

LITIGATING THE 4TH AMENDMENT IN THE SURVEILLANCE STATE

*MSPD Spring Training
April 25, 2019*



OBJECTIVE

Refresh understanding of Fourth Amendment law while learning about emerging police technologies and tactics and how to challenge them under extant SCOTUS jurisprudence.



An abstract, textured background featuring a mix of vibrant colors including red, yellow, green, blue, and purple, with a cracked, marbled appearance. 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, effect, **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



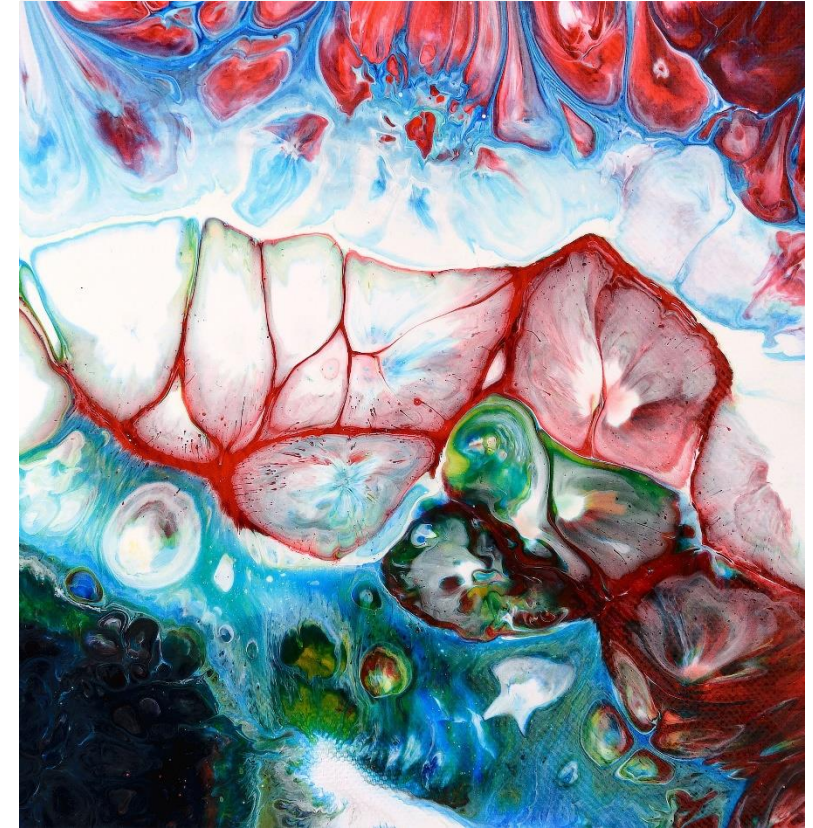
WARRANTS

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

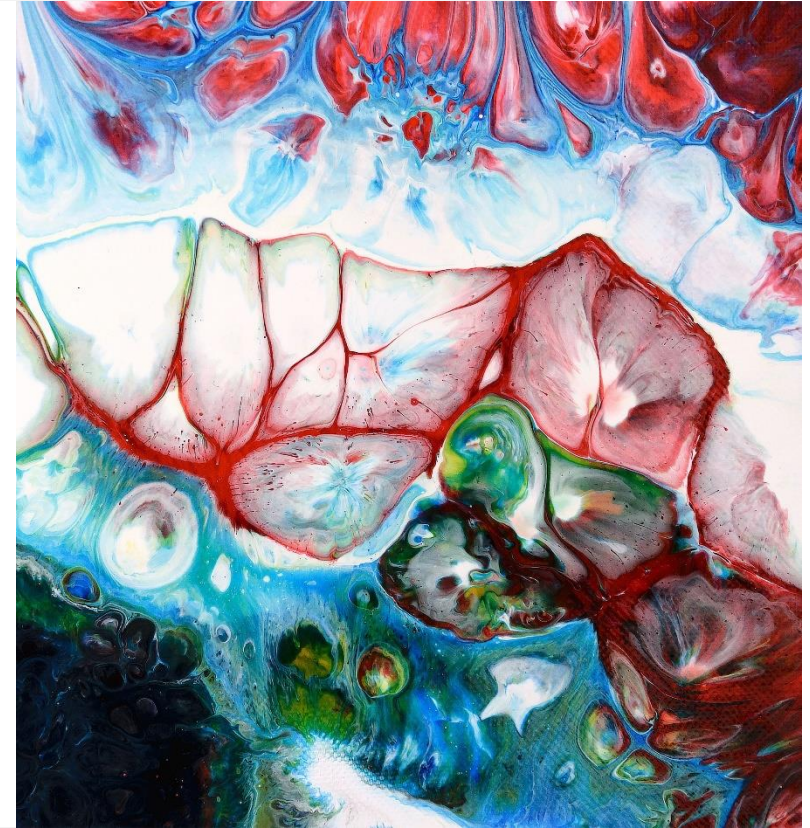
- “The fourth amendment requires that the government describe the items to be seized with as much specificity as the government’s knowledge and circumstances allow, and warrants are conclusively invalidated by their substantial failure to specify as nearly as possible the distinguishing characteristics 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).



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 as3+ necessary

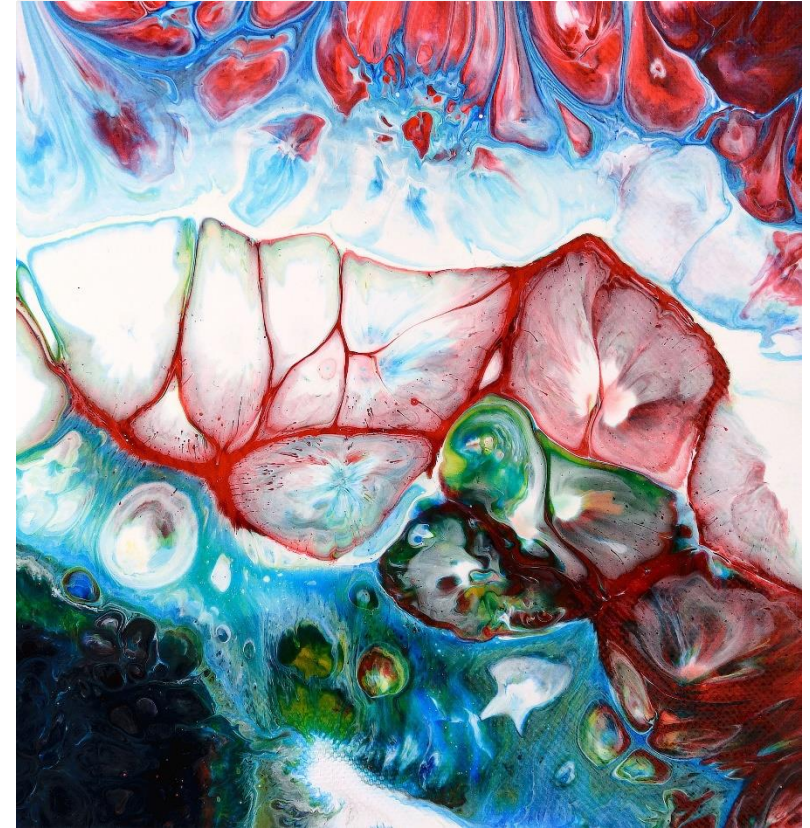
Motion for new trial → claim TC error in both: 1) overruling MTS; and 2) admitting contested evidence



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).

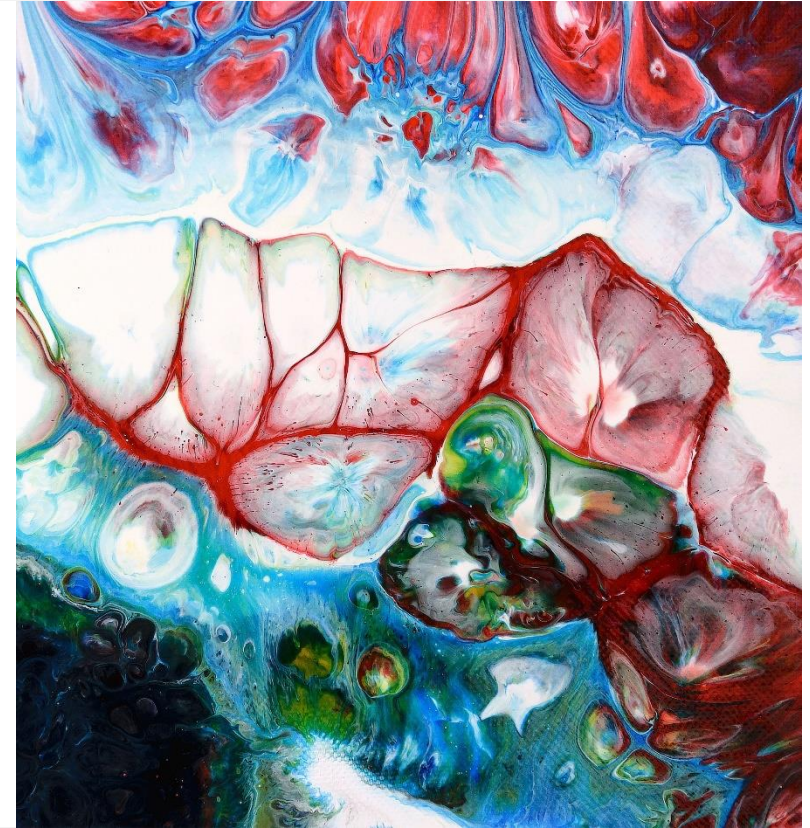
- NYC liable for violating plaintiffs' 4A + 5A rights in departmental practice of suspicionless stops + frisks of African-American + Latino suspects



OUR PROMISE

Lorem ipsum dolor
sit amet.

