warrant.

Birchfield v. North Dakota, 136 S.Ct. 2160 (2016).



IMPLIED CONSENT STATUTE

§ 577.033 RSMo:

- “Any person who is dead, unconscious or who is otherwise in a condition rendering him incapable of refusing to take a test as provided in sections 577.020 to 577.041 shall be deemed not to have withdrawn the consent provided by section 577.020 and the test or tests may be administered.”

“When police have probable cause to believe a person has committed a drunk-driving offense and the driver’s unconsciousness or stupor requires him to be taken to the hospital or similar facility before police have a reasonable opportunity to administer a standard evidentiary breath test, they may almost always order a warrantless blood test to measure the driver’s BAC without offending the Fourth Amendment.”

Mitchell v. Wisconsin, 139 S.Ct. 2525, 2539 (2019).

BUT, SCOTUS did not foreclose “unusual” circumstance where Δ could show blood would not have been drawn if LE had not been seeking BAC info + that LE did not reasonably judge that warrant application interfered with other pressing concerns





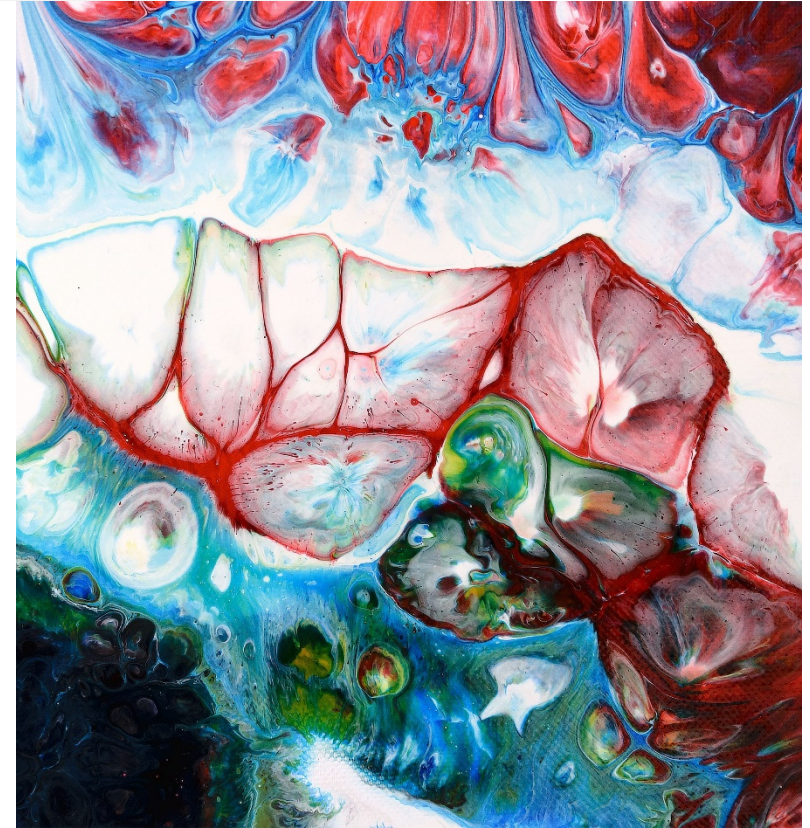
JONES, RILEY, CARPENTER, AND THE NEW “REASONABLE EXPECTATION OF PRIVACY”

*“seismic shift” in 4th
Amendment
jurisprudence*

KATZ + PROGENY

4A protections tied to **places + things**

- *i.e.*, whether person has reasonable expectation of privacy in place like a home, or in a thing, like a car, that was invaded by government's access of information from inside place/thing

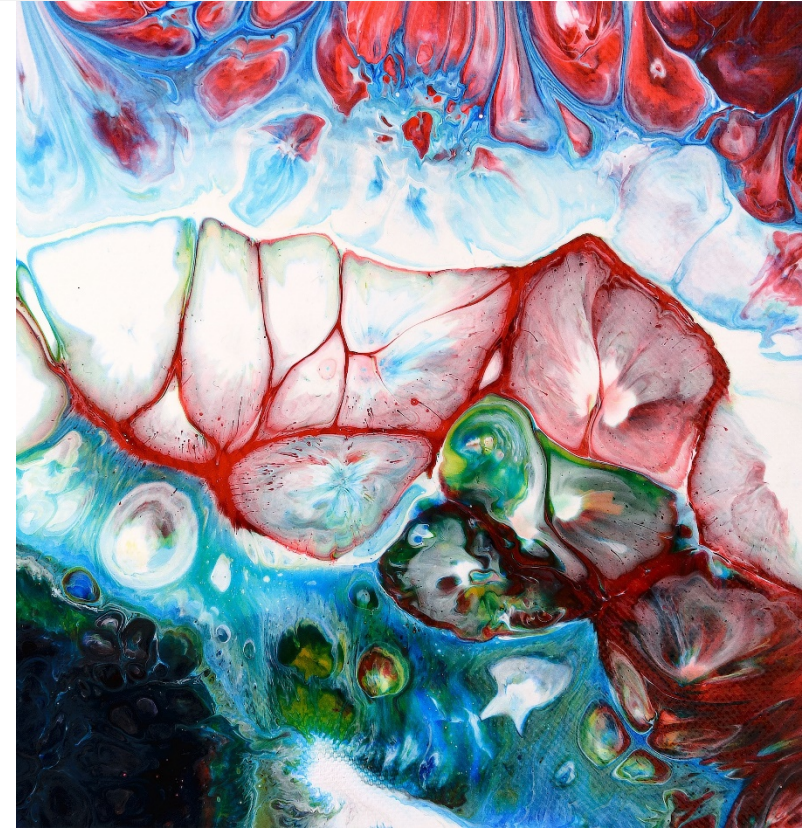


THIRD-PARTY DOCTRINE

No legitimate expectation of privacy in information voluntarily disclosed to 3P

United States v. Miller, 425 U.S. 435 (1976) (bank records).

Smith v. Maryland, 442 U.S. 735 (1979) (pen register \neq search)

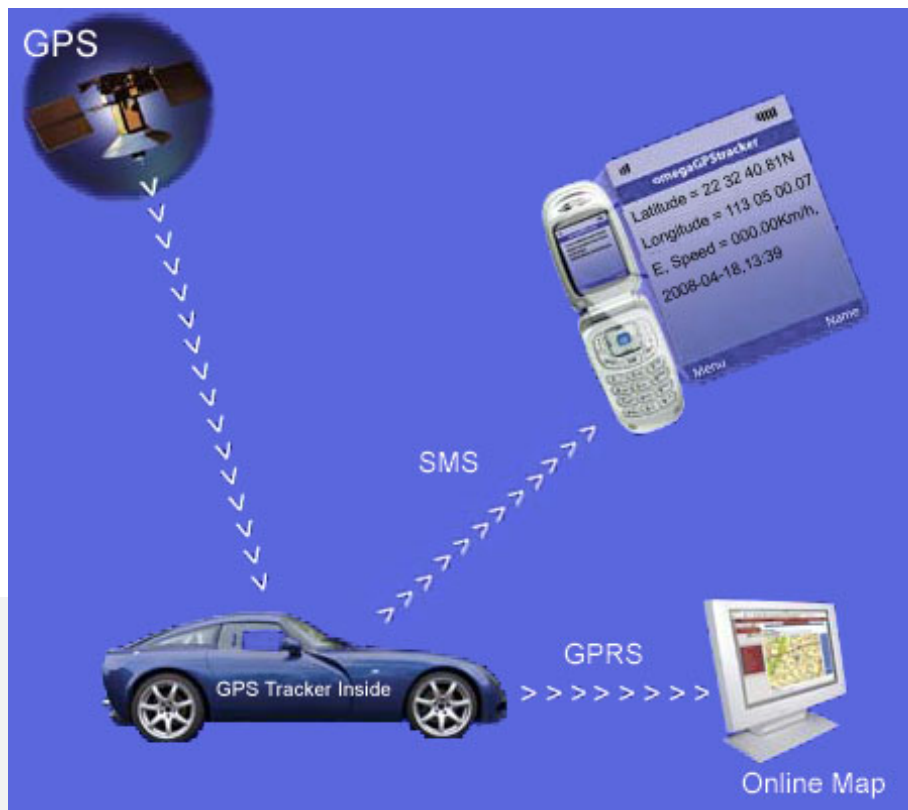


JONES

United States v. Jones, 565 U.S. 400 (2012).

GPS tracker affixed to car + used to monitor movements = “search”

- physical government trespass on “effects”



JONES

United States v. Jones, 565 U.S. 400 (2012).

Concurrence (Sotomayor):

- “More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”

Concurrence (Alito):

- appropriate question + interpretation of 4A is “whether respondent’s reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle that he drove.”
- “a reasonable person would not have anticipated” police to engage in 28 days of location monitoring in routine criminal case



RILEY

Riley v. California, 573 U.S. 373 (2014).

Cell phone searches incident to arrest require a warrant

- hold for many the “privacies of life” → “contains a broad array of private information never found in the home in any form – unless the phone is.”
- “**minicomputers** that also happen to have the capacity to be used as a telephone.”
- “Allowing the police to scrutinize such [voluminous personal] records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.”

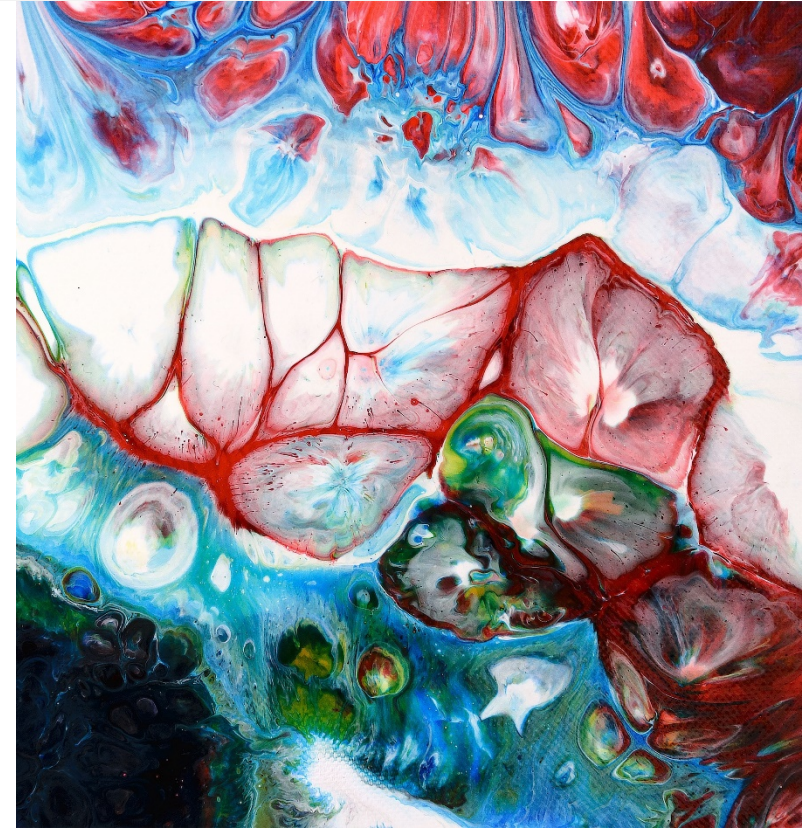
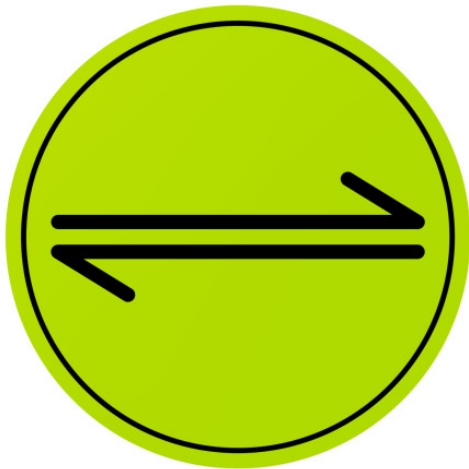


RILEY

Riley v. California, 573 U.S. 373 (2014).

Equilibrium Adjustment theory of 4A:

- SCOTUS tightens 4A protection when technology expands police power and loosens 4A protection when new technology restricts police power.



MISSOURI + RILEY

What does a *Riley* warrant look like?

STATE'S EXHIBIT
14

16BA MC00307

FILED
BOONE COUNTY
FEB 19 2016
CHRISTY BLAKEMORE
CLERK CIRCUIT COURT COLUMBIA, MO

SEARCH WARRANT
TO AUTHORIZE SEARCH FOR:

X PROPERTY, ARTICLE, MATERIAL OR SUBSTANCE THAT CONSTITUTES EVIDENCE OF THE COMMISSION OF A CRIMINAL OFFENSE; Felony Drug Possession RSMO 195.202, Distribution Deliver and Manufacture of a Controlled Substance RSMO 195.211, and Rape in the First Degree RSMO 566.030 to wit:

Illegal controlled substances, and drug paraphernalia. All bedding materials (i.e. sheets, mattress pads, comforters, blankets, pillow cases etc). All cell phones, electronic tablets, computers, digital media storage devices (hard drives, USB devices), (and to conduct an off-premises examination/search of said devices for all data/software as defined by RSMO 556.063) pertaining to the offense Distribution Deliver and Manufacture of a Controlled Substance RSMO 195.211, and Rape in the First Degree RSMO 566.030.

STATE OF MISSOURI)
) ss.
COUNTY OF BOONE)

IN THE CIRCUIT COURT, DIVISION B, WITHIN AND FOR SUCH COUNTY, THE STATE OF MISSOURI TO ANY PEACE OFFICER IN THE STATE OF MISSOURI:

WHEREAS, a complaint in writing, duly verified by oath, has been filed with the undersigned Judge of this Court, stating upon information and belief that

X PROPERTY, ARTICLE, MATERIAL OR SUBSTANCE THAT CONSTITUTES EVIDENCE OF THE COMMISSION OF A CRIMINAL OFFENSE; Felony Drug Possession RSMO 195.202, Distribution Deliver and Manufacture of a Controlled Substance RSMO 195.211, and Rape in the First Degree RSMO 566.030 to wit:

Illegal controlled substances, and drug paraphernalia. All bedding materials (i.e. sheets, mattress pads, comforters, blankets, pillow cases etc). All cell phones, electronic tablets, computers, digital media storage devices (hard drives, USB devices), (and to conduct an off-premises examination/search of said devices for all data/software as defined by RSMO 556.063) pertaining to the offense Distribution Deliver and Manufacture of a Controlled Substance RSMO 195.211, and Rape in the First Degree RSMO 566.030.

127 8th St South Apartment 519, in Boone County/Columbia Missouri. The residence is an apartment on the 5th floor in the District Flats apartment building. The numbers 519 are attached next to the door to the apartment. The residence has a single entrance located in the hallway of the 5th floor. The exterior of the building is a brick construction with a main entrance located at the intersection of South 8th Street and Locust Street. The building is marked by the title "District Flats" above the doors facing Locust Street.

The search warrant should also include all persons, and motor vehicles on the premises, or on the adjacent street near the premises determined to be associated with the listed address; and That the basis of affiant's information and belief is contained in the attached affidavits of witnesses to facts concerning the said matter which affidavits are made a part hereof and are submitted herewith as a basis upon which this court may find the existence of a probable cause for the issuance of said warrant.

WHEREAS, the Judge of this Court from the sworn allegations of said complaint and from the supporting written affidavits filed therewith has found that there is probable cause to believe the allegations of the complaint to be true and probable cause for the issuance of a search warrant herein;

This Court grants permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described herein, including conducting an off-site examination. This Court further grants permission to continue the forensic examination beyond the time at which the return of the search warrant is made to this court.

