Third, FRT raises issues with widespread passive identification that no longer requires a seizure. A person is seized when their freedom of movement is restrained and a reasonable person believes they are not free to leave.[[1]](#footnote-1) Traditional identification cases are predicated on a seizure.[[2]](#footnote-2) But if an officer takes someone’s picture and identifies them without stopping them, then there is no seizure.

Facial recognition technology creates the potential for massive increase in law enforcement’s ability to identify someone beyond human ability. In his *Jones* concurrence, Alito took issue with the “gigantic coach” or “very tiny constable” unimaginable to the framers that replaces large investigative teams with automated tasks. FRT creates a new constable, unimaginable to the framers, with a perfect photographic and encyclopedic memory; an officer who doesn’t need to stop someone to identify them, who never forgets a name or a face, and has painstakingly learned millions or billions of people.

One on hand, a less invasive identification that doesn’t require a seizure can be welcomed. But on the other hand, when a person’s home or effects are searched, or when they are seized, they are given notice of the search.

If the courts or policymakers determine that identification with FRT is a search, they should require law enforcement give notice in a similar manner. This requirement has a statutory history. When the government searches email and other communications, the Stored Communications Act often requires immediate or delayed notice to the target that the search occurred.[[3]](#footnote-3) Government wiretaps, governed by Title III of the Wiretap Act, also require notice and other requirements such as necessity, minimization, time limits.[[4]](#footnote-4)

Most mosaic theory arguments face a steep uphill battle. There is no constitutional protection or reasonable expectation that your picture taken or you won’t be recognized in public.[[5]](#footnote-5) Security camera footage, identification by a familiar officer or witness, and identification through fingerprints and DNA left at a crime scene don’t implicate the Fourth Amendment. But anytime an FRT technology tracks long-term or real-time location, or when identification is on a massive automated scale, the mosaic theory should be considered.

# Identification With FRT Not in General Public Use is a Search

Use of a device not in general public use to ascertain information from inside a home unknowable without physical intrusion is a search.[[6]](#footnote-6) This stems from *Kyllo v. United States*, where the Supreme Court ruled that use of a thermal imaging device capable of detecting heat emanating from a house constituted a search.[[7]](#footnote-7) The device need not look inside the home; heat detected emanating from the walls of the house, sound detected by a high-powered microphone, and light emanating from a house detected by a satellite are similarly protected.[[8]](#footnote-8)

*Kyllo* extends to FRT if three conditions are met: 1) the FRT must not be in public use, 2) the protections of the home must extend to a person in public, and 3) that details would only be known with a more invasive search or seizure.

First, the FRT used by law enforcement must not be in public use. A novice coder can use open-source tools to create their own basic facial recognition program (see Section II.A). Law enforcement differs in that they are presumably using a proprietary software not available to individuals and that they are comparing images to a database not in public use. Databases require a massive number of images. Training a large and accurate database requires proprietary tools, massive computing power, and resources not in regular use.

That amateurs can make a simple model is not dispositive. Millions of Americans train their dogs to perform basic tricks, but that doesn’t mean a drug-sniffing dog (comparable to high-powered binoculars) is in general use.[[9]](#footnote-9)

Second, the Court must be willing to extend *Kyllo* protections from the home to the person. The home is considered “sacred” for purposes of Fourth Amendment protection.[[10]](#footnote-10) But “the Fourth Amendment protects people, not places.”[[11]](#footnote-11) And an “intrusion into the human body” is “an invasion of cherished personal security that is subject to constitutional scrutiny.”[[12]](#footnote-12) If these two conditions are met, it follows that the features extracted from processing an image are akin to *Kyllo’s* thermal camera processing heat emanating from the house. After all, Kyllo is an extension of the *Katz* reasonable expectation of privacy. In *Katz*, the occupant of a glass telephone booth was not protected from being seen in public; they were protected from the use of a high-powered eavesdropping tool in place where they expected aural privacy.[[13]](#footnote-13) Applied to FRT, one can expect their face is seen in public without being algorithmically processed and identified against a massive database.

That someone exposes their face to the world is not dispositive. People expose their breath and other bodily waste to the public with a reasonable expectation of privacy that it is not used to create a massive identification database.

Third, the FRT search would also need to “explore details of the” person that would be otherwise known only thanks to a search or seizure.[[14]](#footnote-14) Applied to the home in *Kyllo*, the details included “any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area.”[[15]](#footnote-15) As discussed, in Section III, identification is usually linked to a seizure. A defendant challenging an FRT identification would have to show that they could not be identified by the police officer without being seized. If they were already legally seized (e.g., in a traffic stop or *Terry* stop) then the officer could constitutionally compel identification.

Courts could rule that the technology is not in public use, but it would require a liberal application of *Kyllo*. Prongs one and two, above, are the most challenging hurdles. Courts would need to distinguish the massive proprietary commercial or law enforcement databases from amateur technology and extend protections of the home to people in public in possible conflict with plain view, *Knotts* tracking, and third-party doctrine.

1. *United States v. Mendenhall*, 446 U.S. 544, 553-54 (1980). [↑](#footnote-ref-1)
2. *See Hiibel v. Sixth Judicial Dist. Court of Nevada, Humboldt Cty.*, 542 U.S. 177, 188 (2004) (holding that “the request for identity has an immediate relation to the purpose, rationale, and practical demands of a Terry stop”); *Brown v. Texas*, 443 U.S. 47, 50 (1979) (holding that stopping someone and requiring them to identify himself is a seizure); *Hayes v. Fla.*, 470 U.S. 811, 814 (1985) (holding that “taking a suspect to the police station for fingerprints without probable cause was an illegal seizure”). [↑](#footnote-ref-2)
3. *See* 18 U.S.C. § § 2703(b), 2705. [↑](#footnote-ref-3)
4. 18 U.S.C. § 2510 et seq. [↑](#footnote-ref-4)
5. *U.S. v. Knotts*, 460 U.S. 276, 281. [↑](#footnote-ref-5)
6. *Kyllo v. United States*, 533 U.S. 27, 40 (2001). [↑](#footnote-ref-6)
7. *Id.* at 34-35. [↑](#footnote-ref-7)
8. *Id.* at 35-36. [↑](#footnote-ref-8)
9. *Florida v. Jardines*, 133 S. Ct. 1409, 1418 (2013) (Kagan, J., concurring) [↑](#footnote-ref-9)
10. *Id.* at 1415. [↑](#footnote-ref-10)
11. *Katz v. United States*, 389 U.S. 347, 351 (1967). [↑](#footnote-ref-11)
12. *Maryland v. King*, 569 U.S. 435, 446 (2013). [↑](#footnote-ref-12)
13. *Kyllo*, 533 U.S. at 35. [↑](#footnote-ref-13)
14. *Kyllo*, 533 U.S. at 40. [↑](#footnote-ref-14)
15. *Id.* at 34 [↑](#footnote-ref-15)