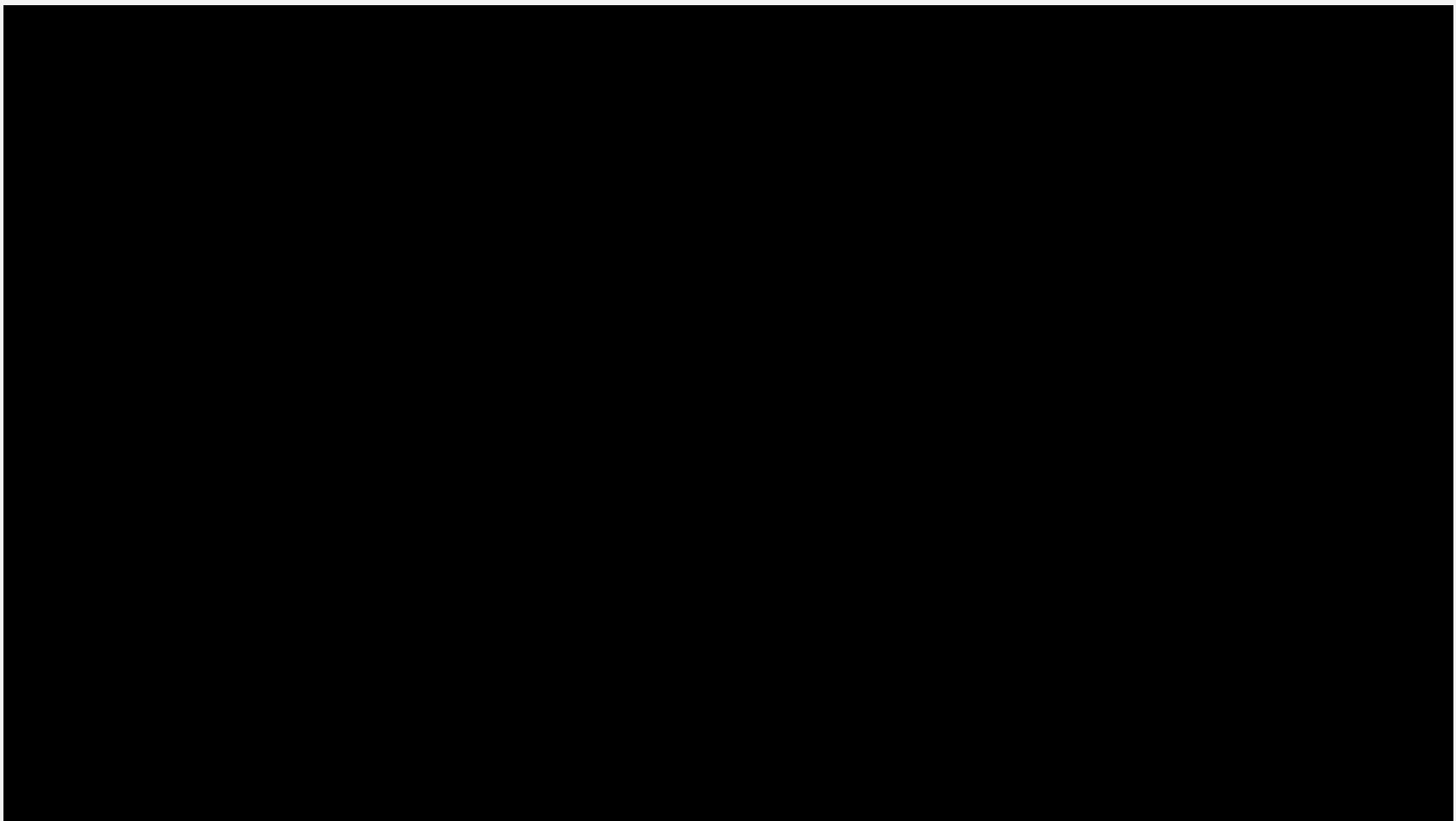
- Ut fermentum a magna ut eleifend. Integer convallis suscipit ante eu varius.
- Suspendisse sit amet ipsum finibus justo viverra blandit.
- Ut congue quis tortor eget sodales.





WARRANTLESS EXCEPTIONS

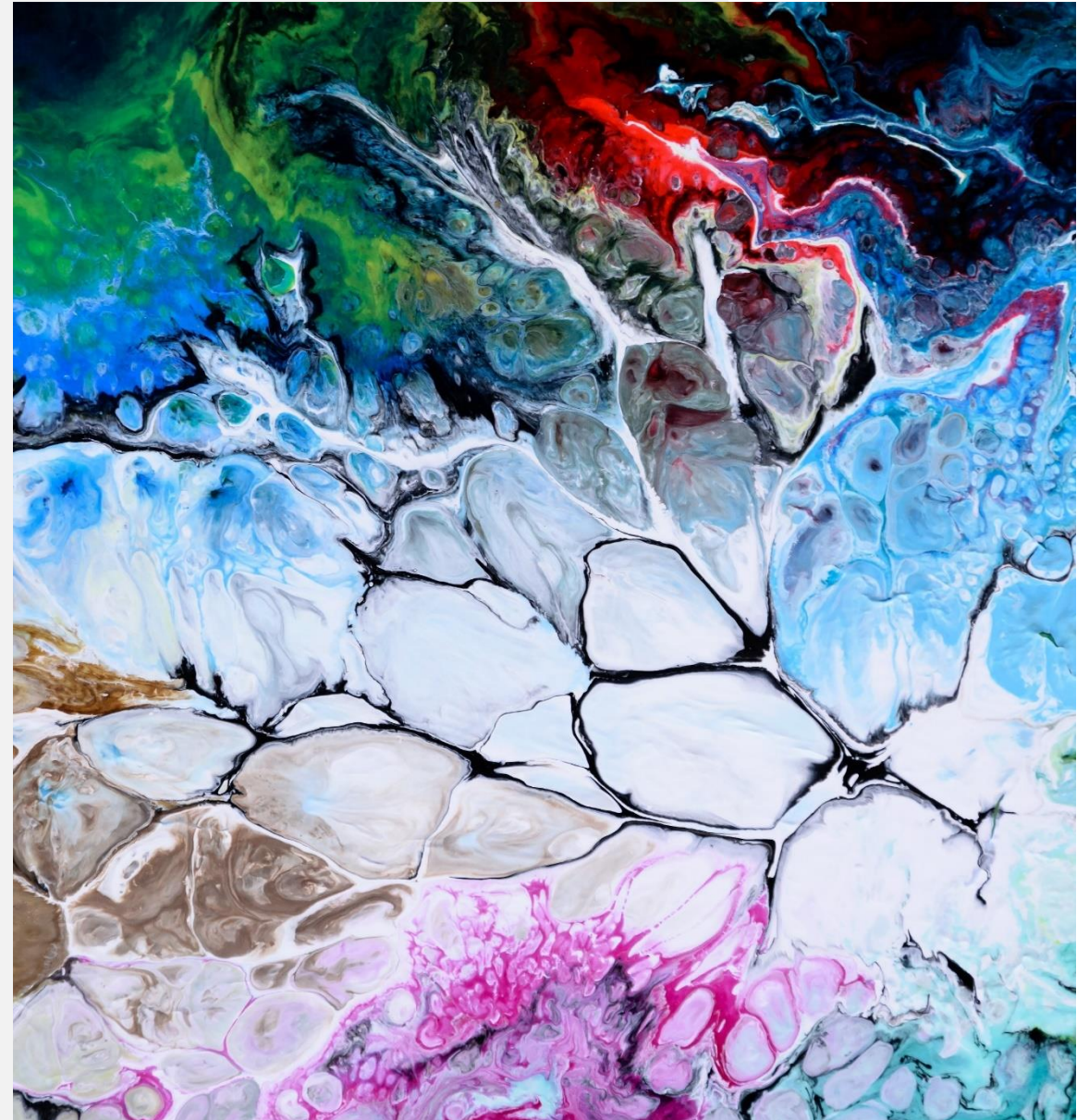
or what I like to call...