NOW, THEREFORE, these are to command you that you search the said premises above described within ten (10) days after the issuance of this warrant, the search may be made at night if making it during the daytime is not practicable, and take with you, if need be, the power of your county, and, if said above described property or any part thereof be found on said premises by you, that you seize the same and take same into your possession, making a complete and accurate inventory of the property so taken by you in the presence of the person from whose possession the same is taken, if that be possible, and giving to such person a receipt for such property, together with a copy of this warrant, or if no person be found in possession of said property, leaving said receipt and said copy upon the premises searched, and that you thereafter return the property so taken and seized by you, together with a duly verified copy of the inventory thereof and with your return to this warrant to this court to be herein dealt with in accordance with law.

Witness my hand and the seal of this court this 19 day of Feb, 2016 at 1:10 pm.

Christy Blakemore
Judge of said Court

2/19/16 Christy Blakemore

MISSOURI + *RILEY*

What does a *Riley* warrant look like?

STATE'S EXHIBIT 14

16BA-MC00307

FILED BOONE COUNTY FEB 19 2016 CHRISTY BLAKEMORE CLERK CIRCUIT COURT COLUMBIA, MO

SEARCH WARRANT TO AUTHORIZE SEARCH FOR:

☒ PROPERTY, ARTICLE, MATERIAL OR SUBSTANCE THAT CONSTITUTES EVIDENCE OF THE COMMISSION OF A CRIMINAL OFFENSE; Felony Drug Possession RSMO 195.202, Distribution, Delivery and Manufacture of a Controlled Substance RSMO 195.211, and Rape in the First Degree RSMO 566.030

Illegal controlled substances, including but not limited to, marijuana, cocaine, heroin, crack cocaine, and other controlled substances, and drug paraphernalia. All bedding materials (i.e. sheets, mattress pads, pillow cases etc). All cell phones, electronic tablets, computers, digital media storage devices (hard drives, USB drives, etc), (and to conduct an off-premise search of said devices for all data/software as defined by RSMO 566.063) pertaining to the offense of Distribution, Delivery and Manufacture of a Controlled Substance RSMO 195.211, and Rape in the First Degree RSMO 566.030.

STATE COURT, DIVISION 1, WITHIN AND FOR SUCH COUNTY, THE COUNTY OF MISSOURI:

It is in writing, duly verified by oath, has been filed with the undersigned Judge of said Court.

ARTICLE, MATERIAL OR SUBSTANCE THAT CONSTITUTES EVIDENCE OF THE COMMISSION OF A CRIMINAL OFFENSE; Felony Drug Possession RSMO 195.202, Distribution, Delivery and Manufacture of a Controlled Substance RSMO 195.211, and Rape in the First Degree RSMO 566.030 to wit:

substances, and drug paraphernalia. All bedding materials (i.e. sheets, mattress pads, pillow cases etc). All cell phones, electronic tablets, computers, digital media storage devices (hard drives, USB drives, etc), (and to conduct an off-premise search of said devices for all data/software as defined by RSMO 566.063) pertaining to the offense of Distribution, Delivery and Manufacture of a Controlled Substance RSMO 195.211, and Rape in the First Degree RSMO 566.030.

Apartment 519, in Boone County/Columbia Missouri. The residence is an apartment on Locust Street. The numbers 519 are attached next to the door to the apartment. The residence has a brick exterior. The exterior of the building is a brick construction with a main entrance located at the corner of Locust Street and Locust Street. The building is marked by the title "District Flats" above the doors facing Locust Street.

should also include all persons, and motor vehicles on the premises, or on the premises associated with the listed address; and That the basis of affiant's information and facts concerning the said matter which affidavits are made a part hereof are sufficient to find the existence of a probable cause for the issuance of said warrant.

Court from the sworn allegations of said complaint and from the facts set forth in this warrant, cause to believe the allegations of the complaint to be true.

Witness my hand and the seal of said Court this 19th day of February, 2016.

2/19/16 Stephanie M. M... Judge of said Court

MISSOURI + *RILEY*

One published post-*Riley* case broaching scope of cell phone search

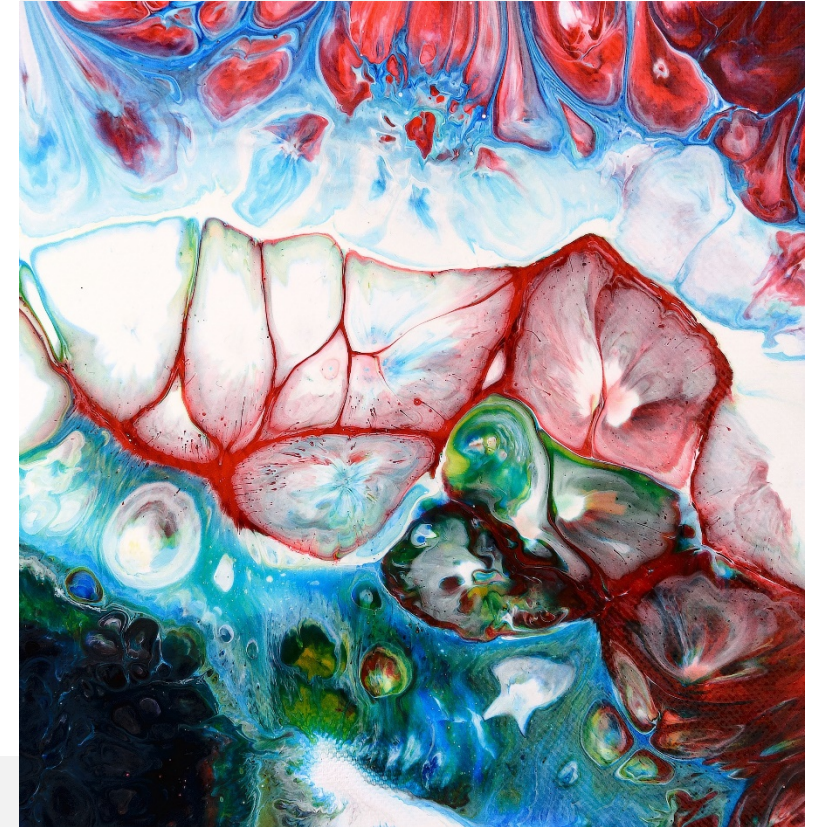
State v. Johnson, 576 S.W.3d 205 (Mo. App. W.D. 2019).

- Warrant to search “all data/software” on phone sufficiently particular + not overbroad

data are concealed there.” *English*, 52 Misc. 3d at 321-22. Just as a warrant authorizing a search of a filing cabinet allows the search of every document in the files because the incriminating evidence may be found in any file or folder, so too should a warrant allow the search of every document on a cell phone, which serves the same function as a filing cabinet. *Bishop*, 910 F.3d at 337 (citing *Andresen v.*

25

Maryland, 427 U.S. 463 (1976) and *Riley*, 134 S. Ct. at 2489). Thus, a warrant is sufficiently particular if it “cabins the things being looked for by stating what crime is under investigation.” *Id.*



MISSOURI + *RILEY*

What does a *Riley* warrant look like?

State v. Bales, 630 S.W.3d 754 (Mo. banc 2021).

SEARCH WARRANT TO AUTHORIZE THE SEARCH FOR EVIDENCE OF VIOLATIONS OF
CHAPTER 568, RSMO

STATE OF MISSOURI)
) ss.
COUNTY OF PULASKI)

IN THE CIRCUIT COURT WITHIN AND FOR SAID COUNTY
THE STATE OF MISSOURI TO ANY PEACE OFFICER IN THE STATE OF MISSOURI:


WHEREAS, a Complaint in writing, duly verified by oath, has been filed with the undersigned Judge of evidence of the crime of Endangering the Welfare of a Child in the 2nd Degree RSMO 568.050 and Abuse or Neglect of a Child 1st Degree RSMO 568.060.

Phone messages, text messages, social media networks, Instagram photos, Facebook messages, passwords to the device, global positioning system coordinates, emails, phone logs, SIM cards, photo galleries, voicemails, or any other evidence pertaining to the crime kept in the following described places, in the County aforesaid, to wit:

A cell phone located at, 13251 Highway O Dixon, in Pulaski County Missouri. This cell phone is described as Black Samsung with black case.

WHEREAS, the Judge of this Court, from the sworn allegations, of said Complaint and from the supporting written affidavit filed therewith, has found that there is probable cause to believe the allegations of the Complaint to be true and probable cause for the issuance of a Search Warrant herein.

NOW THEREFORE, these are to command you that you search the said premises above described to including text messages, passwords, global positioning system, emails, phone records or all other digital folders, in question within ten days after the issuance of this warrant by day or night, and take with you, if need be, the power of your county, and, if said above described articles or any part thereof be found on said premises by you, that you seize the same and take same into your possession, making a complete and accurate inventory of the articles so taken by you in the presence of the person from whose possession the same is taken, if that be possible, and giving to such person a receipt for such property, together with a copy of this warrant, or, if no person be found in possession of said articles, leaving said receipt and said copy upon the premises searched, and that you thereafter return the property so taken and seized by you, together with a duly verified copy of the inventory thereof and with your return to this warrant to this court to be herein dealt with in accordance with law. Witness by hand and seal of this court on this 24th day of MARCH, 2019, at 3:50 o'clock pm


Honorable Michael Headrick
Judge of the 25th Judicial Circuit

MISSOURI + *RILEY*

What does a *Riley* warrant look like?

State v. Bales, 630 S.W.3d 754 (Mo. banc 2021).

SEARCH WARRANT TO AUTHORIZE THE SEARCH FOR EVIDENCE OF VIOLATIONS OF
CHAPTER 568, RSMO

THE CIRCUIT COURT WITHIN
STATE OF MISSOURI

COUNTY OF PULASKI


WHEREAS, a Complaint in writing, duly verified by oath, has been filed in this court charging the defendant with the crime of Endangering the Welfare of a Child in the 2nd Degree and Neglect of a Child 1st Degree RSMO 568.060.

one messages, text messages, social media networks, Instagram photos, Facebook messages, global positioning system coordinates, emails, phone logs, SIM cards, photographs, and other evidence pertaining to the crime kept in the following described places, in the

A cell phone located at, 13251 Highway O Dixon, in Pulaski County Missouri. This Black Samsung with black case.

WHEREAS, the Judge of this Court, from the sworn allegations, of said Complaint and the written affidavit filed therewith, has found that there is probable cause to believe the all the true and probable cause for the issuance of a Search Warrant herein.

NOW THEREFORE, these are to command you that you search the premises, in and about the premises, including text messages, passwords, global positioning system, emails, phone records, and any other articles, within ten days after the issuance of this warrant by day or night, and that you seize the same and take them to the court in and about the premises, and if said above described articles or any part thereof be found, and giving to such person a receipt for such property into your possession, making a complete inventory of said articles, leaving said receipt and said inventory with the person from whose possession you thereafter return the property so taken and seized by you, together with a duly verified copy of the inventory thereof and with your return to this warrant to this court to be herein dealt with in accordance with law. Witness by hand and seal of this court on this 24th day of MARCH, 2019, at 3:50 o'clock PM.

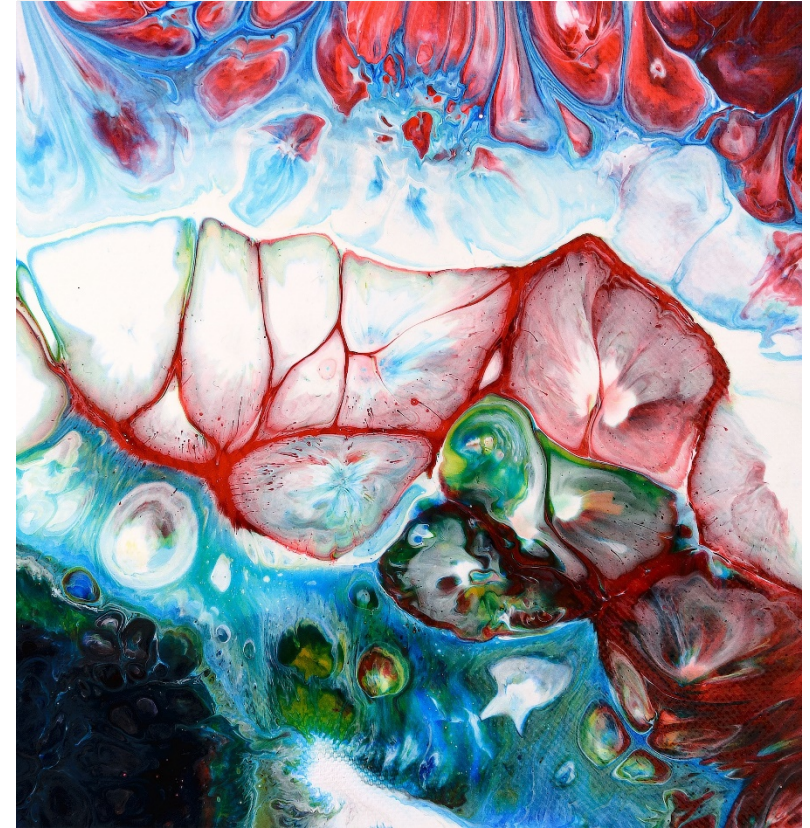

Honorable Michael Headrick
Judge of the 25th Judicial Circuit

MISSOURI + *RILEY*

One published post-*Riley* case on warrant specificity for phone seizure

State v. Bales, 630 S.W.3d 754, 762 (Mo. banc 2021).

- Warrant to seize + search “Black Samsung with black case” at certain residential address
- “The March search warrant authorized the search of a black Samsung cell phone in a black case located at 13251 Highway O, Dixon, and authorized officers to search it for electronic data. Executing the March search warrant at the sheriff’s office, or any location other than 13251 Highway O, Dixon, was beyond the scope of the search authorized by the warrant.”



OTHER JURISDICTIONS + *RILEY*

Significant recent opinion

People v. Coke, 461 P.3d 508, 516 (Colo. 2020).

- Warrant to search for the following:
 - Data which tends to show possession, dominion and control over said equipment; including but not limited to system ownership information, phone number, pictures, or documents bearing the owner's name or information;
 - Any electronic data that would be illegal to possess (contraband), or fruits or proceeds of a crime, or data intended to be used in the commission of a crime;
 - All telephone contact lists, phone books and telephone logs;
 - Any text messages and [MMS] stored, sent, received or deleted;
 - Any photographs or images stored, sent, received or deleted;
 - Any videos stored, sent, received or deleted[;]
 - Any electronic data packets stored, sent, received or deleted.

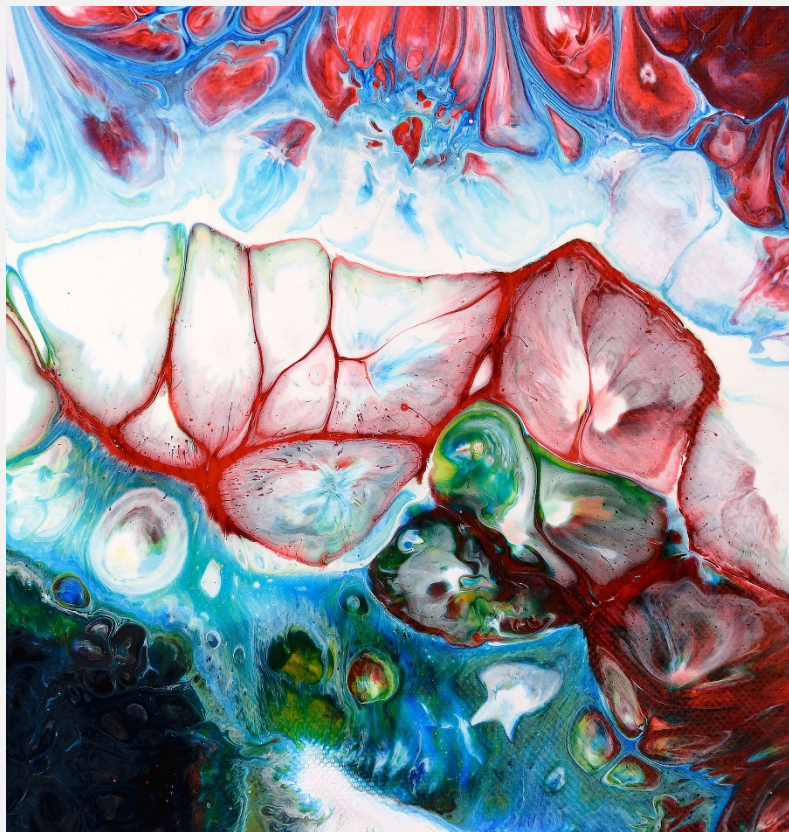
“[T]he warrant at issue here contains no particularity as to the alleged victim or to the time period during which the assault allegedly occurred. Rather, it permitted the officers to search all texts, videos, pictures, contact lists, phone records, and any data that showed ownership or possession. We conclude that such broad authorization violates the particularity demanded by the Fourth Amendment.”



