This fall, the Supreme Court is set to take on what could be one of its most important privacy cases in decades. However, even a sweeping ruling is unlikely to fully resolve the question at issue: How should the government be limited in location tracking? I would like to highlight two key forms of location tracking that will likely be critically important unresolved issues even after this case, and how we should respond.

Location tracking has become a major part of law enforcement investigations. In 2016, the government issued over 120,000 orders for location data. In its significant 2012 ruling in United States v. Jones, the Supreme Court held that attaching a GPS tracking device to a vehicle required a probable cause warrant. Unfortunately, as is far too often the case, law was outpaced by technology. By the time the ruling occurred, and at an even greater rate since then, location tracking via GPS devices was replaced by cell-site location tracking. Because cell phones are far more common than cars and are with their owners far more often, the government is able to more comprehensively track movements with this technique.

This fall, the Supreme Court will look to close this gap by directly taking on the question of whether a warrant should be required for cell phone location tracking, in Carpenter v. United States. The Constitution Project will participate in this case by submitting an amicus brief highlighting the sensitivity of location data, and pervasiveness of cell phone location data. By examining whether individuals have a Fourth Amendment privacy right to location data in which there is no direct contact with law enforcement – and thus no trespass as was the basis of the Jones ruling – the Court could substantially expand privacy rights. Based on the concurring opinions in Jones regarding the sensitivity of location data, and huge risk of unfettered government access to it, along with the Court’s recent emphasis in Riley v. California on how new electronic data can change the nature of Fourth Amendment rules, such an outcome seems likely.

However, even a broad ruling that sets clear and strong limits on cell-site tracking is unlikely to resolve the issue of government’s unprecedented location tracking power. It would be difficult for the Supreme Court to create a blanket rule on electronic aids to location tracking. A rule that would cover all problematic techniques without also hampering basic access to items like traffic cameras would likely require far too detailed and proscriptive a standard for a court ruling.

I would like to highlight and examine two emerging technologies that are highly likely to continue to raise concerns about location tracking surveillance in the wake of Carpenter, explain their significance, and propose a response for each. These technologies are facial recognition
surveillance, and aerial surveillance incorporating new computer analysis and camera magnification capacity.

Facial recognition is a powerful emerging technology, increasingly being used by law enforcement throughout the country. According to the Georgetown Law Center on Privacy and Technology, one in two American adults are already enrolled in a law enforcement facial recognition network, and at least one in four police departments have the capacity to run face recognition searches.¹ As government CCTV cameras become more common and vendors continue to develop police body cameras with facial recognition technology, facial recognition surveillance will become an effective means of location tracking.² This is incredibly worrisome; facial recognition can occur without notification or consent, can identify and catalog thousands of individuals with little human effort, and can be targeted at sensitive locations such as places of worship, protests, and political rallies. Many states have already passed laws requiring a warrant for electronic location tracking to address cell-site location tracking, but they are written in a manner that does not limit facial recognition location tracking. I would propose legislation that directly requires a probable cause warrant for facial recognition surveillance to prevent using it for location tracking in a manner that is likely to avoid whatever limits are installed in Carpenter.

Second, aerial surveillance is also an emerging law enforcement technique with tremendous power. I have previously published research on how existing aerial surveillance programs such as Baltimore’s “Persistent Surveillance” program involving continually flying Cessna planes over the city is boasted to allow location tracking without connection to cell phones, or use of software like facial recognition technology, and how new camera magnification technology developed by DARPA could soon expand such capabilities to permit aerial location tracking of every individual an area half the size of Manhattan.³ I would propose legislation following the “naked-eye rule” I have previously put forward to create a balanced system that does not fully limit law enforcement use of aerial activities, but does require a warrant for those activities and techniques that would involve pervasive and worrisome location tracking with little devotion of human resources.

Location tracking is a critical privacy issue. Even if Carpenter marks a significant step forward in checking government surveillance and giving adequate protection to privacy rights, it is highly important that we recognize the ongoing risks of technology outpacing law, and give due focus on future technologies that will permit pervasive location tracking in the future. I believe this


proposal – conducted as an individual presentation with opportunity for audience questions and feedback – will contribute to building focus on these important topics, and how we should respond.