WARRANTLESS SEARCHES

Permissible when

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

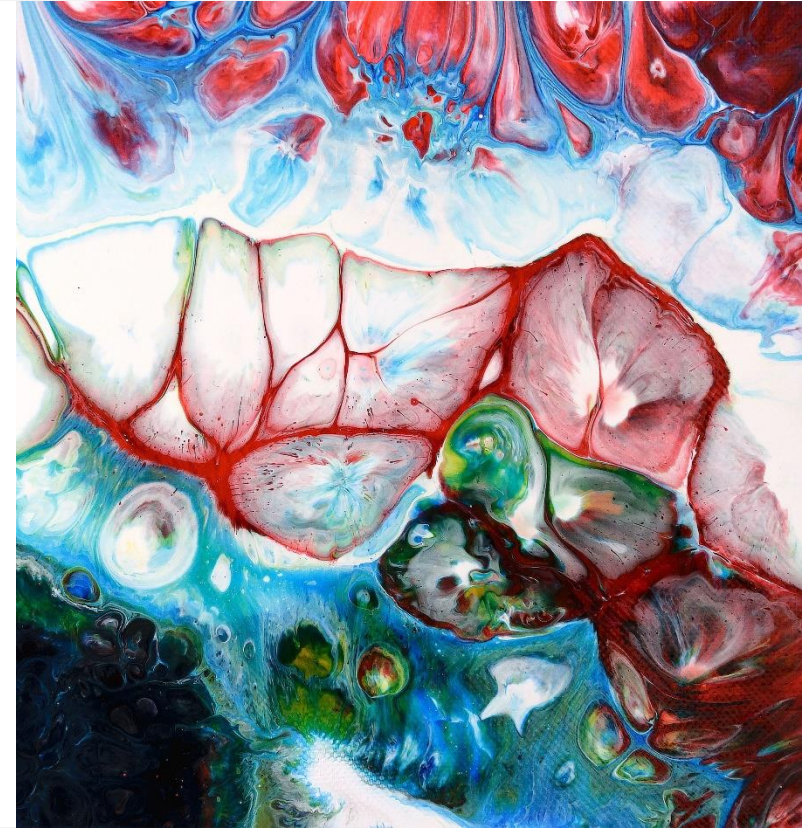


CURTILAGE

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



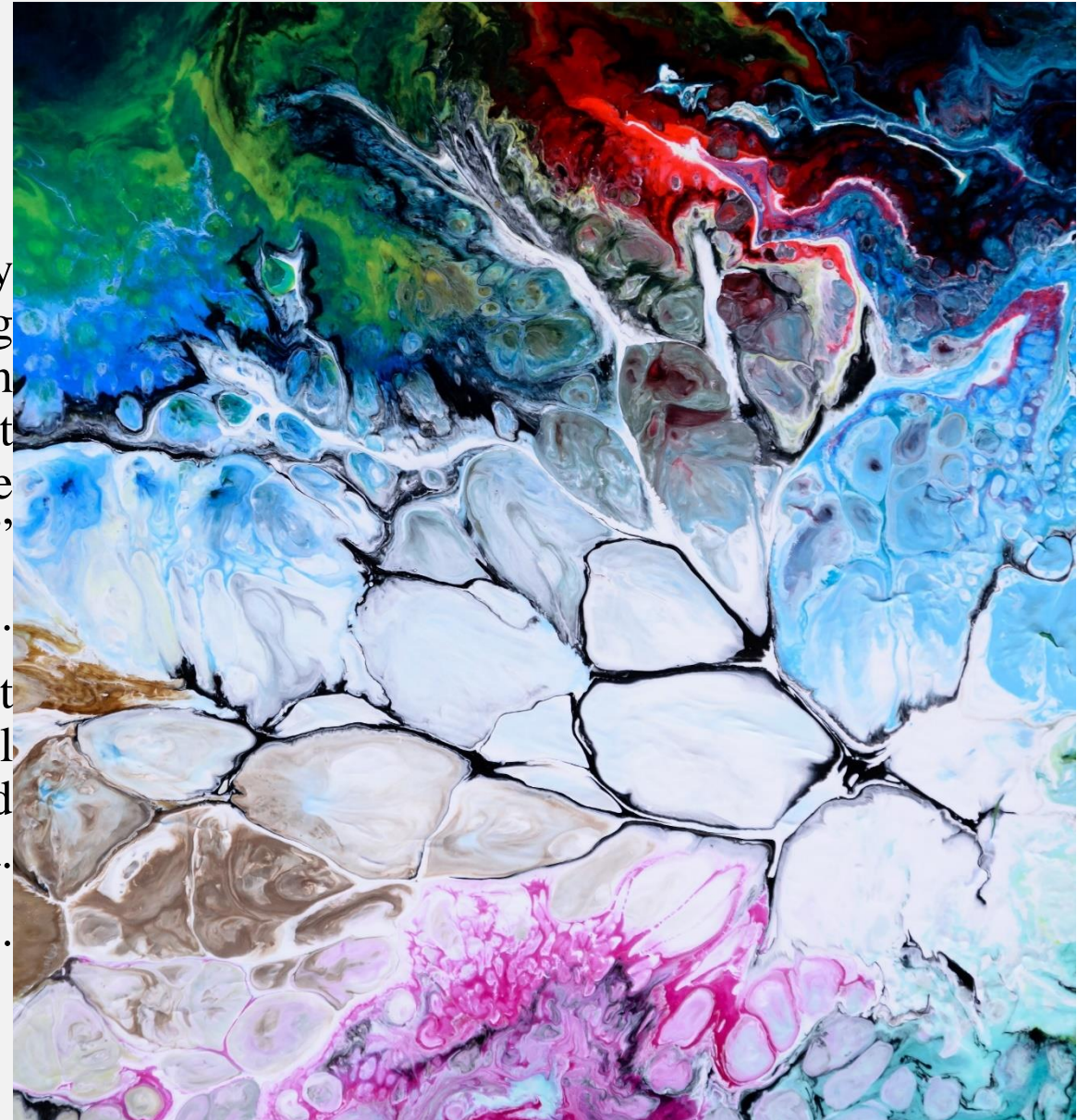
FORCIBLE BLOOD DRAW

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

A HUGE victory for our clients!

“[W]e hold that Section 577.033 does not allow warrantless blood draws of unresponsive drivers in criminal cases unless exigent circumstances are present as required by *McNeely*.”

State v. Osborn, No. WD80959, 2019 WL 1599307 (Mo. App. W.D. Apr. 16, 2019).



IMPLIED CONSENT STATUTE

A HUGE victory for our clients...for now?

“[W]e hold that Section 577.033 does not allow warrantless blood draws of unresponsive drivers in criminal cases unless exigent circumstances are present as required by *McNeely*.”

State v. Osborn, No. WD80959, 2019 WL 1599307 (Mo. App. W.D. Apr. 16, 2019).

Mitchell v. Wisconsin, No. 18-6210 (argued Apr. 23, 2019).

QP: “Whether a statute authorizing a blood draw from an unconscious motorist provides an exception to the Fourth Amendment warrant requirement.”





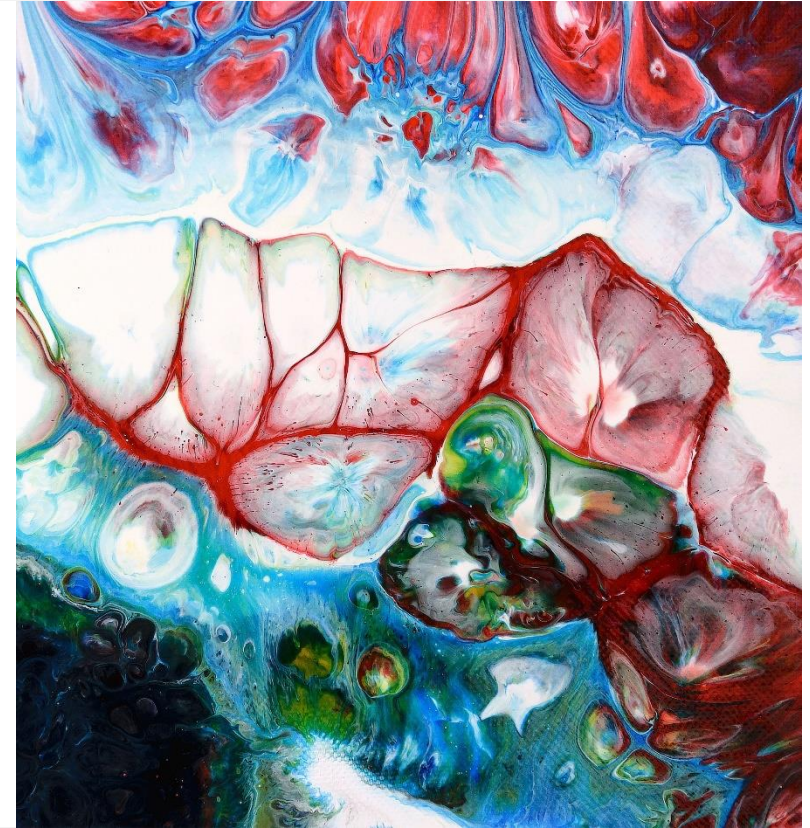
JONES, RILEY, CARPENTER, AND THE NEW “REASONABLE EXPECTATION OF PRIVACY”

*“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)

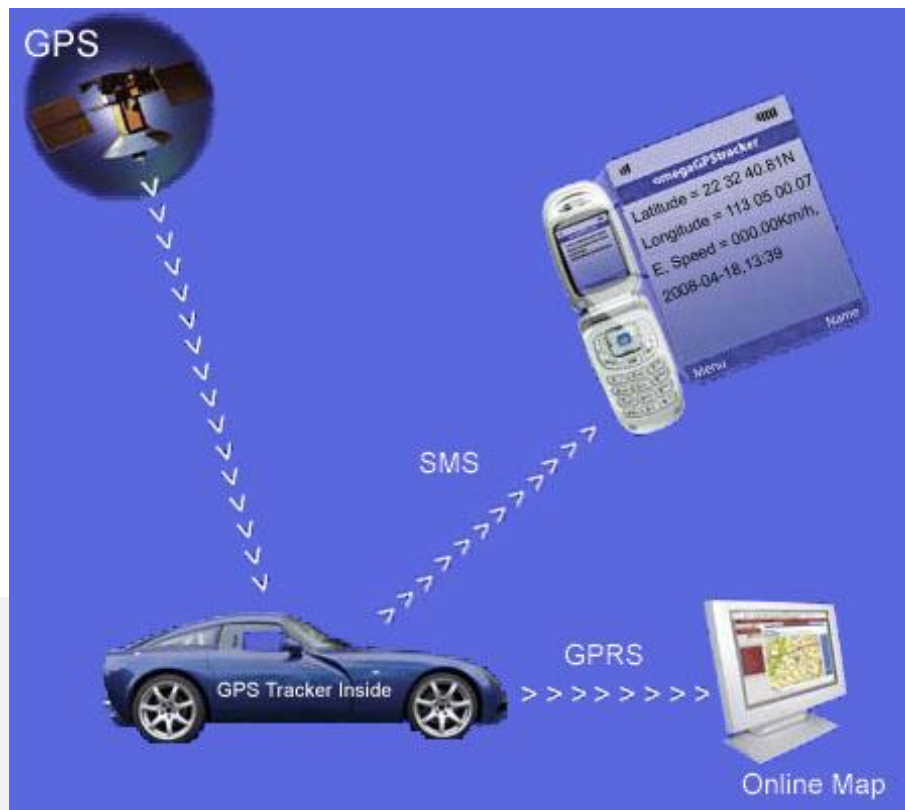


JONES

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

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

- physical government trespass on “effects”



JONES

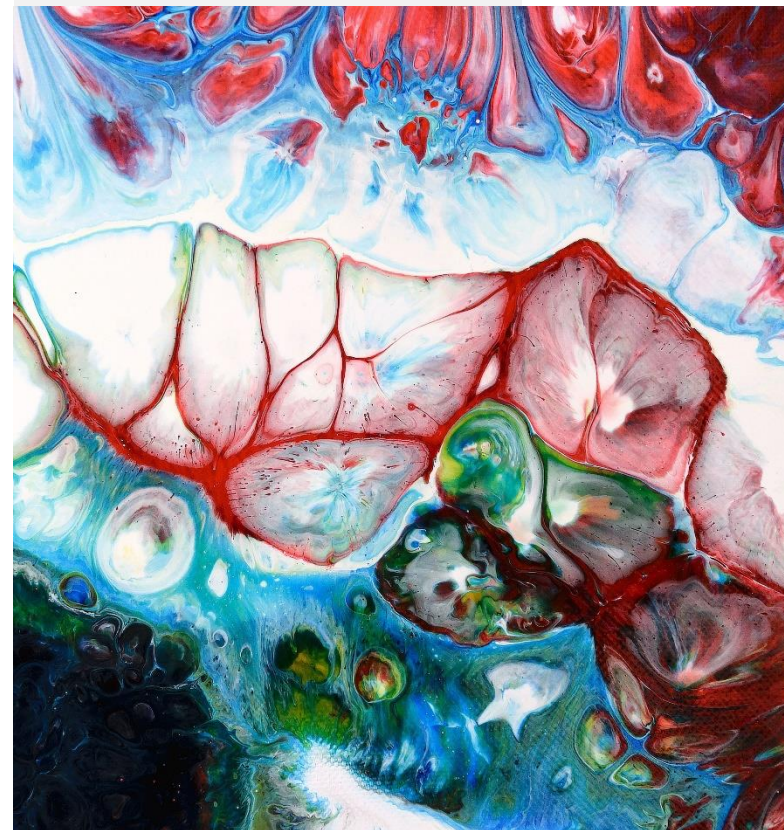
United States v. Jones, 565 U.S. 400 (2012).