CARPENTER

Carpenter v. United States, 138 S.Ct. 2206 (2018).

A new expectation of privacy test



DECIDED

Carpenter v. United States

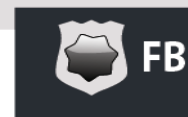
6.22.18

Government needs a 4th Am. warrant to get your cell phone location data.

Carpenter and Sanders were convicted of robberies based on cell phone location data that the FBI got from their cell phone providers.



The FBI did not get a warrant by showing "probable cause." The FBI got a court order by showing less: "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation."



Did the government need a warrant with *probable cause*?

Warrants covered by the 4th Amendment require *probable cause*.

The 4th Amendment applies if you have a "*reasonable expectation of privacy*."

The government argued cell phone location data is not covered.

A 1976 case says there's *not a reasonable expectation of privacy* for this data.

Third Party Doctrine:

United States v. Miller (1976)

Information you *voluntarily give* to a *third party* does not carry a reasonable expectation of privacy. E.g. bank records and dialed phone numbers.

The Supreme Court ruled:

The *Third Party Doctrine* does not apply to cell phone location data.

Cell location data relates more to this concern:

Privacy in physical movements

Location data must be strongly protected.

Than it does to this exception:

Voluntarily handing over

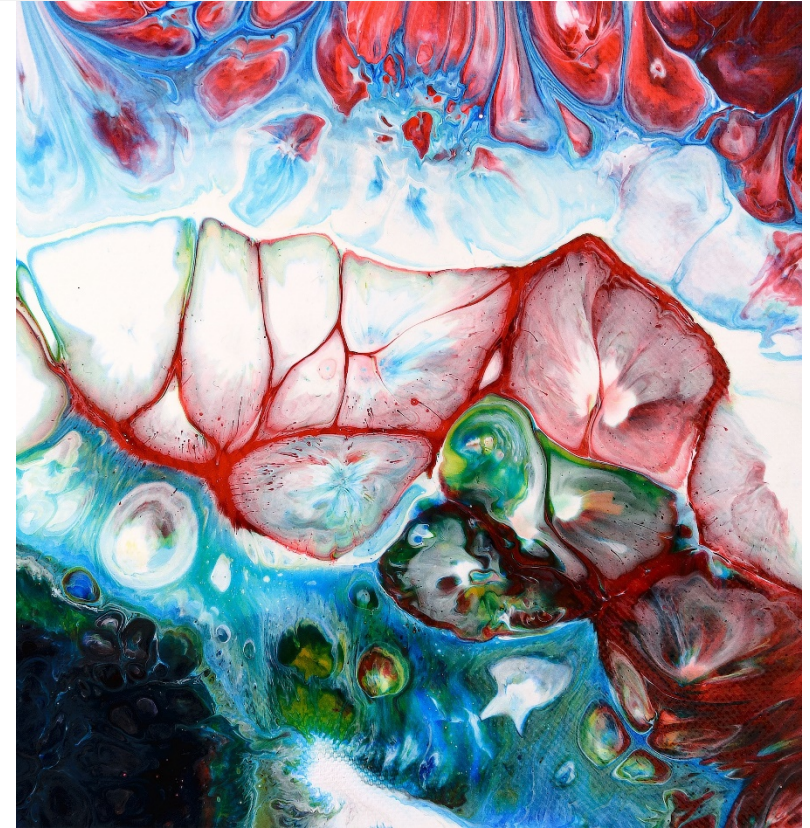
We don't exactly "share" cell location data.

CARPENTER

Carpenter v. United States, 138 S.Ct. 2206 (2018).

“an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI.”

- info divulged to/obtained thru third party (wireless carrier) = search
- ∴ warrant generally required to acquire records



CARPENTER

Carpenter v. United States, 138 S.Ct. 2206 (2018).

concurring). Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so “for any extended period of time was difficult and costly and therefore rarely undertaken.” *Id.*, at 429 (opinion of ALITO, J.). For that reason, “society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual’s car for a very long period.” *Id.*, at 430.

Allowing government access to cell-site records contravenes that expectation. Although such records are generated for commercial purposes, that distinction does not negate Carpenter’s anticipation of privacy in his physical location. Mapping a cell phone’s location over the course of 127 days provides an all-encompassing record of the holder’s whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person’s life, revealing not only his particular movements, but through them his “familial, political, professional, religious, and sexual associations.” *Id.*, at 415 (opinion of SOTOMAYOR, J.). These location records “hold for many Americans the ‘privacies of life.’” *Riley*, 573 U. S., at ____ (slip op., at 28) (quoting *Boyd*, 116 U. S., at 630). And like



INTERPRETING *CARPENTER*

How did SCOTUS reach its decision?

Public policy → adopted new theory by looking
backwards + forwards



INTERPRETING *CARPENTER*

How did SCOTUS reach its decision?

Echoes *Jones* concurrence (Alito, J.):

Search because “a reasonable person **would not have anticipated**” police to track Carpenter’s location over 127 days for routine robberies



INTERPRETING *CARPENTER*

How did SCOTUS reach its decision?

Echoes *Jones* concurrence (Sotomayor, J.):

Cell phone users don't generate CSLI voluntarily, because carrying [a cell phone] is “**indispensable** to participation in modern society.”

i.e., no “**meaningful**” voluntary choice in CSLI creation



INTERPRETING *CARPENTER*

How did SCOTUS reach its decision?

***Riley* equilibrium adjustment theory:**

When invasive digital tracking capability – even that possessed by third parties – expands government power in a transformative way, SCOTUS changes the extant *Katz* REP test to restore preexisting limits on that power.

“To avoid a dramatic increase in government power, the new surveillance tools that digital technology creates are to be slotted into the legal box of searches that require a warrant.”



INTERPRETING *CARPENTER*

How did SCOTUS reach its decision?

Carpenter reframes the REP test → asks:

“Has technology changed citizens’ expectations of *what police can do?*”

CSLI = “absolute surveillance”; “deeply revealing”; “detailed chronicle of a person’s physical presence”; “all-encompassing”

Creates **narrative** → not merely person’s location, “but through them [their] familial, political, professional, religious, and sexual associations.”



INTERPRETING *CARPENTER*

One test for a *Carpenter* search:

1. Records sought are available because of digital technology
2. Record created without subject's meaningful voluntary choice
3. Records tend to reveal “privacies of life”

Orin Kerr, *The Digital Fourth Amendment* (forthcoming).



INTERPRETING *CARPENTER*

Another test for a *Carpenter* search:

1. **Comprehensiveness**
2. **Intimacy**
3. **Expense**
4. **Retrospectivity**
5. **Voluntariness**

Laura Hecht-Felella, *The Fourth Amendment in the Digital Age*, Brennan Center for Justice (2021).



INTERPRETING *CARPENTER*

WHEN does a *Carpenter* search begin?

“The location information obtained from Carpenter’s wireless carriers was the *product* of a search.”

1. Search occurred without a taking of information from any particular person/place/thing.
2. Result > Process → *i.e.*, How gov’t ended up with too much info is irrelevant because search occurred somewhere in steps to get info
3. Access or acquisition?



IMPLEMENTING *CARPENTER*

What does it mean for other emergent technologies + tactics?

Three approaches:

1. Subjective
2. Mosaic Theory
3. Source Rule



IMPLEMENTING *CARPENTER*

Subjective

Focus on when government learned the kind of private information that *Carpenter* protects

- Search occurs moment the government learns particular invasive, private fact about a person



IMPLEMENTING *CARPENTER*

Mosaic Theory

-
-
-

Short-term or narrow evidence collection akin to
traditional surveillance \neq search



IMPLEMENTING *CARPENTER*

Mosaic Theory



Long-term or broad surveillance = search



IMPLEMENTING *CARPENTER*

Source Rule

Government access to **any** information that owes its source to *Carpenter*-protected information is a search

- issue becomes whether government obtained **compelled** access to data that reveals any part of information covered by *Carpenter*
- protects one datum equivalent to entire database



IMPLEMENTING *CARPENTER*

Source Rule


Example: text message metadata

Historical 4A analysis → SMS content protected, but non-content metadata not

Post-Carpenter:

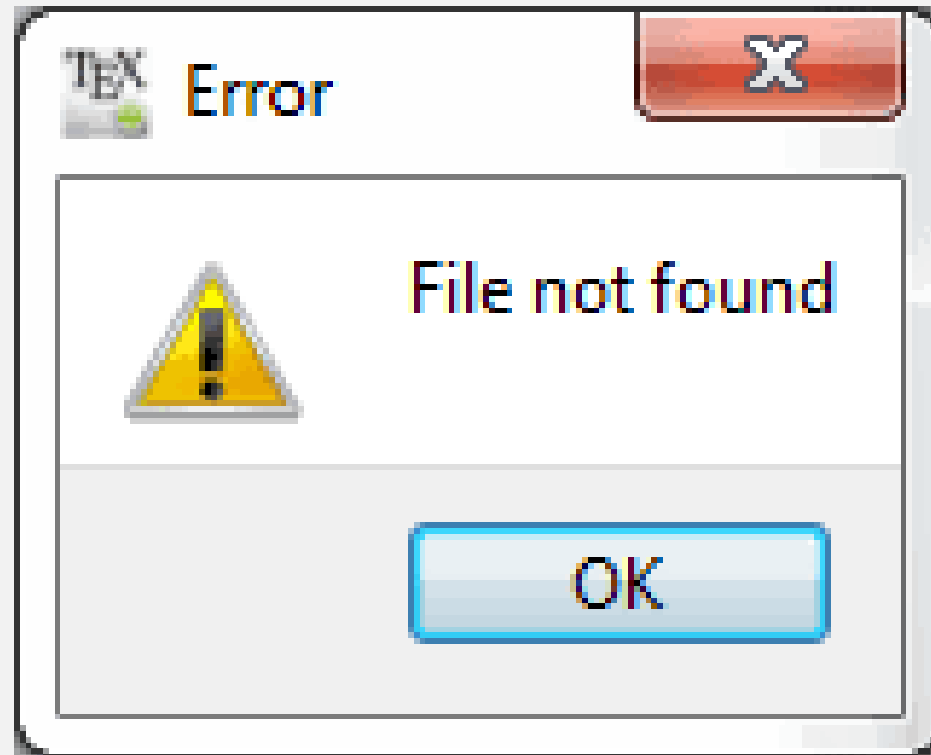
1. SMS metadata category of info not readily acquired in pre-digital age → orders of magnitude different than phone calls/postal mail
2. SMS, email, Facebook messaging, etc. have become “indispensable to participation in modern society” → metadata created without “meaningful” voluntary choice
3. Metadata shows lifestyles, relationships, precisely with whom communicating → reveals “intimate portrait” of person’s life





APPLYING *CARPENTER* TO EMERGING TECHNOLOGIES

*Opportunities for
creative practice*



THE RISE OF SOCIAL MEDIA

- Facebook, the largest social media platform in the world, has 2.4 billion users. Other social media platforms including Youtube and Whatsapp also have more than one billion users each.
- These numbers are huge – there are **7.7 billion people** in the world, with at least **3.5 billion of us online**. This means social media platforms are used by one-in-three people in the world, and more than two-thirds of all internet users.
- Social media has changed the world. The rapid and vast adoption of these technologies is changing how we **find partners**, how we **access information from the news**, and how we **organize to demand political change**.



YOUR DIGITAL FINGERPRINT

Who Is Using Social Media for Investigative Purposes?



Federal: 81%



State: 71%



Local: 82%



Rank & File: 79%



Supervisory: 85%



Agencies serving smaller populations and with fewer sworn personnel use social media more often



86% usage in cities under 50K



76% usage in cities 51-100K



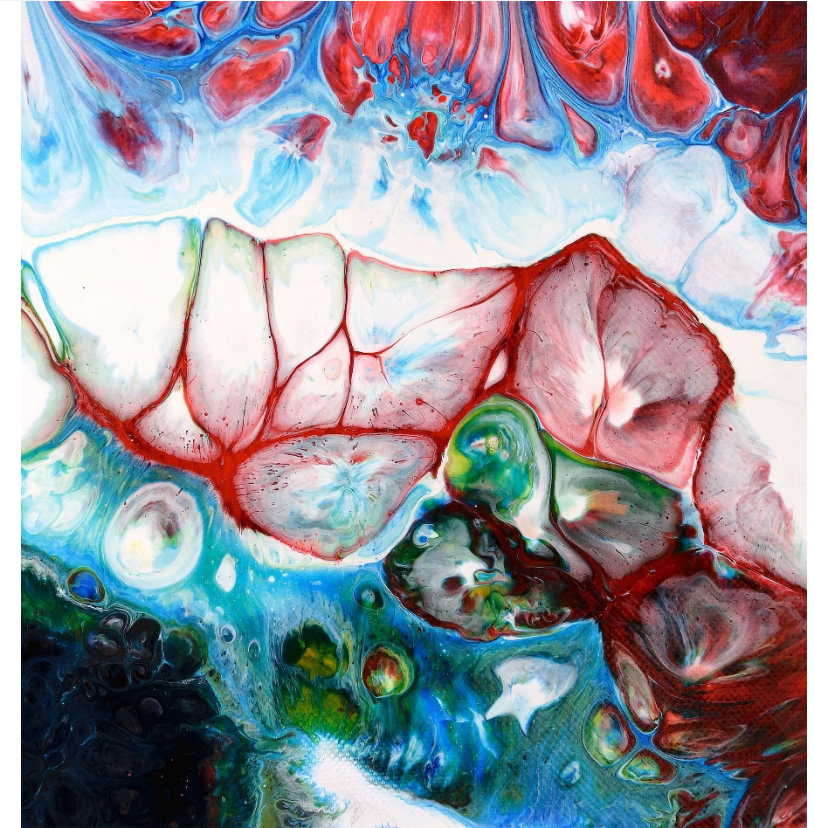
78% usage in cities over 100K

SMMS

Social Media Monitoring Software

Cf. SMS

DigitalStakeout



WHAT WE (ALL) SEE



Donald J. Trump ✓

@realDonaldTrump

Follow

Everywhere Marie Yovanovitch went turned bad. She started off in Somalia, how did that go? Then fast forward to Ukraine, where the new Ukrainian President spoke unfavorably about her in my second phone call with him. It is a U.S. President's absolute right to appoint ambassadors.



Donald J. Trump ✓

@realDonaldTrump



Very little pick-up by the dishonest media of incredible information provided by WikiLeaks. So dishonest! Rigged system!

3:46 PM - 12 Oct 2016 · United States



Donald J. Trump ✓

@realDonaldTrump

Follow

Inconceivable that the government would break into a lawyer's office (early in the morning) - almost unheard of. Even more inconceivable that a lawyer would tape a client - totally unheard of & perhaps illegal. The good news is that your favorite President did nothing wrong!