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

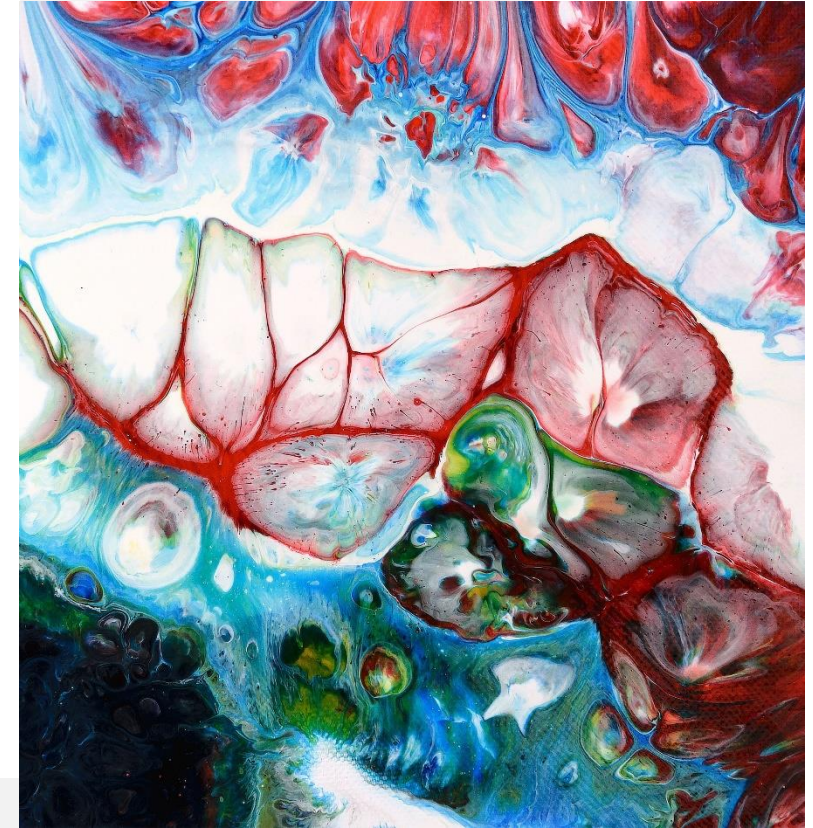


RILEY

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.”

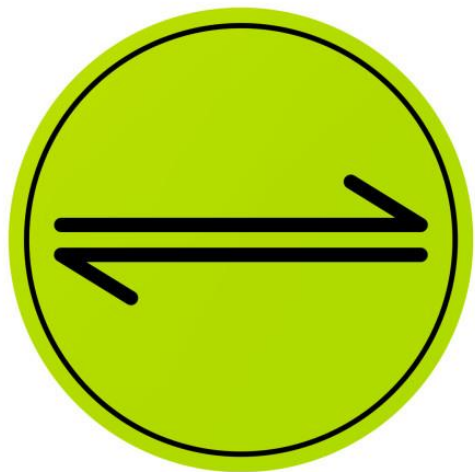


RILEY

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*

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

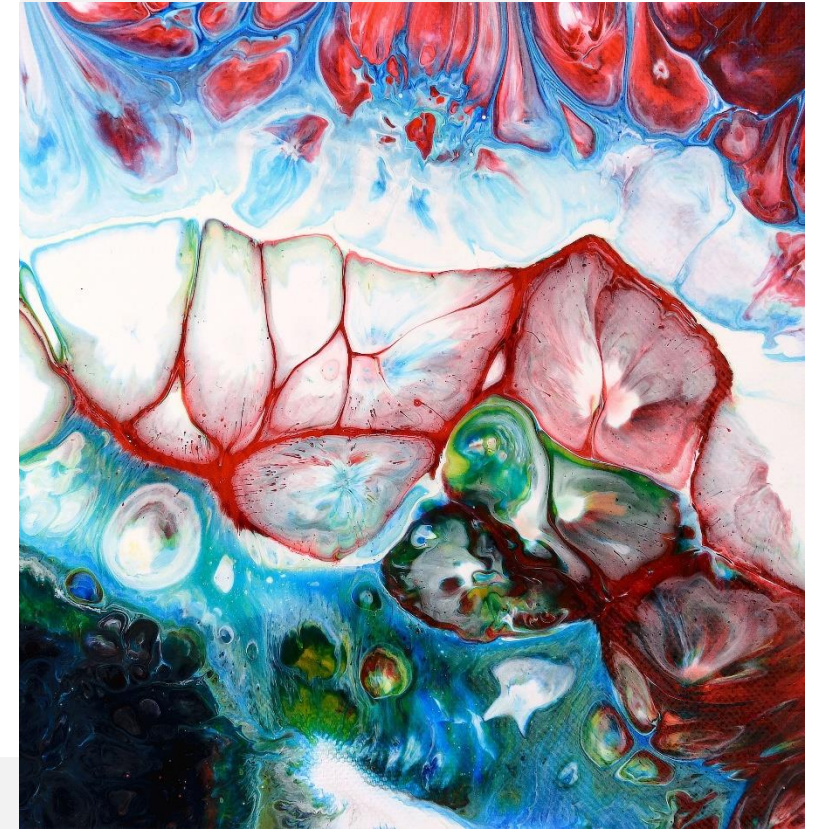
State v. Johnson, 2019 WL 1028462 (Mo. App. W.D. Mar. 5, 2019).

- 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.*



CARPENTER

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

A new expectation of privacy test



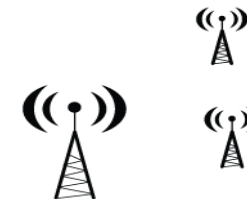
DECIDED

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

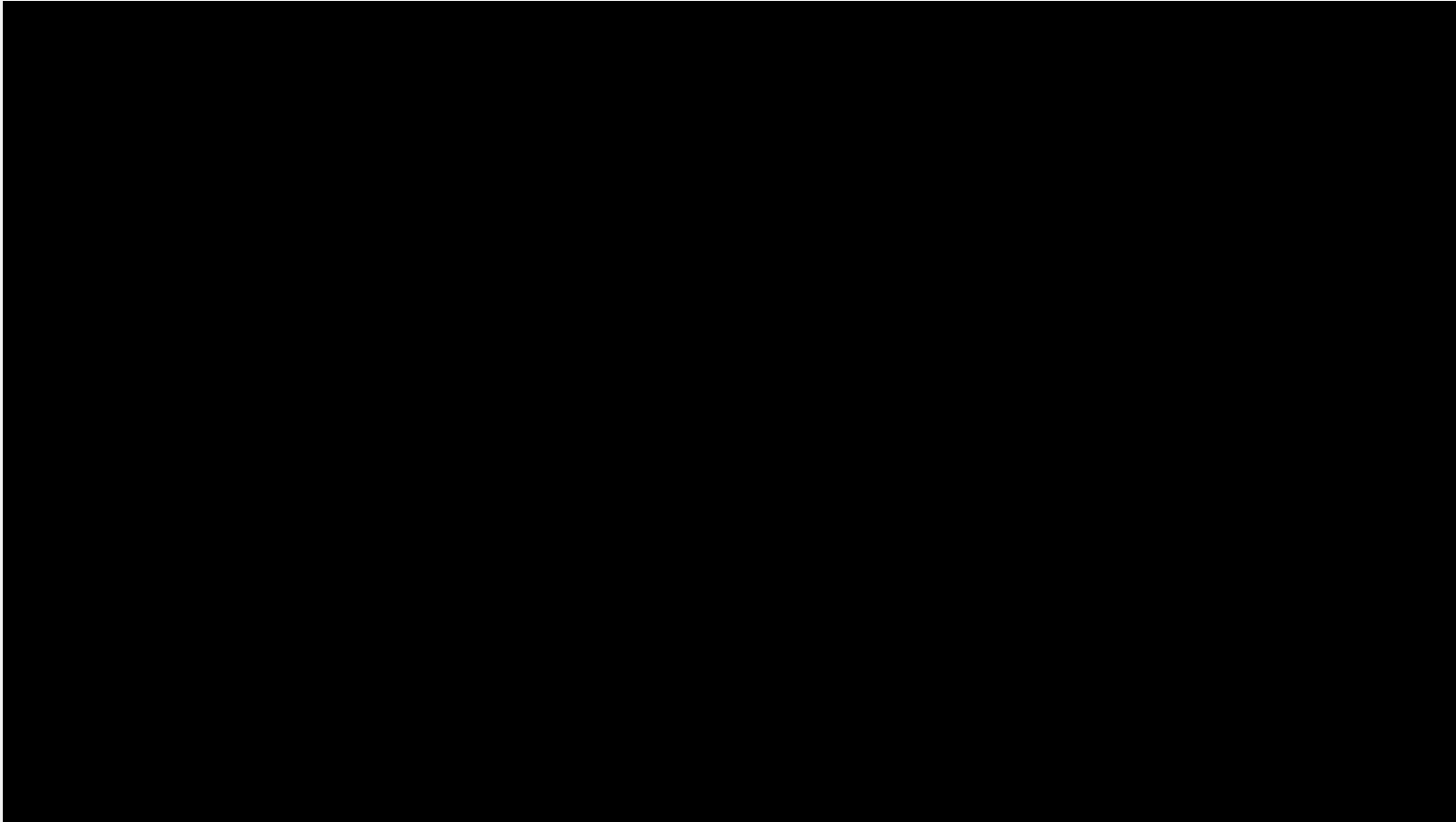


INTERPRETING *CARPENTER*

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 search 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 2019).