7:10 AM - 21 Jul 2018

24,745 Retweets 104,357 Likes



74K 25K 104K



Donald J. Trump ✓

@realDonaldTrump

Follow

I am being investigated for firing the FBI Director by the man who told me to fire the FBI Director! Witch Hunt

Retweets
17,911

Likes
50,048

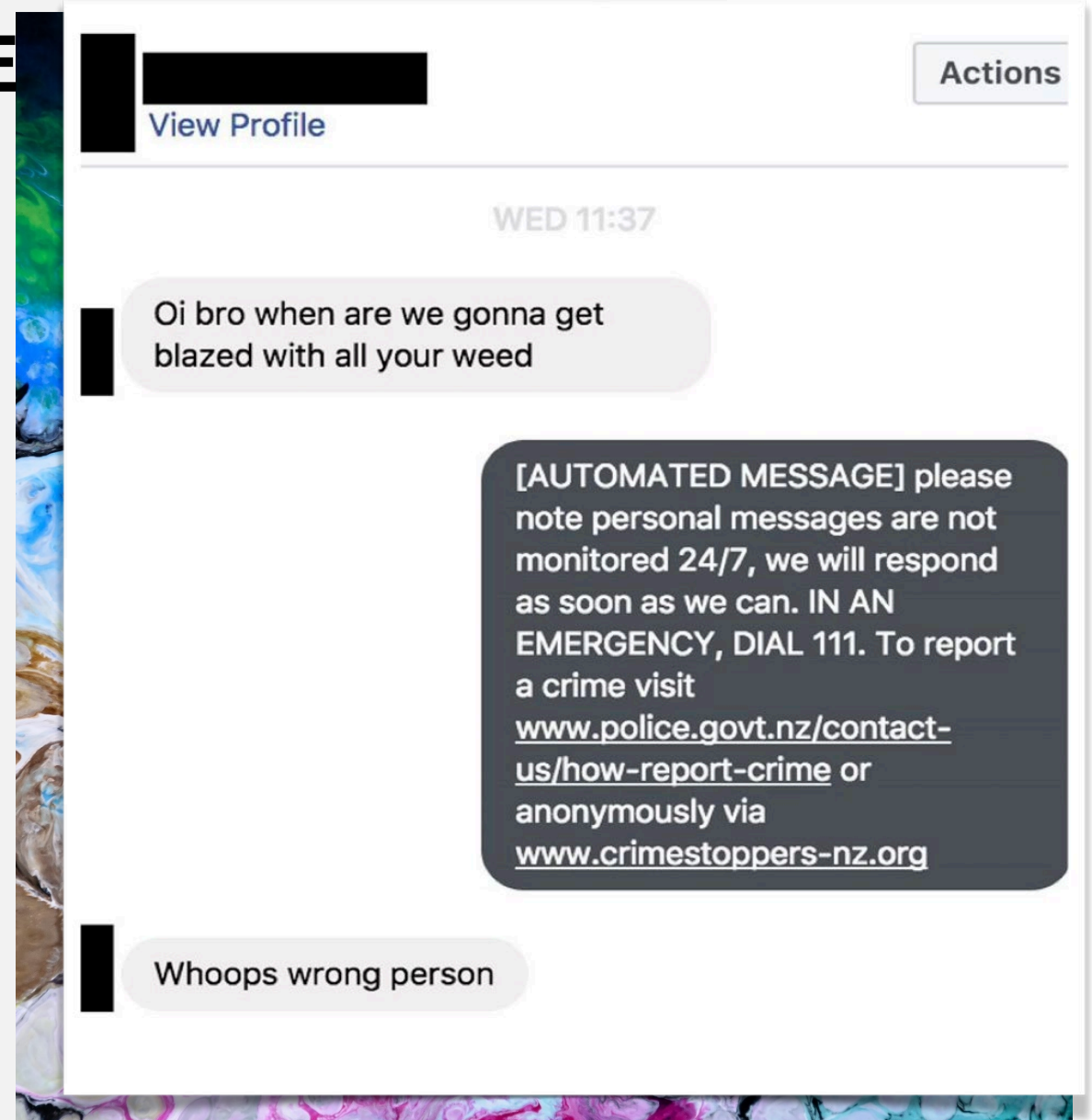


9:07 AM - 16 Jun 2017

7

WHAT WE ARE STARTING TO SEE

- Facebook and Twitter direct message information
- GPS tracking information from social media sites
- IP address information
- Length of time spent on service
- What a user looks at (regardless of likes, shares, etc.)



FROM GPS DATA TO PRIVATE MESSAGES

Where do people expect privacy on social media apps?

- *We increasingly see discovery that is not accessible to the general public on social media.*
- *The predominant law governing those subpoenas and warrants is the Stored Communications Act of 1986.*
- *The SCA was originally intended for ISP's and the information they stored*



STORED COMMUNICATIONS ACT

18 U.S.C. § 2701, *et seq.*

- If the items sought are less than 180 days old, there must be a warrant.
- If the information sought is more than 180 days old, there need only be an administrative subpoena to satisfy the statute (more on this later).
- The standard for the subpoena requires relevancy of the evidence but arguably does not require probable cause.
- Those subpoenas are required to give the service time to object to the production of any information. Many services do object - perhaps most famously by Twitter in *People v. Harris*, 949 N.Y.S.2d 590 (C.C.N.Y. 2012)
- One exception is for basic description of who owns an account or account information. That requires no warrant or subpoena.

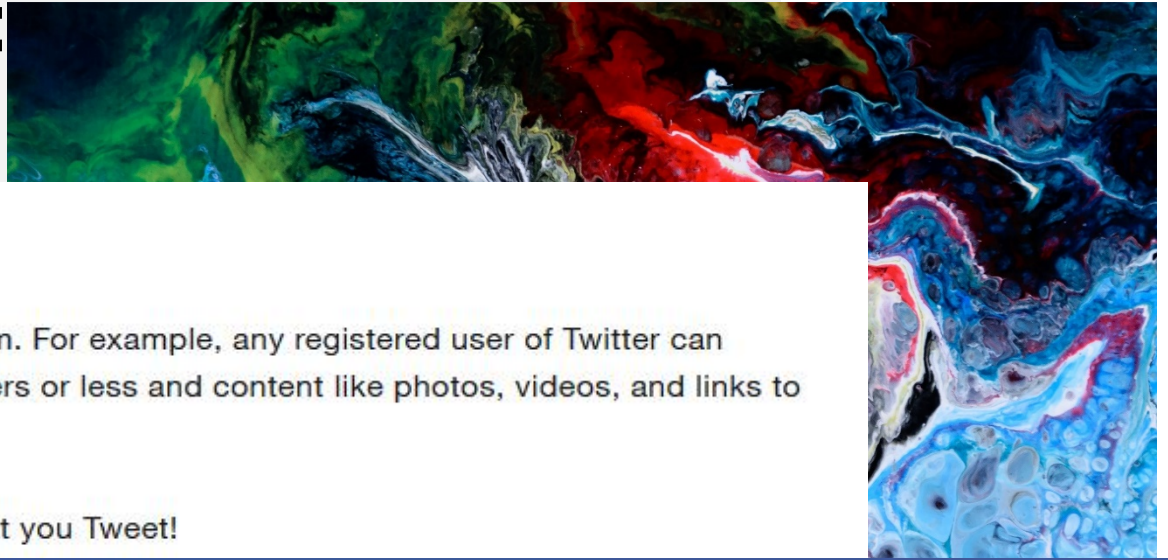


PEOPLE V. HARRIS

- Harris was an Occupy Wall Street protestor
- Charged with disorderly conduct for the Brooklyn Bridge protest
- The DA subpoenaed Twitter seeking all user information
- The DA did not notify Harris and admonished Twitter not to, either
- Twitter moved to quash and notified Harris
- The ACLU and a number of other parties filed *amicus* briefs
- These briefs are goldmines for our motions



ANOTHER FAVORITE GOV'T ARG: PRIVACY POLICIES



Twitter Privacy Policy

Our Services instantly connect people everywhere to what's most meaningful to them. For example, any registered user of Twitter can send a Tweet, which is public by default, and can include a message of 140 characters or less and content like photos, videos, and links to other websites.

What you share on Twitter may be viewed all around the world instantly. You are what you Tweet!

This Privacy Policy describes how and when we collect, use, and share your information. It covers our use of cookies, notifications, applications, buttons, embeds, ads, and [our other covered services](#) from our partners and other third parties. For example, you send us information when you use our services on a mobile device, such as an application such as Twitter for Mac, Twitter for Android, or TweetDeck.

Last Updated: January 28, 2013

Privacy 101

What we think about when we think about privacy

Foursquare deals with location and social information, and we're thrilled to have so many passionate users both trust us and find the Foursquare app useful enough to open it up every day.

However, we know an important concern for most anyone using location-based services is privacy. We want everyone to feel comfortable that their trust has been well placed, which is why we've written this description of our privacy ethos - the guiding principles that inform how we develop Foursquare and the decisions we make. Our full Privacy Policy is available [here](#) and our Privacy FAQs are available [here](#).

Foursquare is meant to help you make the most of where you are, and, as such, we attempt to craft our product so that your digital privacy mirrors what real-world privacy is like. Here are some examples of what that means:

- When you check in at a location, it's like telling a friend where you are. Your check ins are ONLY shared with others when you proactively decide to "check in" to tell Foursquare you're at a particular location.
- A business owner (say, a restaurant manager) can see their top customers on Foursquare, just as they could identify the people who walk through their door most often.
- Foursquare can tell you who is at a location (we call this "Here Now"), but we make the visibility match what happens in the real world.

facebook

Search

Home Profile Account

We're working on communicating about privacy in a simpler, more interactive way. Let us know what you think by commenting here. This isn't our official privacy policy, which can be found [here](#).

Data Use Policy

Your information and how it is used

Learn about the types of information we receive, and how that information is used.

Your information on Facebook

Get to know the privacy settings that help you control your information on facebook.com.

Your information on other websites and applications

Find out about the ways your information is shared with the games, applications and websites you and your friends use off Facebook.

How advertising works



Facebook has been awarded TRUSTe's Privacy Seal. This means that our policies and practices have been reviewed by TRUSTe for compliance with their [program requirements](#). If you have questions or complaints regarding our privacy policy or practices, please contact us by mail at 1601 S. California Avenue, Palo Alto, CA 94304 or through this [help page](#). If you are not satisfied with our response you can [contact Truste](#).

More resources

Interactive Tools

Videos

Chat (Offline)

CONSTITUTIONAL CHALLENGES

- Warrants must be founded on Probable Cause
- *Argue that subpoenas must do so as well*
- *i.e.*, This IS actually an intrusion on private data that requires probable cause
- “The implications of the government’s position are profound. Anonymous internet speakers could be unmasked by an administrative, civil or trial subpoena or by any state or local disclosure regulation directed at their ISP and the Government would not have to provide any heightened justification for revealing the speaker. Considering as is undisputed here the importance of the internet as a forum for speech and association, the Court rejects the invitation to permit the rights of internet anonymity and association to be placed at such a grave risk.” *Doe v. Ashcroft*, 334 F.Supp.2d 471 (S.D.N.Y. 2004).



CONSTITUTIONAL CHALLENGES

Even if based on PC, the requests are often unconstitutionally **overbroad**

- “Where, as here, the government seeks information that is protected by the Constitution, it ‘must use a scalpel, not an axe.’” *Shelton v. Tucker* 364 U.S. 479 (1960).

First Amendment Challenges

- “Courts have recognized that government demands for information concerning expressive activities inherently burden speech and therefore implicate the First Amendment.” *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539 (1963).
- Requires an overriding, compelling gov’t interest
 - And a substantial nexus to the facts
- “If people know that the government will be monitoring their speech and creating dossiers on their past, present and future communications such that they will be held accountable for everything they say, people will be less inclined to speak or read as freely. This is especially the case with ‘causal’ spontaneous speech because individuals would likely refrain from publicly making such statements if they thought the government might obtain that information and hold it against them.”
- “Anonymous pamphleteering is not a pernicious, fraudulent practice but an honorable tradition of advocacy and dissent.” *Doe v. 2TheMart.com Inc.* 140 F.Supp.2d 1088 (W.D. Wash. 2001).



CONSTITUTIONAL CHALLENGES

GPS Data Should Be Considered More Private than Even That on a Car Tracker

- It goes inside houses and businesses and into all sorts of hidden places.
- Even when movements take place in public “the whole of a person’s progress through the world” will reveal “with breathtaking quality and quantity a highly detailed profile, not simply of where we go, but by easy inference of our associations - political, of religious, amicable and amorous, to name only a few – and the pattern of our professional and avocational pursuits.” *People v. Weaver*, 909 N.E.2d 1195, 1199-1200 (N.Y. 2009).
- “Society’s expectation has been that law enforcement agents and others would not secretly monitor and catalogue every single movement of an individual’s car for a very long period.” *Jones*, 565 U.S. at 430 (Alito, J., concurring).

*Consider the **source** - Was the source constitutionally impermissible?*



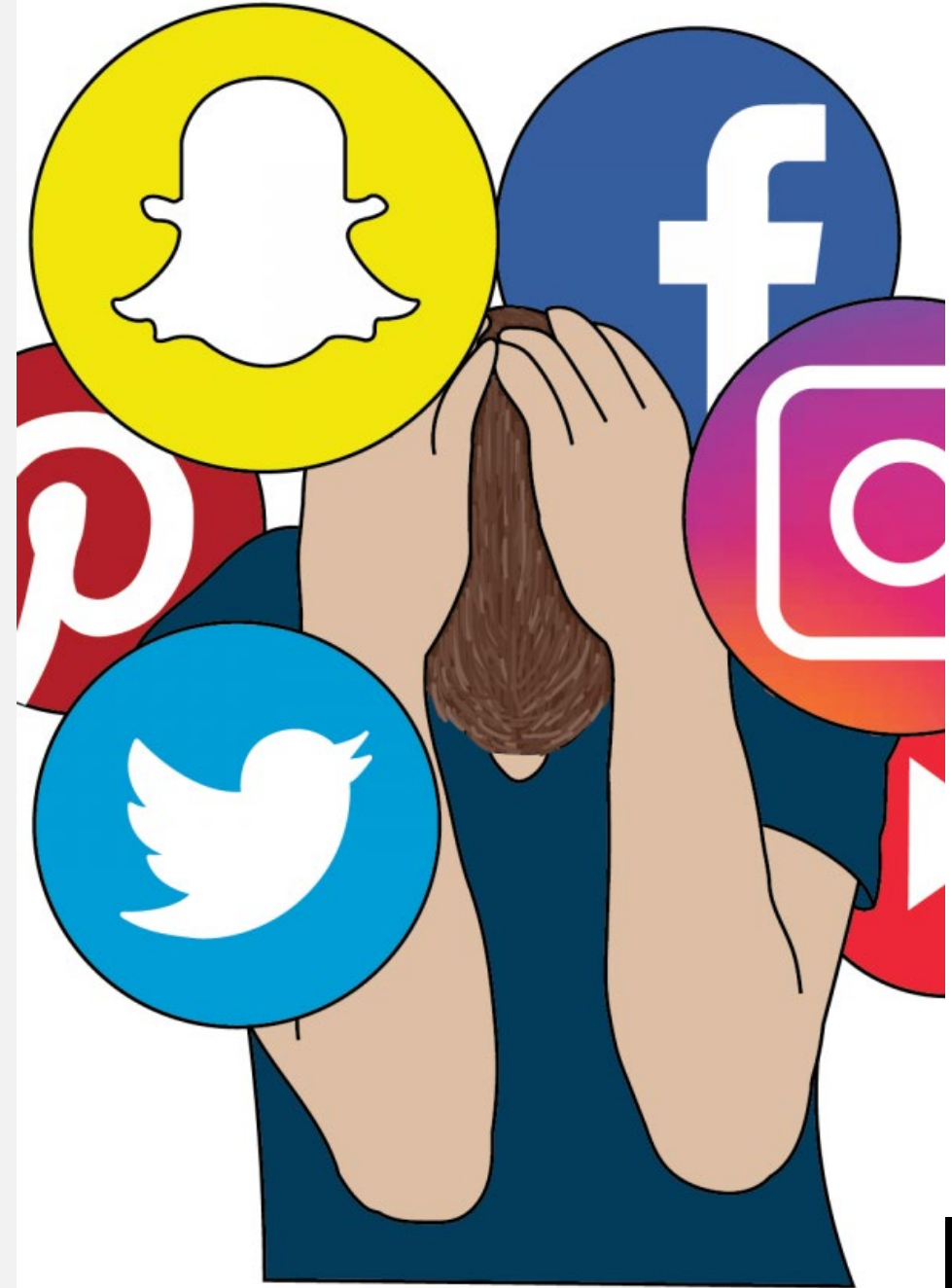
AUTHENTICATION:

A prosecutor's chief social media concern

- The predominant training for PA's and AUSA's on social media evidence spent thirty minutes of its hour on **authentication**. This is a huge concern for PA's and they are talking about it.
- File your motions *in limine* on these issues and you will find favorable resolutions, concessions, or agreements to limit evidence.
- Often the evidence they have is even cruder than having a complete profile from Facebook.
 - much better opportunity to attack gov't's ability to show **authorship** and **ownership**

But see State v. Snow, 437 S.W.3d 396, 403 (Mo. App. S.D. 2014).