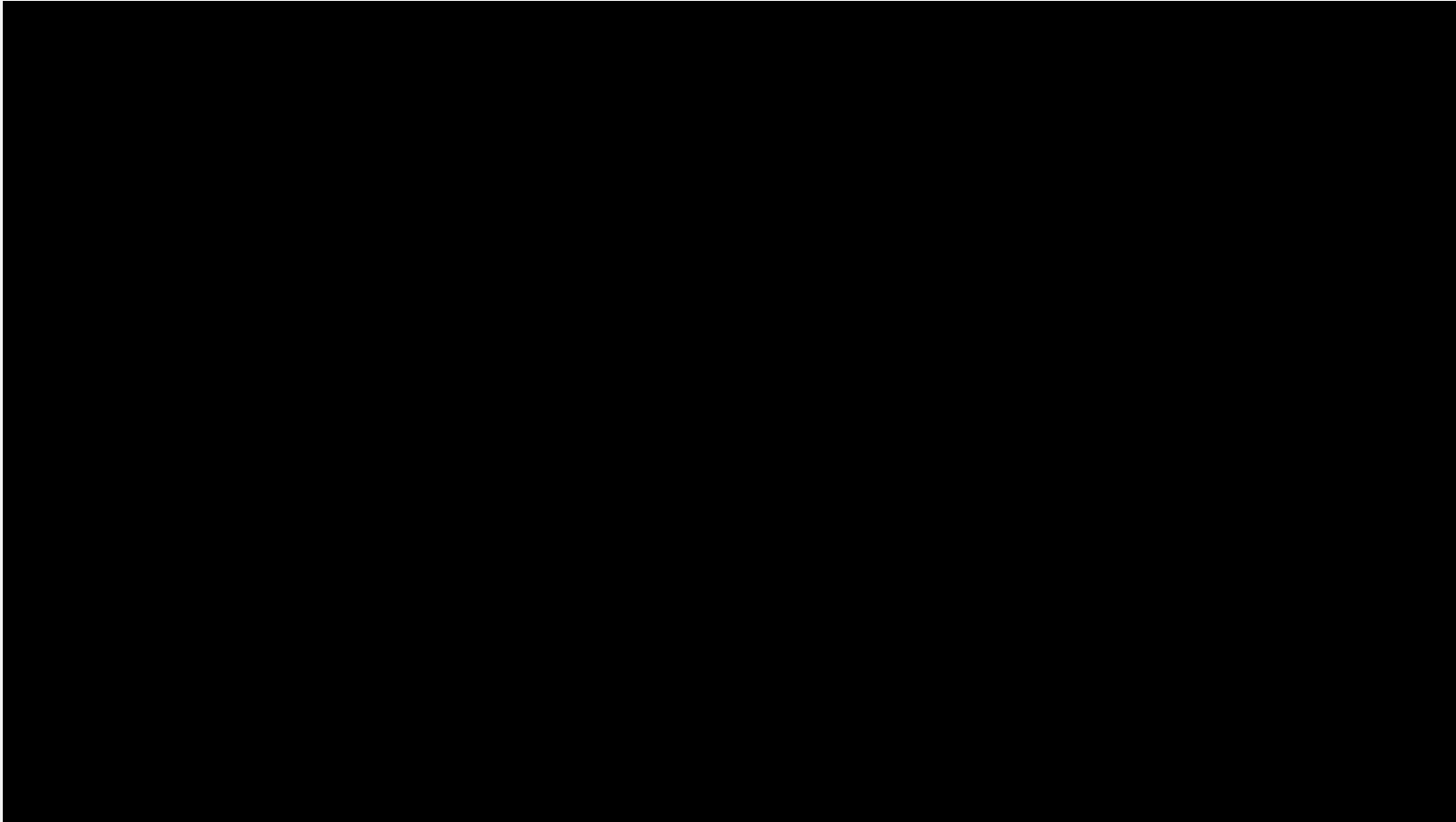
IMPLEMENTING *CARPENTER*

What does it mean for other emergent technologies + tactics?

Three approaches:

1. Subjective
2. Mosaic Theory
3. Source Rule



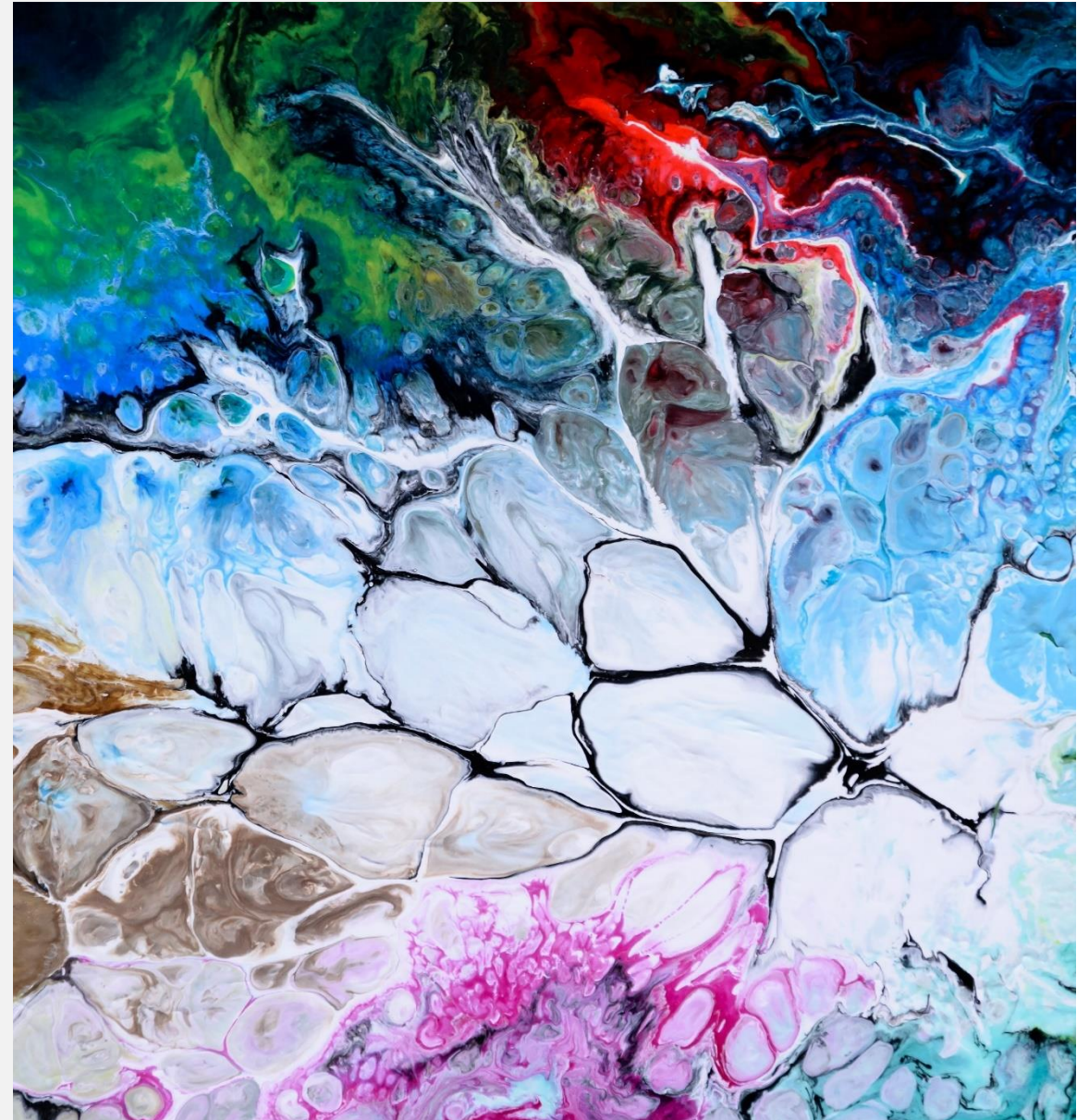


IMPLEMENTING *CARPENTER*

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:

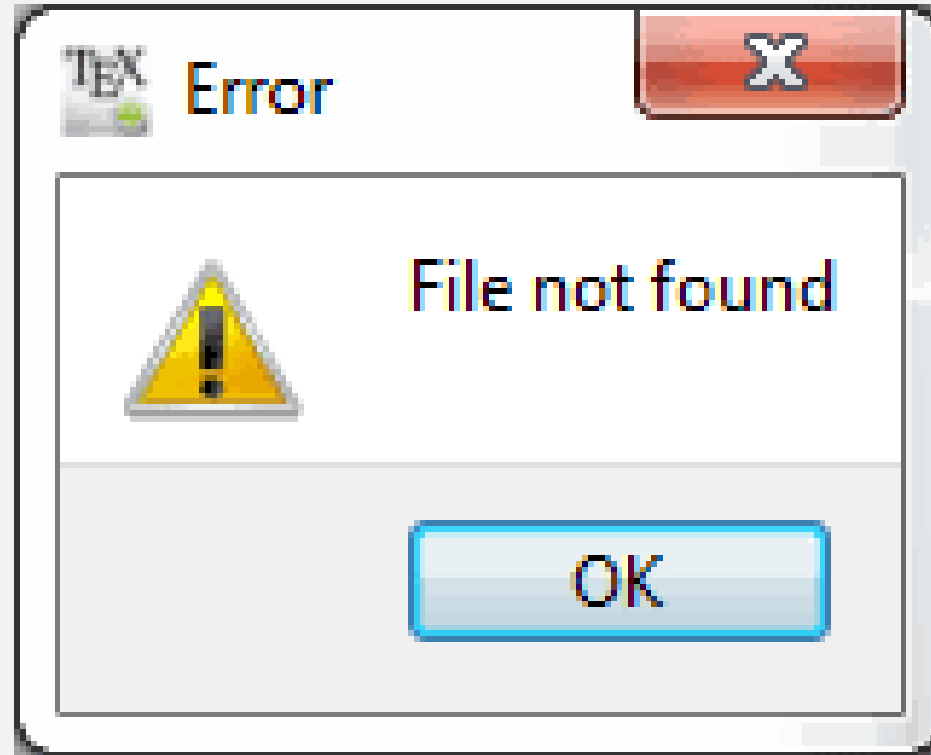
1. SMS metadata category of info not readily acquired in pre-digital age → orders of magnitude different than phone calls/postal mail
2. SMS, email, Facebook messaging, etc. have become “indispensable to participation in modern society” → metadata created without “meaningful” voluntary choice
3. Metadata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





APPLYING *CARPENTER* TO EMERGING TECHNOLOGIES

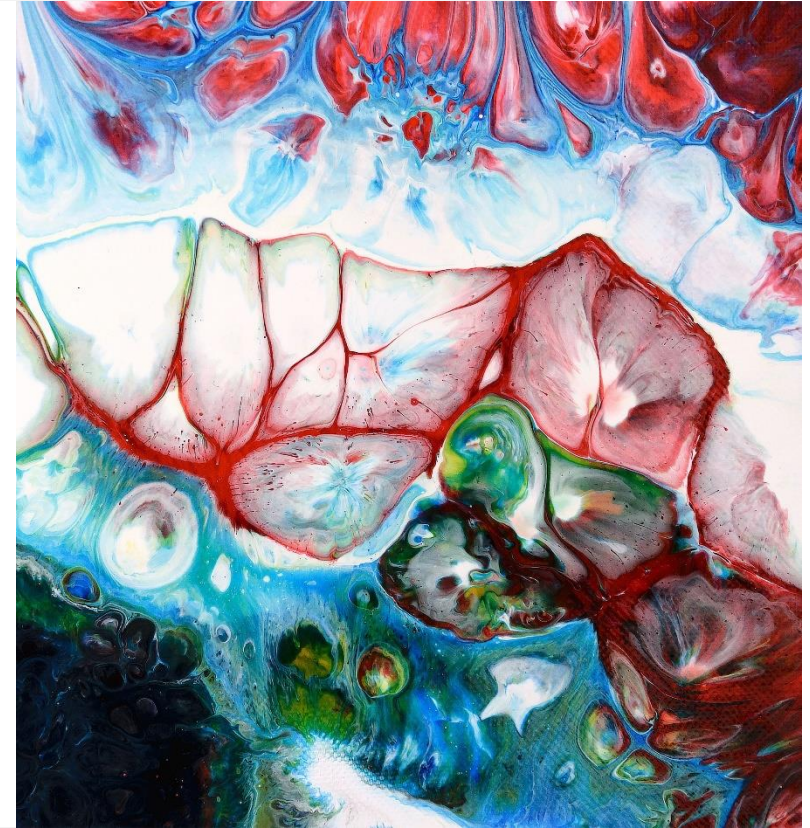
*Opportunities for
creative practice*



“REVERSE LOCATION SEARCH WARRANTS”

What is the government to do when it has no:

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



“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”).



“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

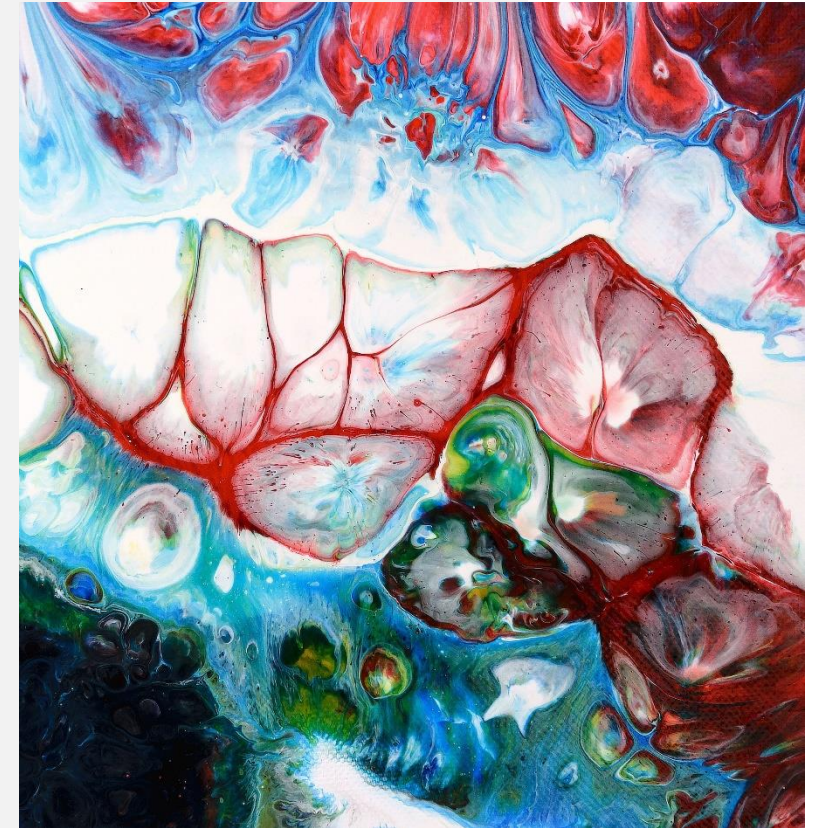
Point 2: 44°57'24.24" N 93°07'30.94" W

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

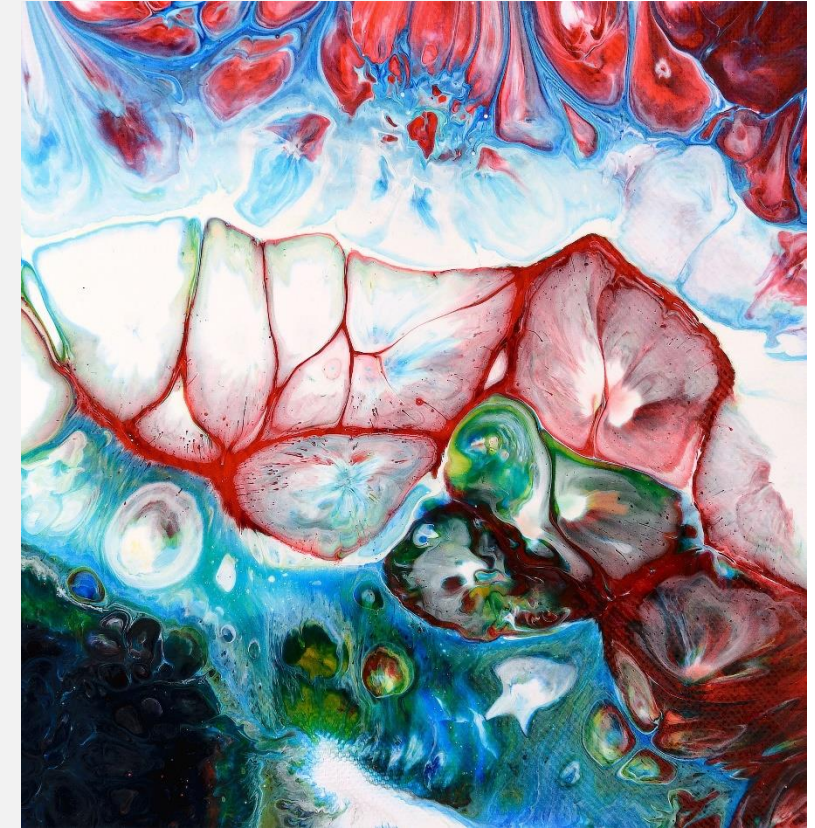
Point 4: 44°57'14.85" N 93°07'45.69" W

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):



“REVERSE LOCATION SEARCH WARRANTS”



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

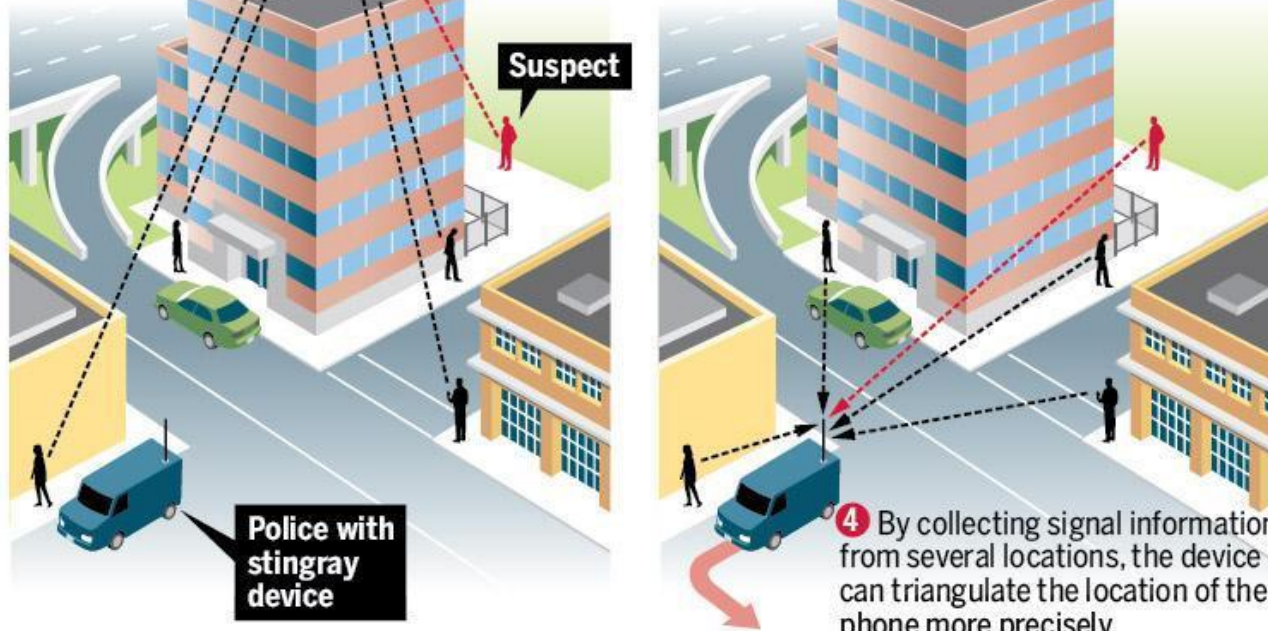
Police with stingray device

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.