- 9x circumstantial indicia sufficient to authenticate Δ 's authorship of incriminating MySpace message
- "Weaknesses in the authentication evidence (including the testimony of Defendant's girlfriend that she wrote the message because she 'wanted [Defendant] to get in trouble, because he was being looked at and I was helping create suspicion') were for the jury to consider in determining the weight the jury accorded the MySpace message."



INVESTIGATION TACTICS

FAKE FRIENDS

The Government is generally allowed to create fake profiles to monitor your client's profiles

Hoffa v. U.S., 385 U.S. 273 (1966).

U.S. v. White, 401 U.S. 745 (1971).

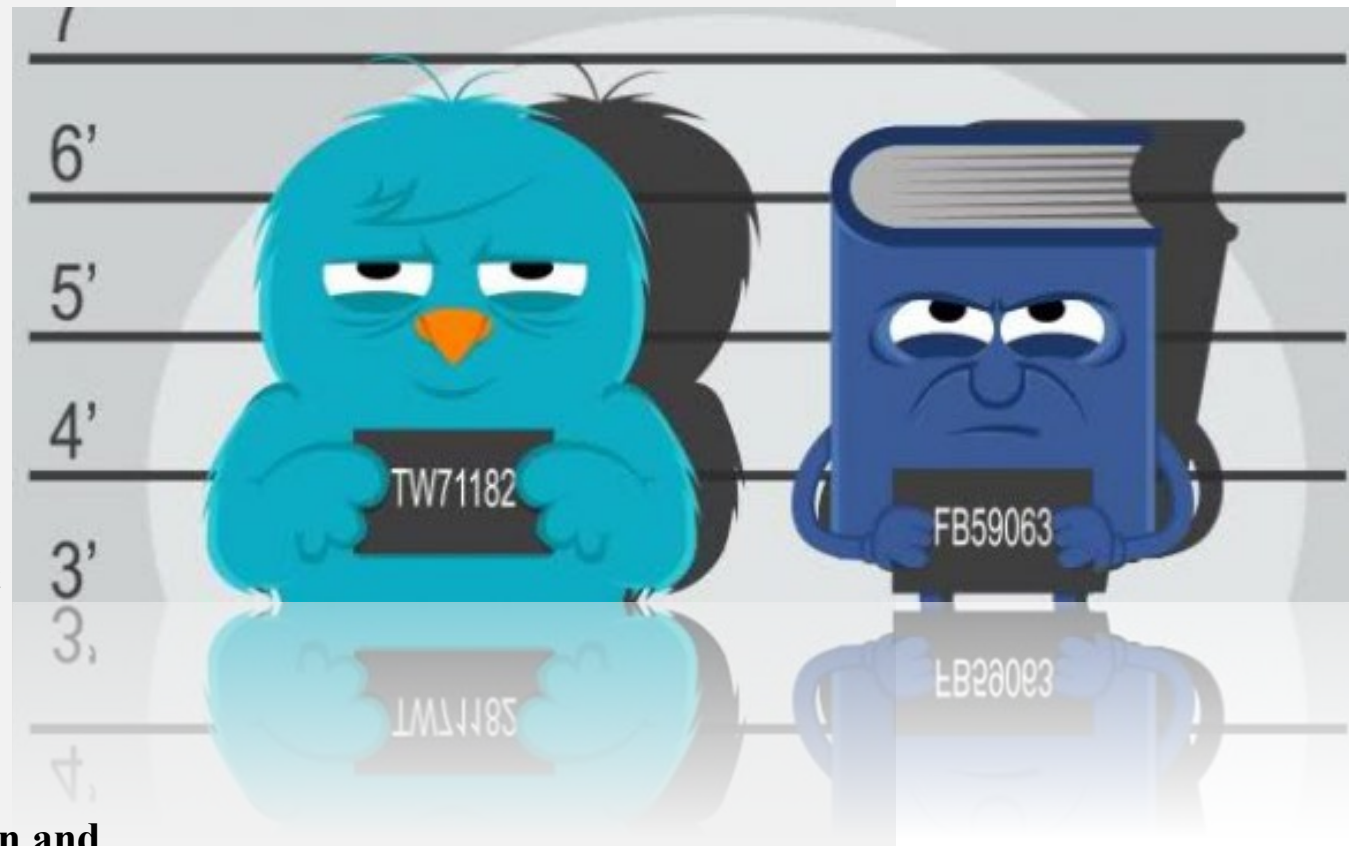
This can be attacked when your client is represented and the PA is involved

We are barred from doing the same thing with victims, which is fodder to get judges to be restrictive with evidence garnered from fake friend requests

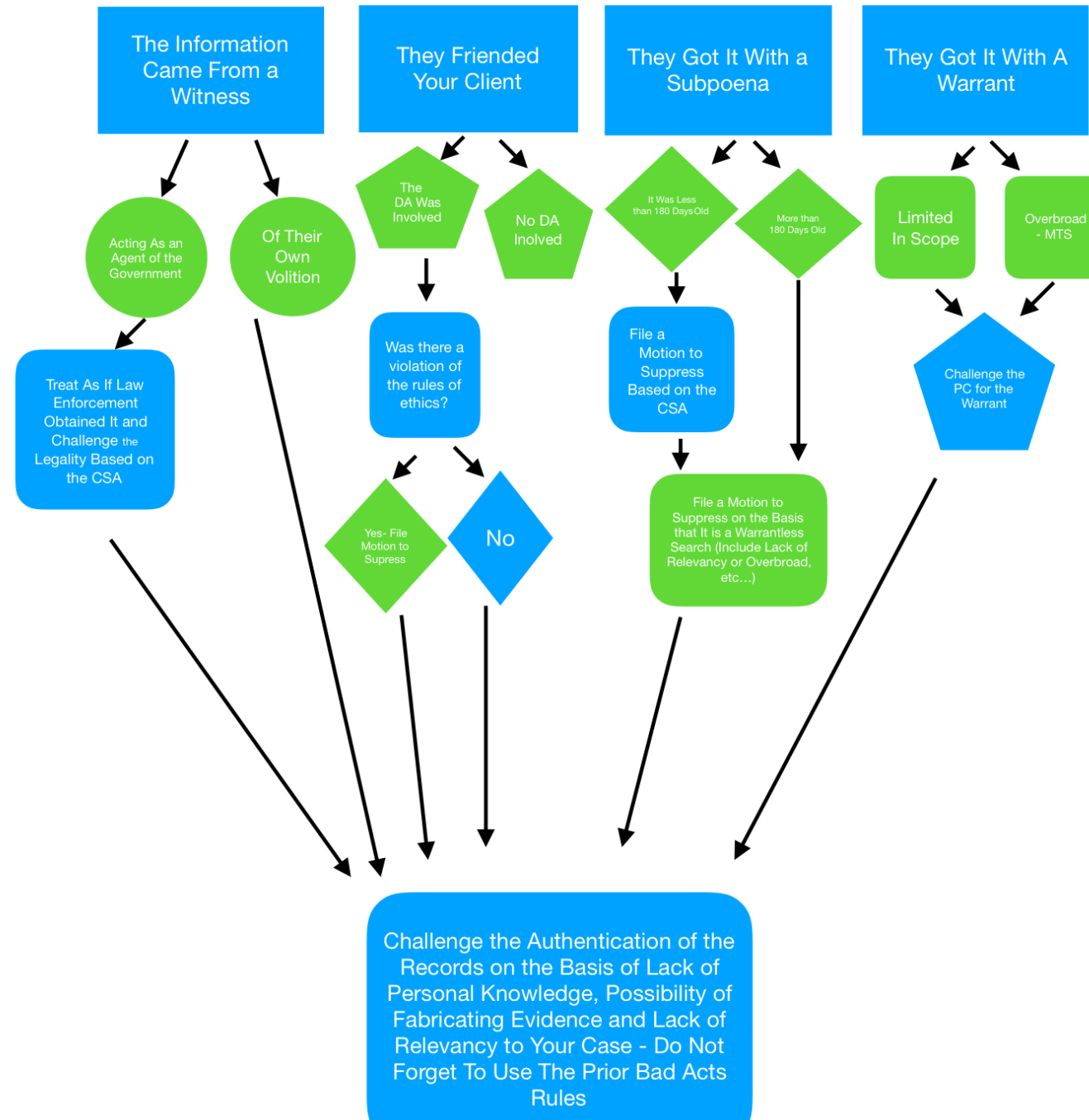


WHAT IF *YOU* NEED SOCIAL MEDIA EVIDENCE?

- File a “Motion for Early Production of Documents”
- Ask that it be set at least three weeks prior to trial
- Serve a **subpoena** on the service and give them time to object
- This frequently requires out of state service, but Social Media companies often make it easy
- If you are stymied by a Judge, ask for an *in camera* inspection and **protective order**



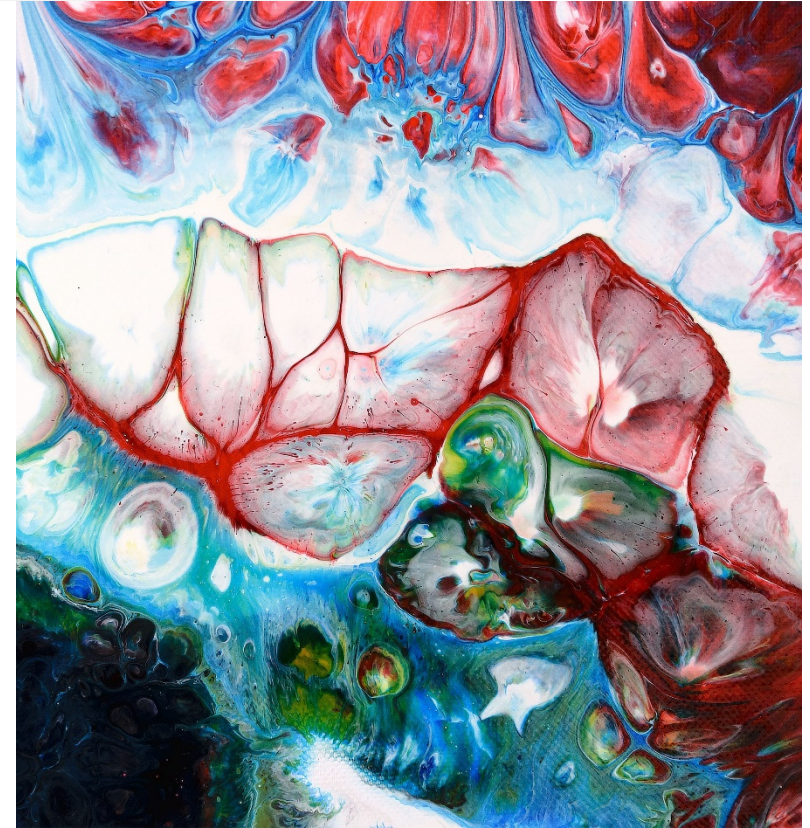
The Government Wants to Introduce Social Media Evidence Against Your Client



GEOFENCING: “REVERSE LOCATION SEARCH WARRANTS”

What is the government to do when it has no:

- suspect?
- PC to seek evidence of suspect's crimes?



GEOFENCING: “REVERSE LOCATION SEARCH WARRANTS”

What is the government to do when it has no:

- suspect?
- PC to seek evidence of suspect’s crimes?

Gather up information from an **unknown**, potentially **large number** of bystanders to ID one unknown suspect:

WHEREAS, Dan Peterson has this day on oath made an application to this Court for a warrant to search the following described premises :

Google LLC, which is headquartered at 1600 Google Amphitheatre Parkway, Mountain View, California.

located in city or township of Eden Prairie, State of Minnesota for the following described property and thing(s):

1. GPS, WiFi or Bluetooth, and/or cell tower sourced location history data generated from devices that reported a location within the geographical region bounded by the following latitudinal and longitudinal coordinates, dates, and times listed below.
2. For each location point recorded within the Initial Search Parameters, Google shall produce anonymized information specifying the corresponding unique device ID, timestamp, coordinates, display radius, and data source, if available (the “Anonymized List”).