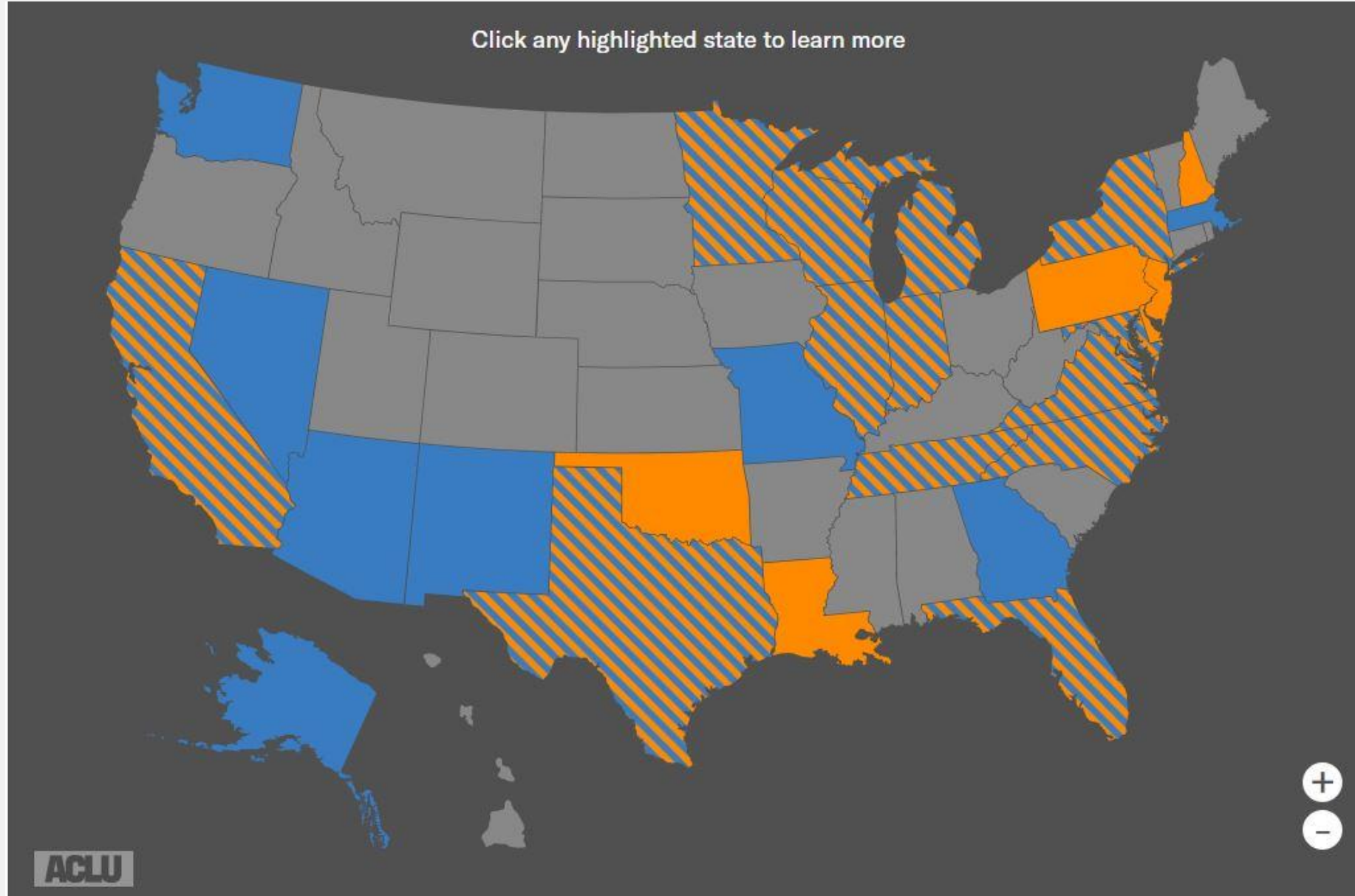
DOUG GRISWOLD/BAY AREA NEWS GROUP



Source: Washington Post, Wall Street Journal, USA Today



STINGRAY



STINGRAY

Considerations:

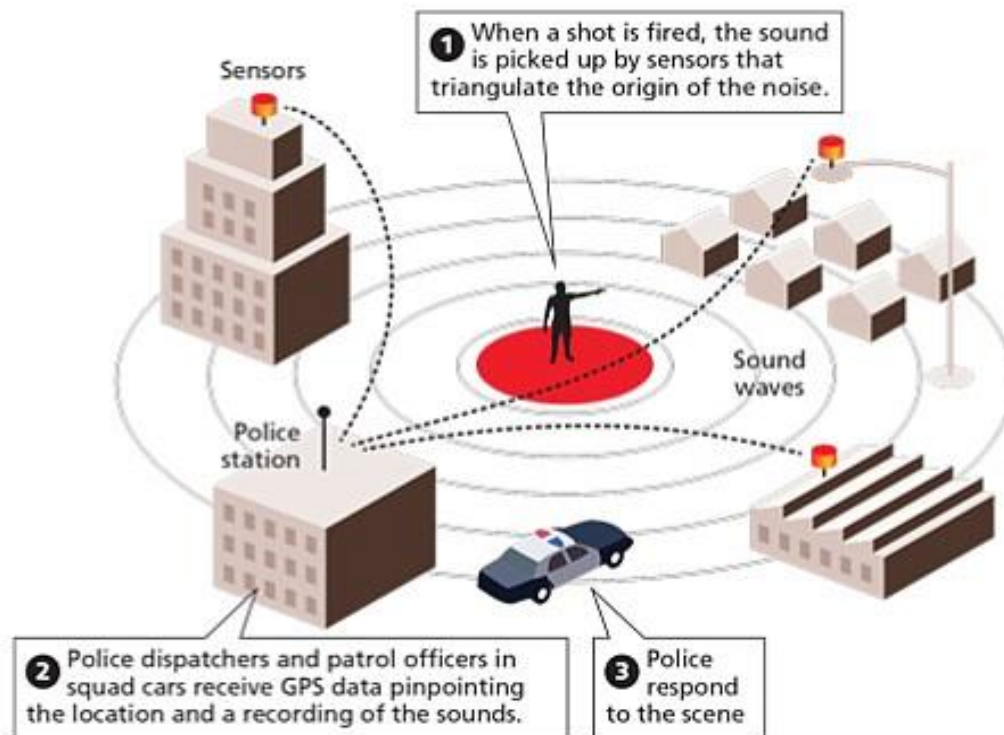
- Real-time CSLI more intrusive than historic CSLI?
- Isn't snatching texts + convos out of mid-air *exponentially* more intrusive than historic CSLI?
- Limited reading of *Carpenter*'s holding
 - *Andres v. State*, 254 So.3d 283 (Fla. 2018) → refused to extend *Crawford* to suppress evidence seized 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:

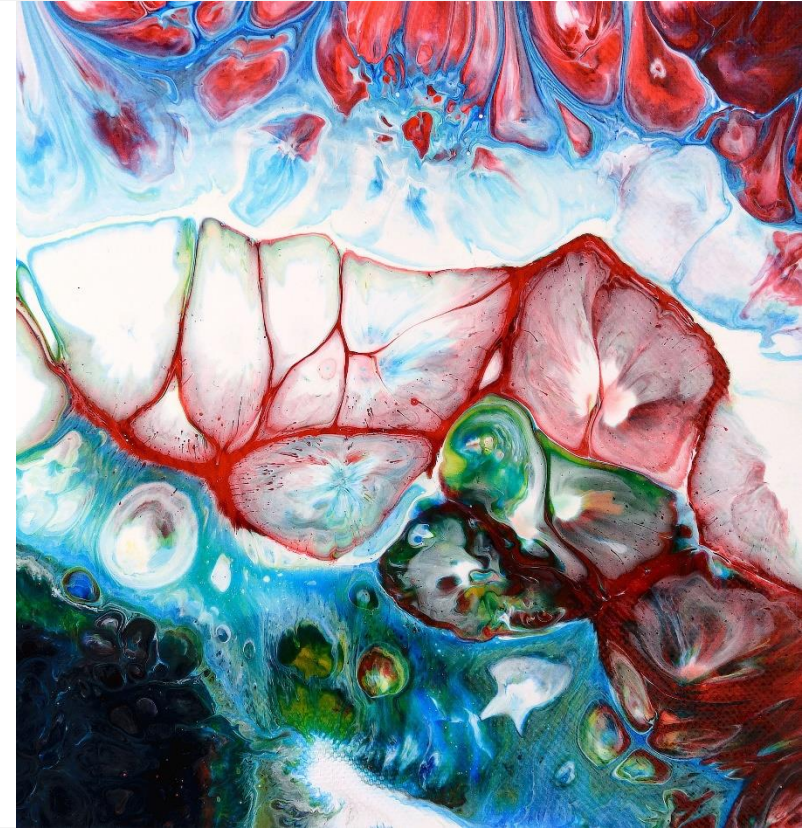
- “agnostic...gunshot detection, acoustic surveillance technology that uses sophisticated sensors to detect, locate and alert law enforcement agencies of illegal gunfire incidents in real time.”