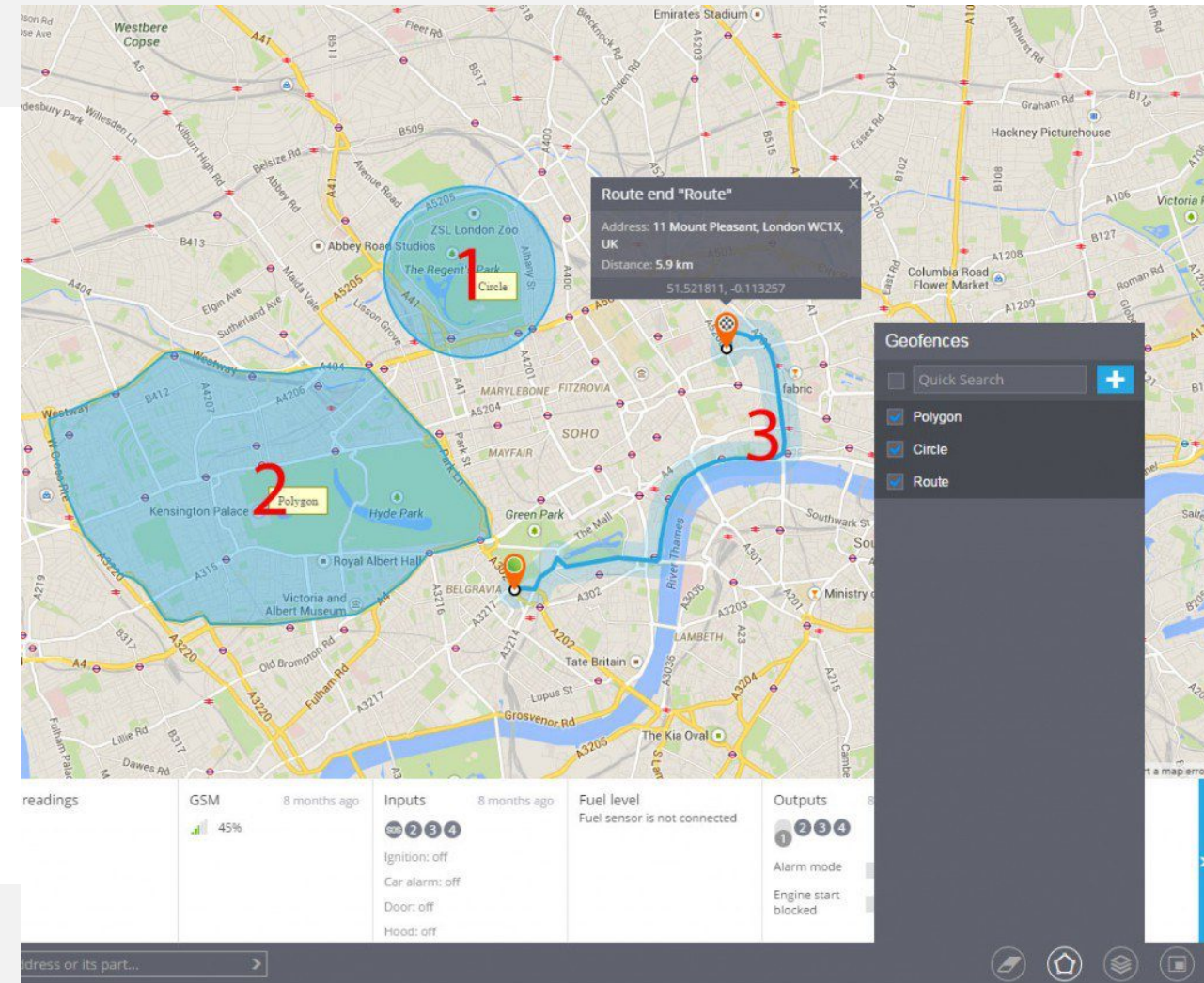
GEOFENCING: “REVERSE LOCATION SEARCH WARRANTS”

Geofence

n. virtual perimeter for a real-world geographic area

Can be:

1. Dynamically generated → radius around a point location
2. Predefined boundaries → neighborhood, school zone, residential lot
3. Linear route



GEOFENCING: “REVERSE LOCATION SEARCH WARRANTS”

- CSLI → cell tower → provider → Google Sensorvault
- **Sensorvault** = mega server farm + gigantic aggregation of data points extending back years
 - incl. GPS data → calls/texts/apps like Maps
 - Tracks **location data** generated by **every device** accessing the network **at all times**
- Nature of breadth + depth of data retained by Sensorvault is privy only to Google employees → no way to assess/challenge the accuracy of the records sent to LE
- Chain of custody issue → Google spreadsheets to LE, but who/what inside Google selected data from server farm?
 - 3P interference? Source code?
- Ripe for **reliability + foundational** challenge → data literally locked in vault + vault keeper is sole arbiter of what info released therefrom

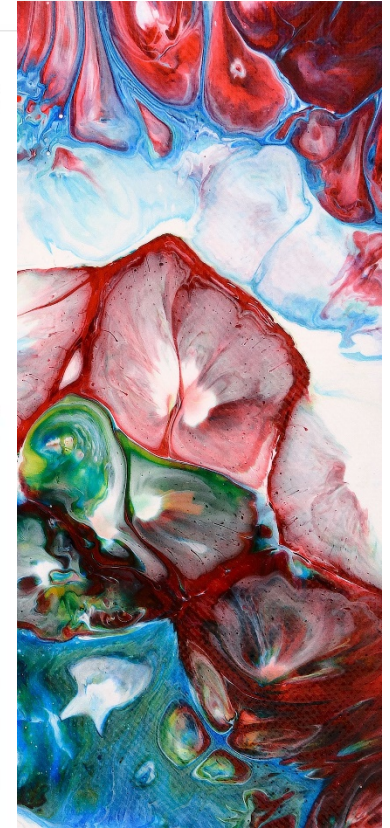
The New York Times

Google's Sensorvault Is a Boon for Law Enforcement. This Is How It Works.

Investigators have been tapping into the tech giant's enormous cache of location information in an effort to solve crimes. Here's what this database is and what it does.



By Jennifer Valentino-DeVries
April 13, 2019



GEOFENCING: “REVERSE LOCATION SEARCH WARRANTS”

Date & Time Period of Target Location #3: 10/06/2018 1200rs - 10/07/2018 2130 hrs

Geographical area identified as a polygon defined by the following latitude/longitude coordinates and connected by straight lines:

Point 1: 44°57'24.34" N 93°07'45.72" W

Point 2: 44°57'24.24" N 93°07'30.94" W

Point 3: 44°57'14.73" N 93°07'30.91" W

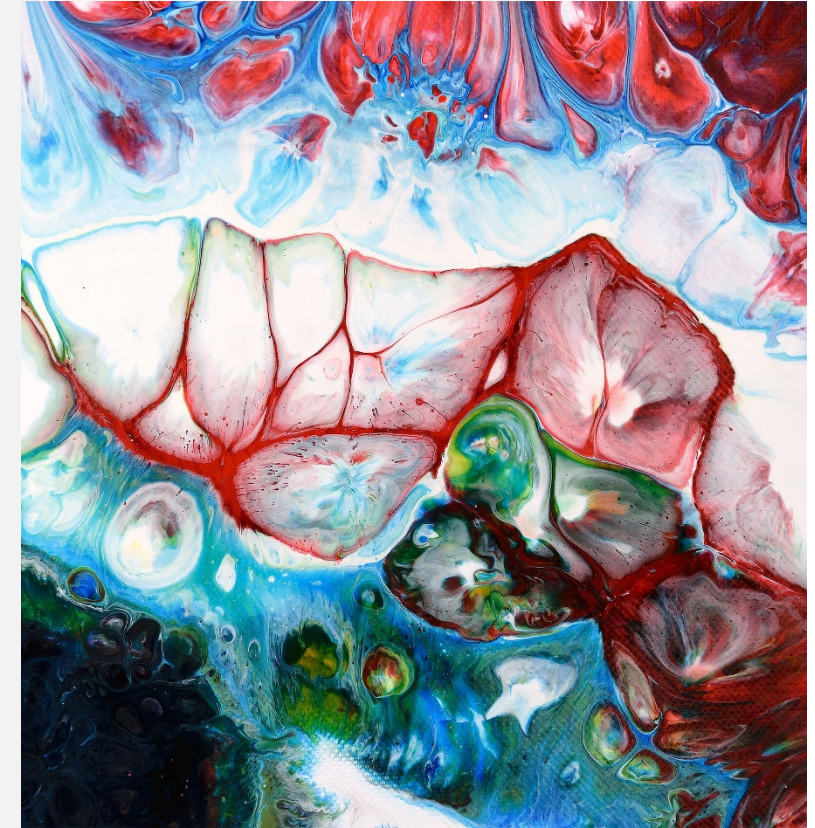
Point 4: 44°57'14.85" N 93°07'45.69" W

WHEREAS, the application of Dan Peterson was duly presented and read by the Court, and being fully advised in the premises.

NOW, THEREFORE, the Court finds that probable cause exists for the issuance of a search warrant upon the following ground(s):



GEOFENCING: “REVERSE LOCATION SEARCH WARRANTS”



GEOFENCING: “REVERSE LOCATION SEARCH WARRANTS”

Challenging geofencing:

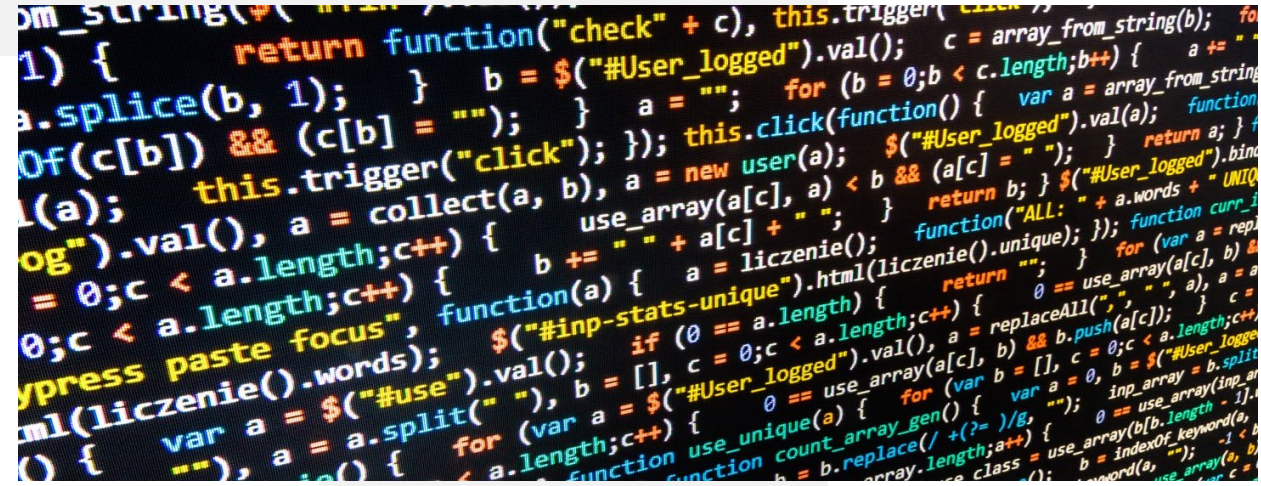
- Cell data **never precise** → 30m to 1mi variance
 - Loading/capacity of towers
 - Tower health
 - Line of sight
 - Radio signal interference
 - Make/model/condition of tower
 - Multi-pathing/terrain considerations → Rayleigh fading
 - Strength/quality of tower signals
- Maps are misleading
 - Distance b/w cell towers on map have no real bearing on tower coverage
 - Non-uniform tower service sectors → no circles/triangles
- Software is proprietary → Cell Hawk
 - Source code unavailable → not subject to scientific scrutiny



GEOFENCING: “REVERSE LOCATION SEARCH WARRANTS”

Challenging geofencing:

- 1) **Discovery** → Sensorvault spreadsheets
 - Demand the **source code**
- 2) **Expert** → analyze spreadsheets, maps, raw data
- 3) **Warrant?**
- 4) **Probable cause?**
 - Emphasize risk of dragging in completely innocent people
 - **Assumption** perp using phone at time of crime is not “fair probability”
evidence of crime will appear w/n digital polygon
- 5) **Insufficient nexus?**
 - ‘Contraband’ sought = perp’s ID; ‘place’ = crime scene
 - Parameters encompass locations **not** part of crime scene = insufficient
- 6) **Insufficient particularity/overbreadth?**
 - “items” sought = data
 - Sensorvault = firehose of *personal* records + precise location info → “broad array of private information never found in a home in any form.” (*Riley*); “retrospective quality of the data here gives police access to a category of information otherwise unknowable.” (*Carpenter*)



PEER-TO-PEER SHARING

Because sometimes downloading music just isn't enough...
eDonkey2000 network

- P2P client software → eMule + Shareaza (share protocol)
- Index servers → permit P2P client software to locate IP addresses of computers sharing files

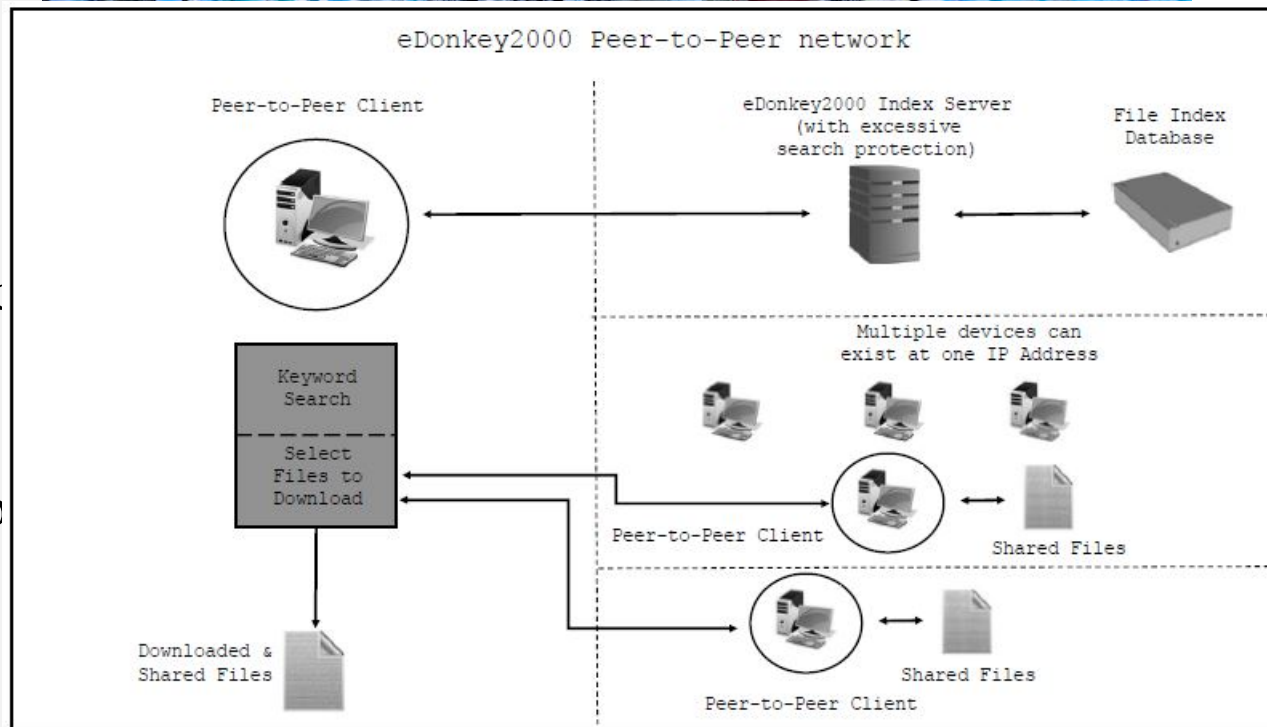
IP address → owned by ISP

- *But* the IP address's activities may be entitled to an expectation of privacy to the extent they are aggregated to obtain information otherwise available through ordinary observations. *See Jones; Carpenter*

Hash value → unique numerical ID assigned to file, group of files, folder + contents, hard drive, etc.

RoundUp eMule → centralized gov't server storing database of hash file values related to child porn

- also eDonkey2000 search results ID'ing the hash value + IP address of computers sharing child porn

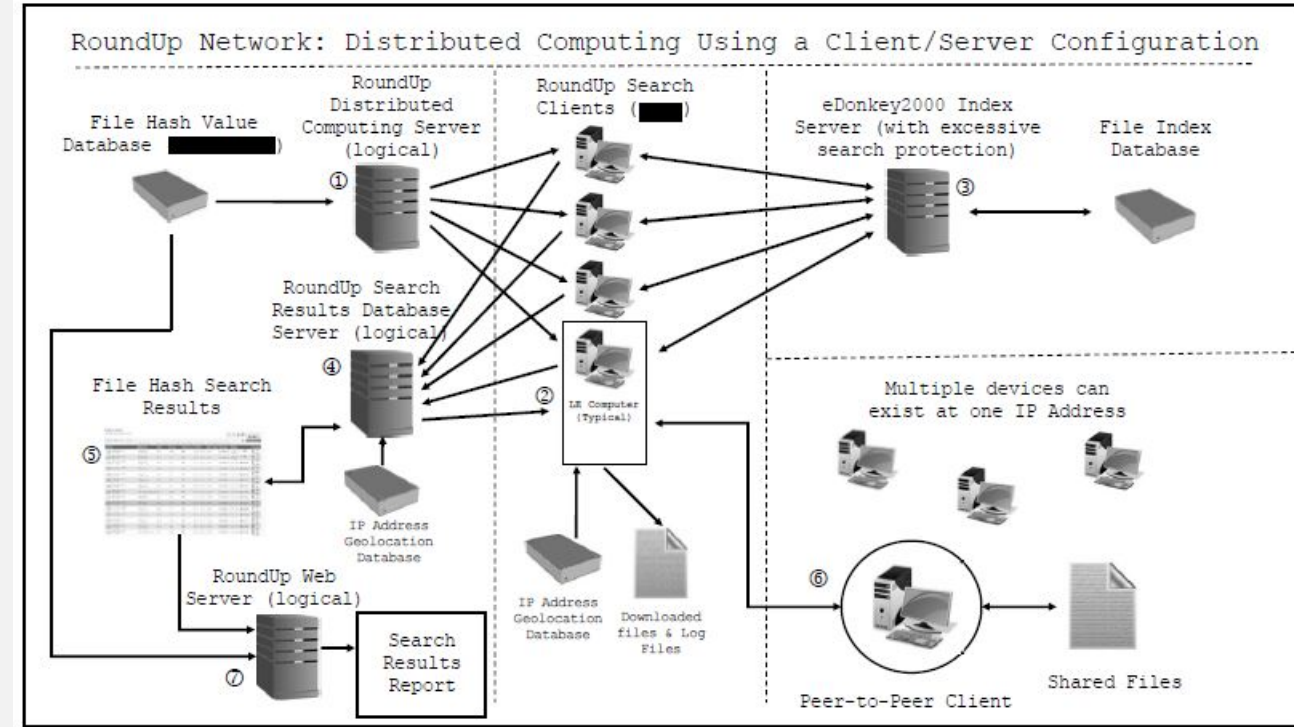


PEER-TO-PEER SHARING

RoundUp eMule + RoundUp Scheduler + RoundUp Downloader

Tracer Tagging

- “RoundUp eMule will log identifying data that may later be recovered from a confiscated computer, providing further evidence that that investigator’s system communicated with the confiscated system.”
- eMule “client that supports tagging separately logs its own user hash and public key each time it is used by an investigator. When the investigator attempts to make a case for obtaining a warrant, our modified eMule client will always offer a secure identity exchange to the suspect’s client. The remote client defaults to storing the investigator’s user hash and public key in its clients.met file. When agents seize a system, the clients.met file can be recovered. Using tools that we have developed, agents can output clients.met into a human-readable format, demonstrating that the investigator’s user hash and public key have been stored.”



PEER-TO-PEER SHARING

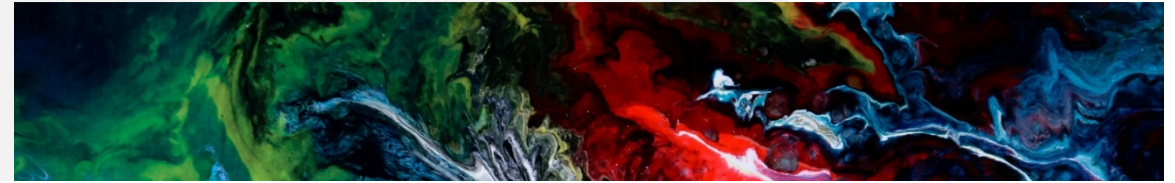
Two Big Takeaways

Hire an Expert!

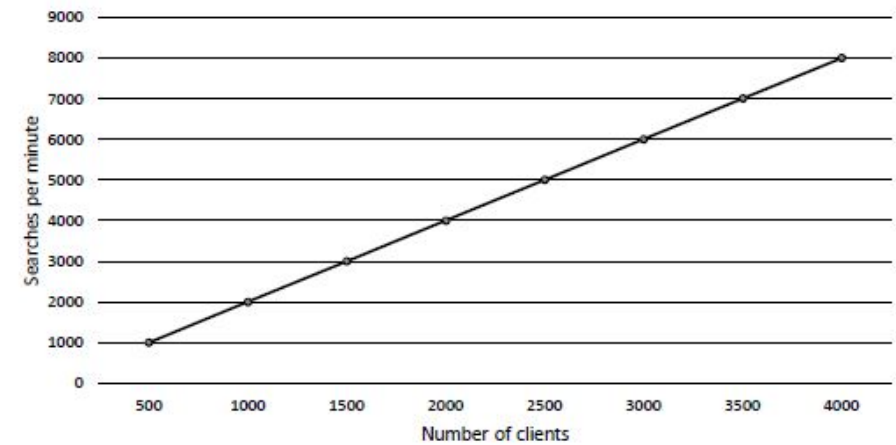
- Won't know what to ask for in discovery
- Won't understand how to consume info
- Won't know how to develop a litigation strategy
- Won't be able to effectively advocate issues

Discovery

- Source code material
- Copy of hard drive
- Validate copy of hard drive with hash value of original hard drive
- RoundUp eMule user manual + testing report



RoundUp Searches Per Minute



STINGRAY

Secretively tracking cellphones

Law enforcement agencies are using high-tech information-gathering devices to track cellphones. The government considers information about these devices to be sensitive, and not much is known publicly about how the devices are used. Though generally called stingrays, model names for these devices include KingFish, Triggerfish and Hailstorm. Here is basically how they work:

① Cellphones are constantly seeking to connect to the nearest cellphone tower, even when not being used to make a call.

Cellphone tower

Suspect

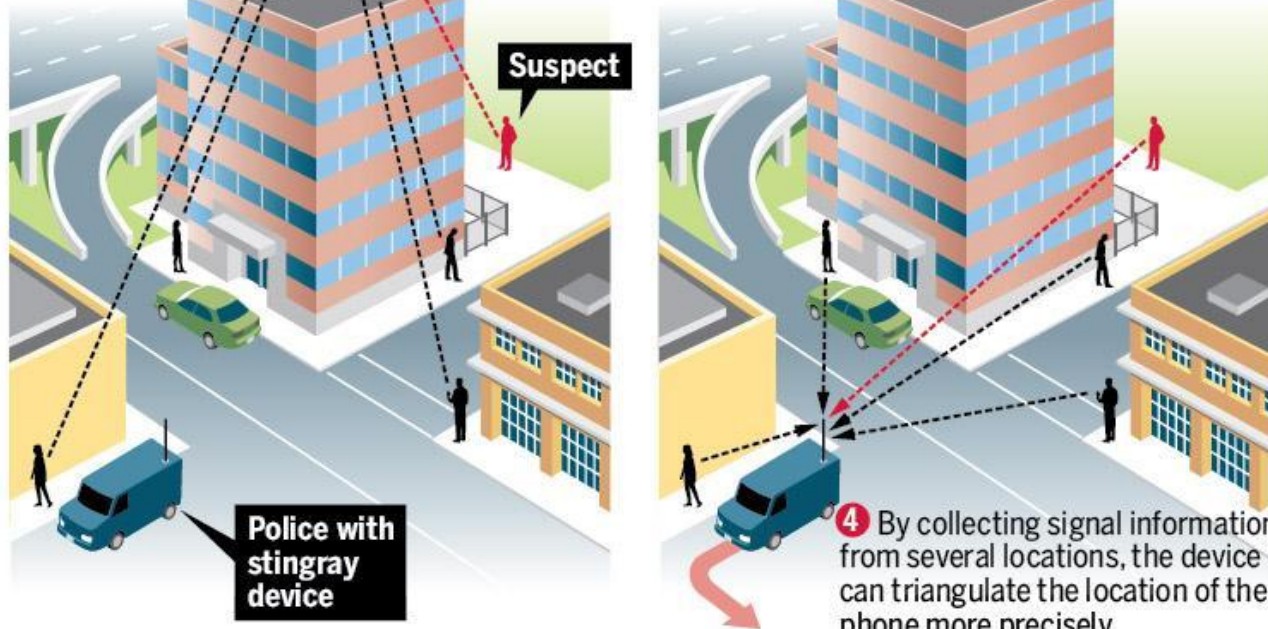
Police with stingray device

② When the stingray device is turned on, it simulates a cellphone tower, forcing cellphones in the area to register with it.

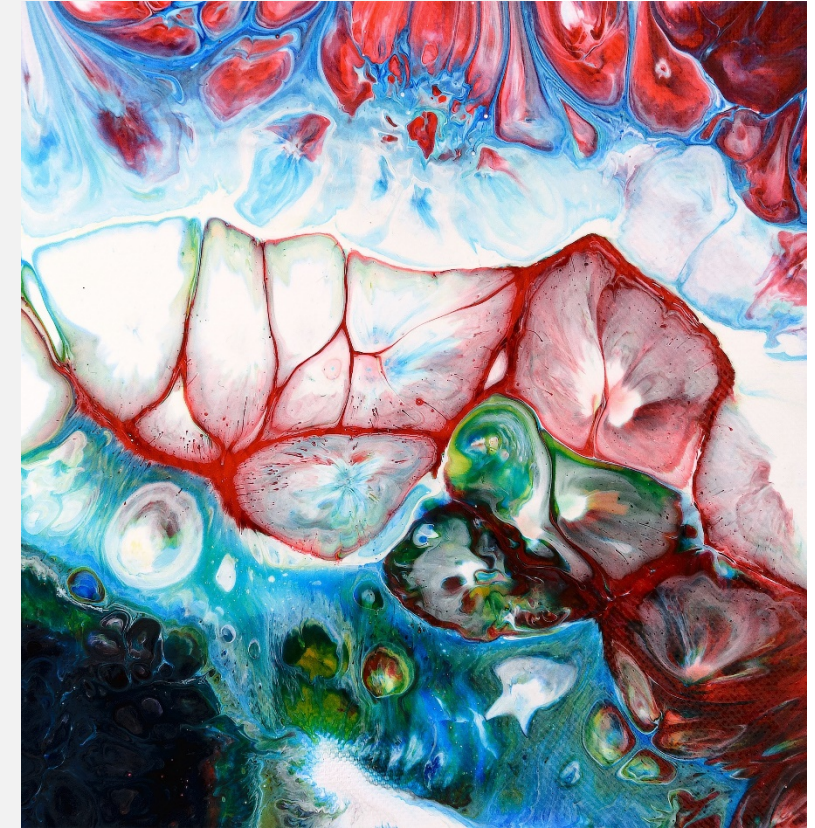
③ Once the signal from a suspect's phone is found, the device measures its strength and can provide a general location on a map.

④ By collecting signal information from several locations, the device can triangulate the location of the phone more precisely.

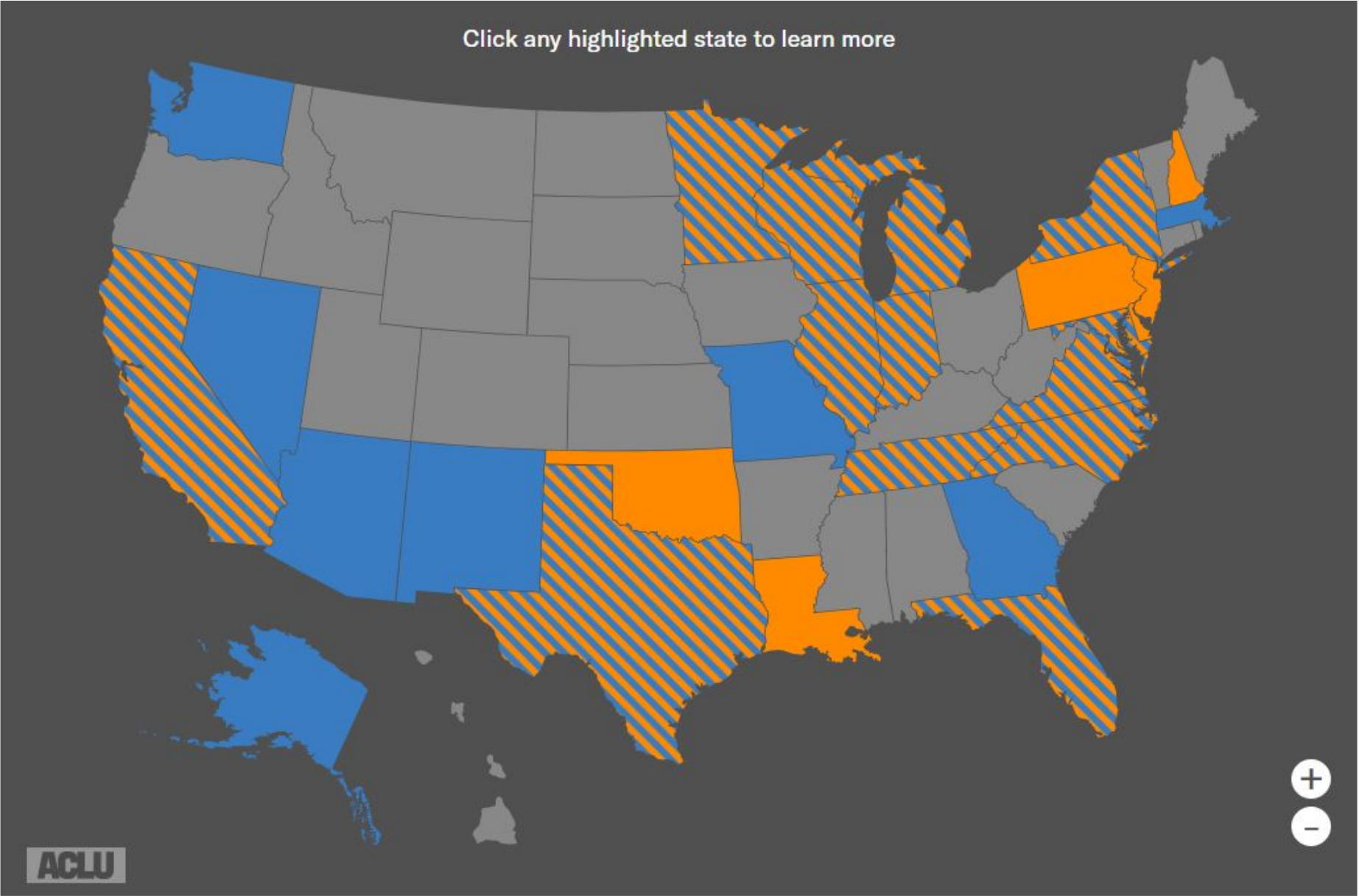
DOUG GRISWOLD/BAY AREA NEWS GROUP



Source: Washington Post, Wall Street Journal, USA Today



STINGRAY



STINGRAY

Considerations:

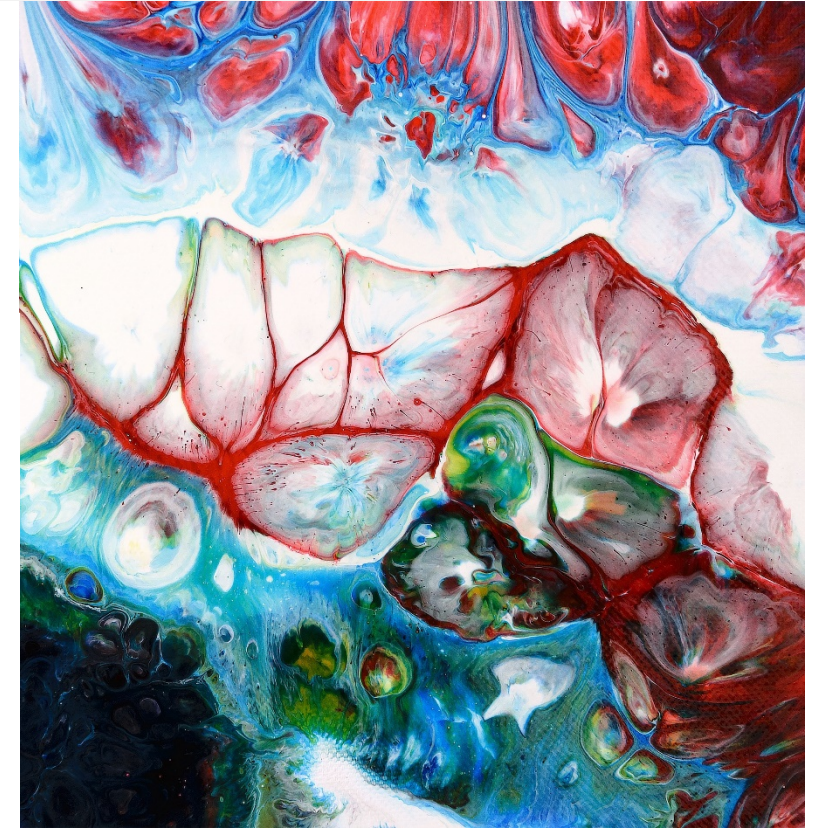
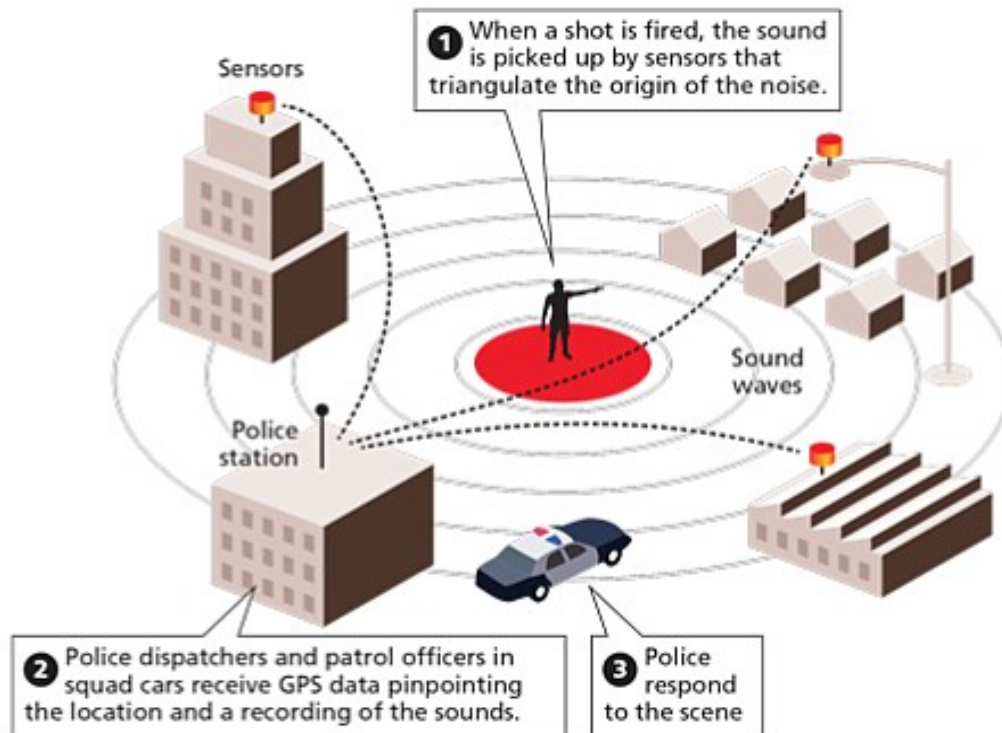
- Real-time CSLI more intrusive than historic CSLI?
- Isn't snatching texts + convos out of mid-air potentially *more* intrusive than historic CSLI?
- Limited reading of *Carpenter*'s holding
 - *Andres v. State*, 254 So.3d 283 (Fla. 2018) → refused to extend *Crawford* to suppress evidence seized from determining Δ's location with Stingray search
 - *State v. Brown*, 921 N.W.2d 804 (Neb. 2019) → "By obtaining the CSLI in this case under the Stored Communications Act and without the benefit of the U.S. Supreme Court in *Carpenter*, officers were merely following the statute as written. That is not the type of police activity the exclusionary rule seeks to deter."



SHOTSPOTTER

What they say it does:

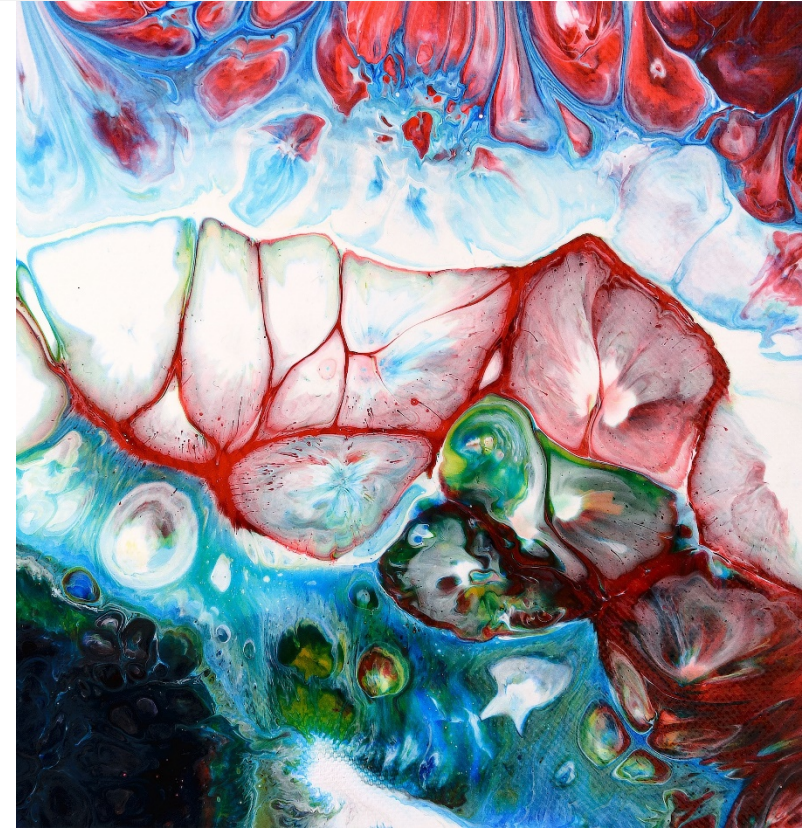
- “agnostic...gunshot detection, acoustic surveillance technology that uses sophisticated sensors to detect, locate and alert law enforcement agencies of illegal gunfire incidents in real time.”



SHOTSPOTTER

What it could be doing:

- ShotSpotter admits “three extremely rare ‘edge cases’” out of 3 million detected incidents in the last decade where sensors recorded people shouting in a public street at the location where the sensors detected gunfire
 - “brief period (a few seconds)”



VIRTUAL PERSONAL ASSISTANTS

Amazon Echo + Google Home

Does a consumer have a REP when she brings “always on” devices into her home?

A Team At Amazon Is Listening To Recordings Captured By Alexa

An Amazon spokesperson said that "an extremely small sample of Alexa voice recordings" is annotated.



Nicole Nguyen
BuzzFeed News Reporter

Posted on April 10, 2019, at 8:15 p.m. ET

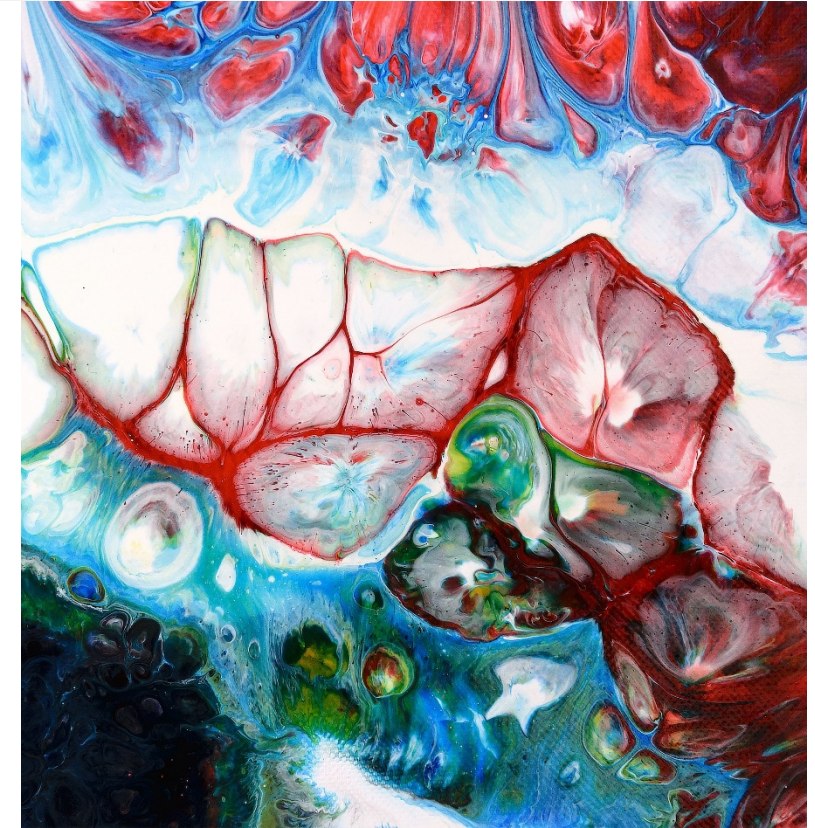


AUTOMATIC LICENSE PLATE RECOGNITION

Camera pix of plates

Recognition software creates record of plate number

Computer **automatically** compares plate number against plate database → sex offenders, crime suspects, fugitives, amber alert subjects, stolen/unregistered vehicles; also **location**



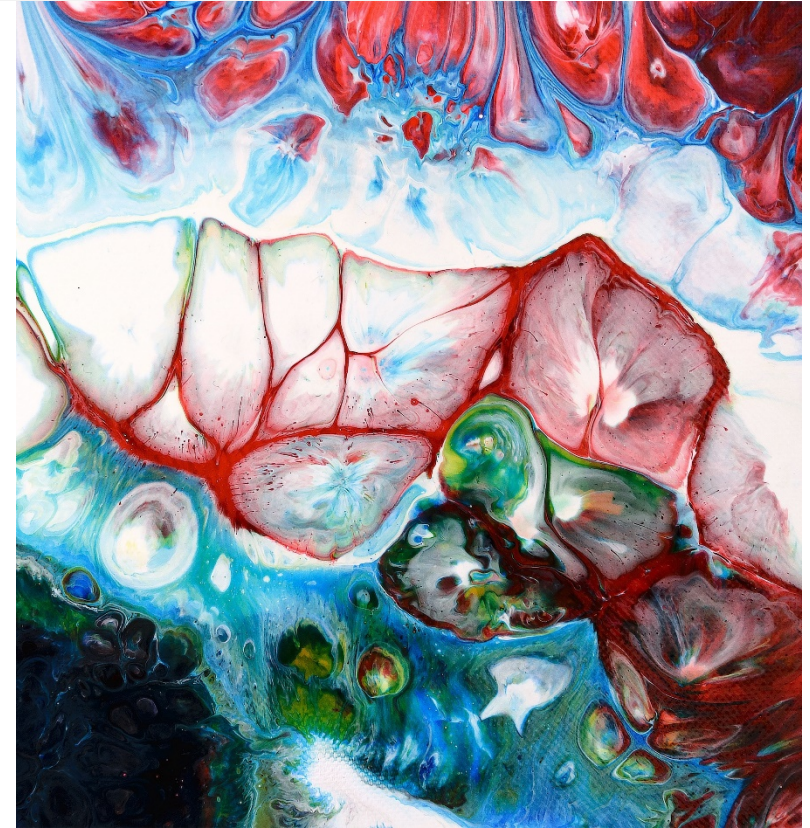
AUTOMATIC LICENSE PLATE RECOGNITION

It's already here...

“On January 26, 2013, Officer Jennifer Hendricks of the St. Louis Metropolitan Police Department was driving her patrol car when its license plate recognition (“LPR”) system gave an alert about a nearby car. The LPR system scans the license plates of cars that are within range of cameras mounted on the patrol car and can generate an alert if a scanned car is connected to a wanted person.

The alert showed Officer Hendricks that a man named Otis Hicks was associated with a nearby car and was wanted by the St. Louis County Police Department, a department that neighbors Hendricks's, for first-degree domestic assault. The alert also said that Hicks may be armed and dangerous. The LPR alert did not explain how or when Hicks was associated with the car.”

United States v. Williams, 796 F.3d 951, 955 (8th Cir. 2015).



BIOMETRIC SURVEILLANCE TECH

What is a biometric?

Characteristic: “measurable biological (anatomical + physiological) and behavioral characteristic that can be used for automated recognition”

Process: “automated methods of recognizing an individual based on measurable biological (anatomical + physiological) and behavioral characteristics”

- Fingerprints
- Retinal scans
- Iris scans
- Voice recognition
- Face recognition
- Vascular/vein recognition
- DNA
- Dynamic signature verification
- Gait analysis



BIOMETRIC SURVEILLANCE TECH

Are biometric processes a search?

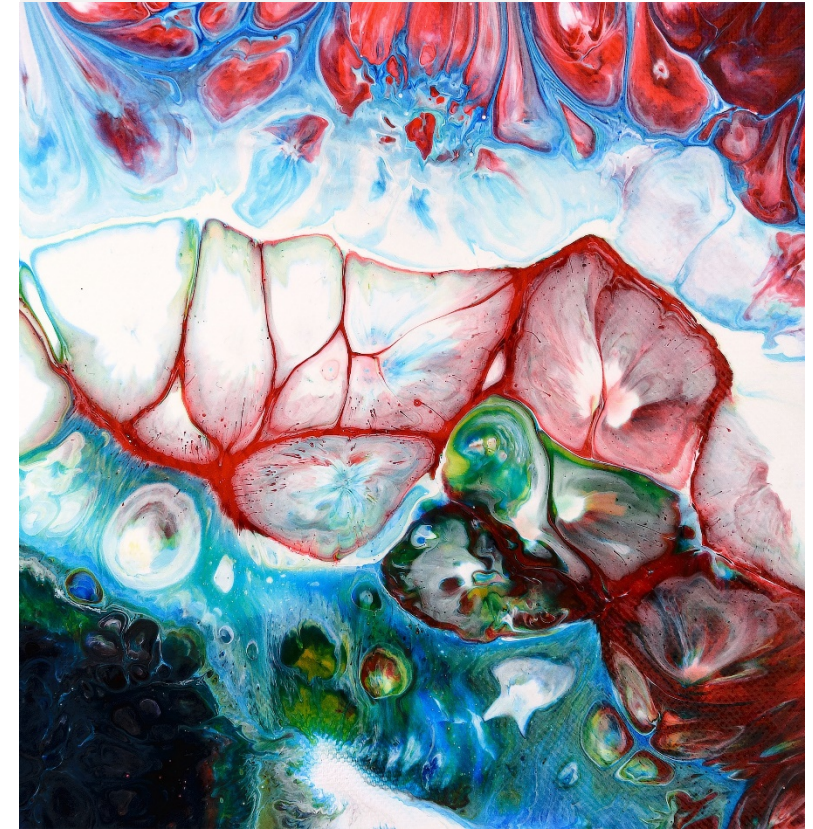
Historically → no protection for biometrics (4A or 5A)

Carpenter framework? → citizens cannot be “at the mercy of advancing technology.”

- Does using thumbprint to unlock phone create a “record”?

Matter of Residence in Oakland, Cal., 354 F.Supp.3d 2010 (N.D.Cal. 2019).

- warrant to search + seize all digital devices and compel “any individual” found at premises “to unlock the device using biometric features” was not based on PC and **overbroad**
- “biometric features serve the same purpose of a passcode, which is to secure the owner’s content, pragmatically rendering them functionally equivalent.”
- “If follows...that if a person cannot be compelled to provide a passcode because it is a testimonial communication, a person cannot be compelled to provide one’s finger, thumb, iris, face, or other biometric feature to unlock that same device.”



THANK YOU

The Founders

Profs. Orin Kerr + Adam Gershowitz

Special Thanks to Justin Rosas + Catherine Turner + Mo Hamoudi,
Attorneys at Law

Jedd C. Schneider 📞 573.777.9977 x325

Area 50 ✉ Jedd.Schneider@mspd.mo.gov