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

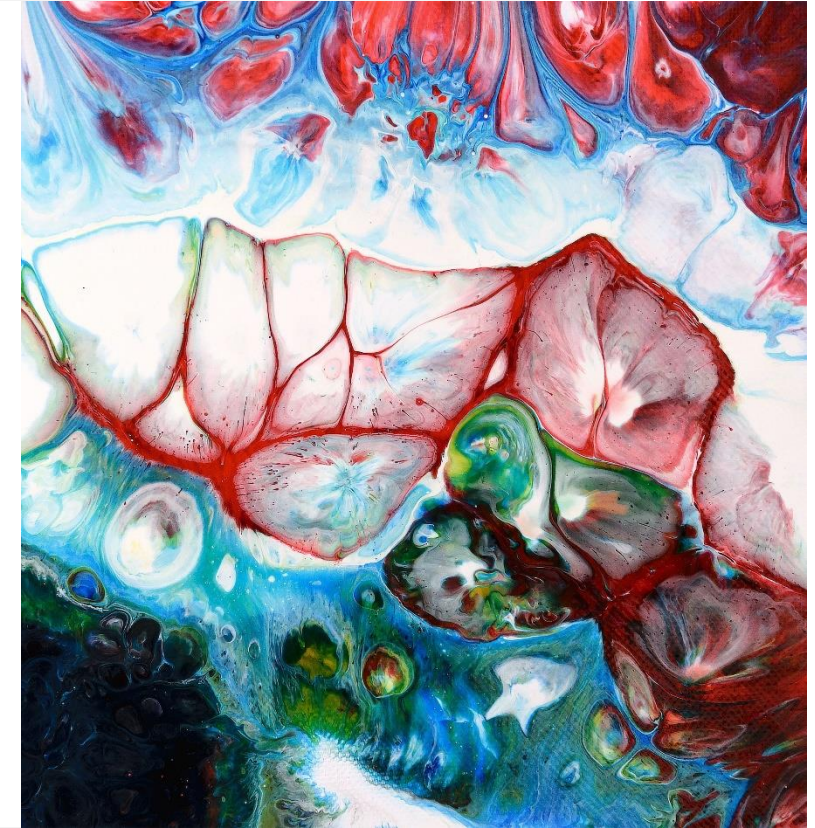


AUTOMATIC LICENSE PLATE RECOGNITION

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**



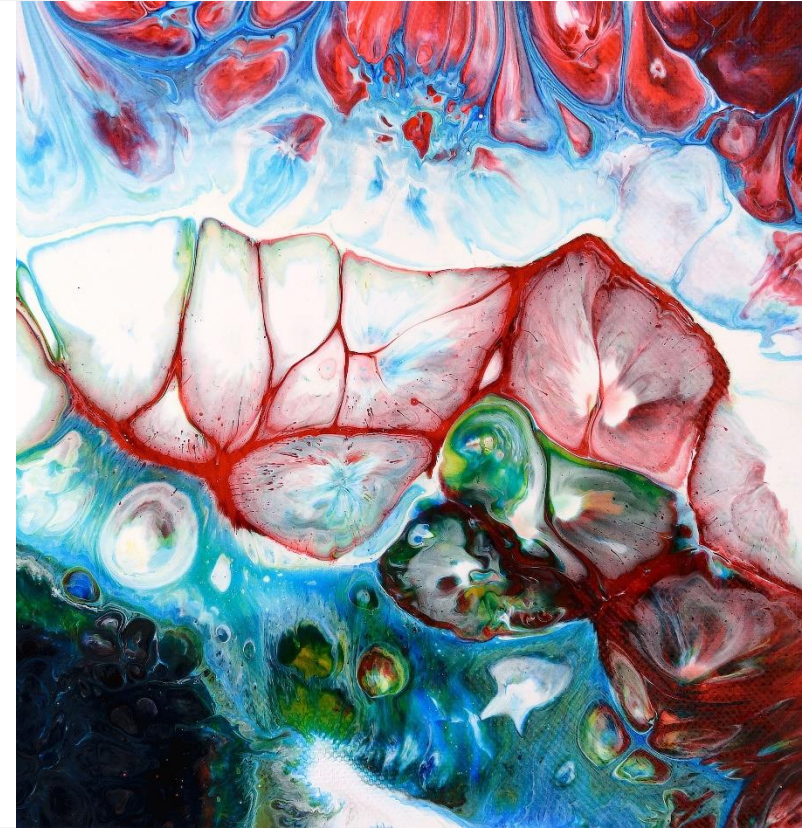
AUTOMATIC LICENSE PLATE RECOGNITION

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).



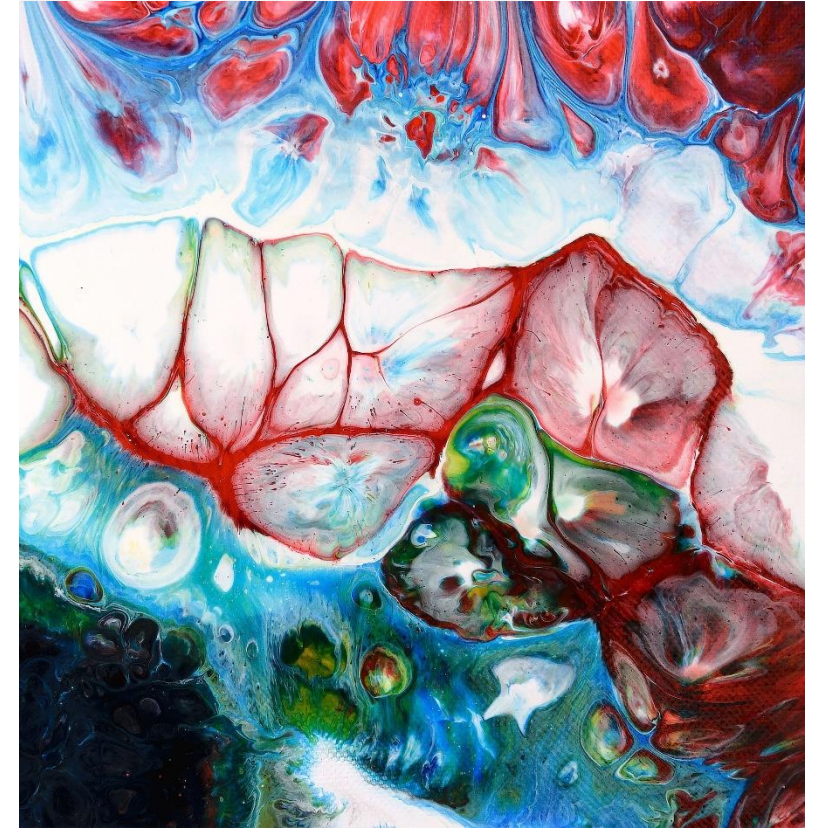
BIOMETRIC SURVEILLANCE TECH

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?

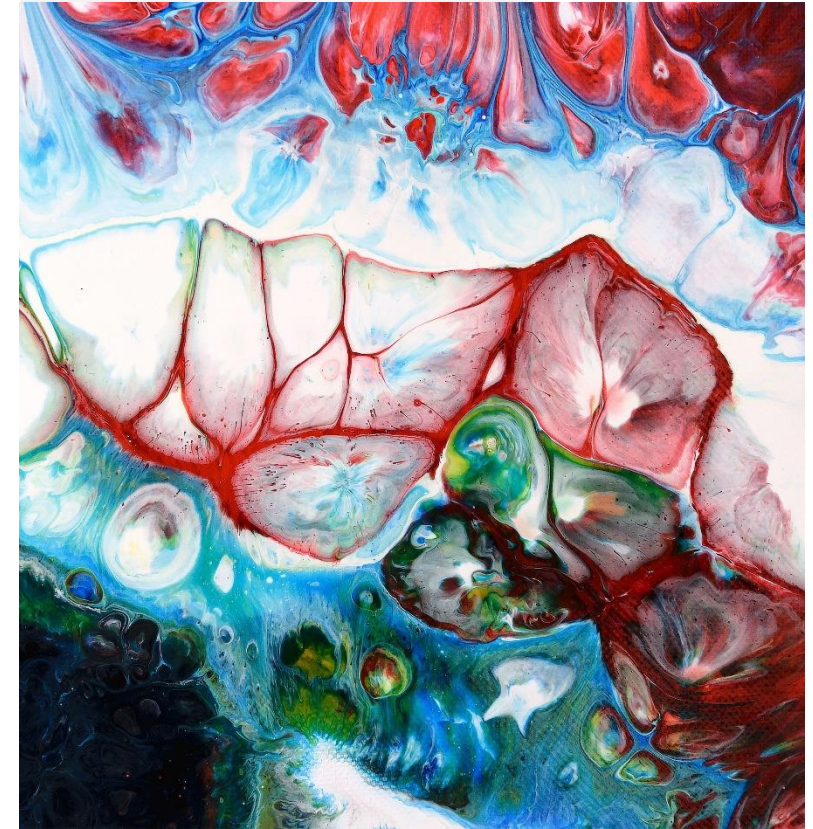
Historically → no protection for biometrics (4A or 5A)

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.”
- “It 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.”

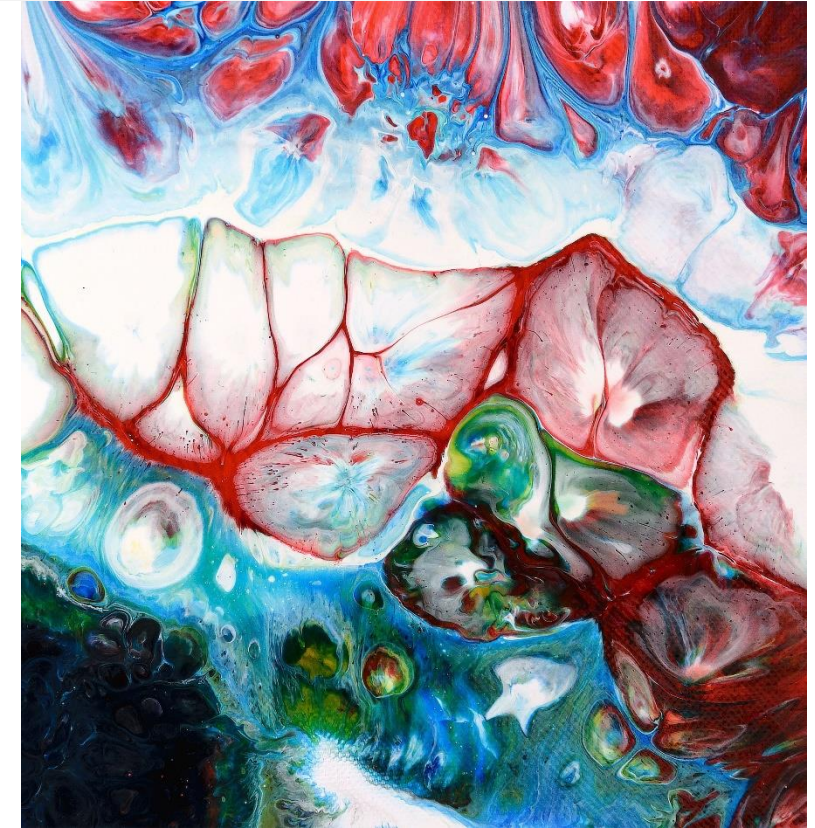


SMMS

Social Media Monitoring Software

Cf. SMS

DigitalStakeout



THANK YOU

Ellen Flottman + the Area 50 attorneys
Profs. Orin Kerr + Adam Gershowitz
The Founders

Jedd C. Schneider 📞 573.777.9977 x325

✉ *Jedd.Schneider@mspd.mo.gov*