Surveilling in Secret

Government surveillance is much more advanced than most people realize—thanks in part to the government’s studious efforts to keep these programs secret. At Cato’s 2017 Surveillance Conference, Sarah St. Vincent of Human Rights Watch explained how the government conceals many of these programs through parallel construction, while Clare Garvie of Georgetown Law’s Center on Privacy and Technology discussed the findings of the center’s alarming new report on face recognition technology, “Perpetual Lineup.”

Sarah St. Vincent: Parallel construction is one of the most frightening civil liberties issues that you may never have heard of. For the purposes of this discussion, I’m defining parallel construction as something that the government body does deliberately to create an alternative explanation for how it found a piece of evidence. The government did Thing A, but it doesn’t want the defense attorney, for example, to know that it did Thing A, so it goes back and does Thing B.

So how might this work? The Intercept recently had an article about immigration enforcement in Texas, and how state troopers are starting to find people through traffic stops. And I thought, my gosh, when somebody gets pulled over for having windows that are tinted too dark, and then lo and behold! They have an immigration issue! That is kind of too happy for law enforcement to be a coincidence.

So, hypothetically, say the government has some very large database of phone records—as we know they have had, thanks to the Snowden revelations—and suppose they use those phone records to look at someone who they know is undocumented. They could then ask: “Who was that person in touch with? Who else might be undocumented?” Because they know that this might raise constitutional issues, they might ask a local officer to pull over the car that belongs to a person that interests them. And they don’t always tell the officer what they’re looking for. So, the officer follows the car, waits for it to drift over a line, or to not signal 20 feet before a turn. They pull the person over and then say, “Hey, now that I checked your license, can I ask you a couple of questions? Where do you live? How long have you lived there? What’s your nationality?” And then as far as you would know, as the defense attorney, for example, to know that it did Thing A, so it goes back and does Thing B.

What does the government seek to conceal through parallel construction? Well, potentially anything—and I mean, really, anything. It could be a wiretap with a warrant. It could be a human source, or it could be a gigantic NSA or DEA program.

SARAH ST. VINCENT: Parallel construction as something that a government body does deliberately to create an alternative explanation for how it found a piece of evidence. The government did Thing A, but it doesn’t want the defense attorney, for example, to know that it did Thing A, so it goes back and does Thing B.

So, hypothetically, say the government has some very large database of phone records—as we know they have had, thanks to the Snowden revelations—and suppose they use those phone records to look at someone who they know is undocumented. They could then ask: “Who was that person in touch with? Who else might be undocumented?” Because they know that this might raise constitutional issues, they might ask a local officer to pull over the car that belongs to a person that interests them. And they don’t always tell the officer what they’re looking for. So, the officer follows the car, waits for it to drift over a line, or to not signal 20 feet before a turn. They pull the person over and then say, “Hey, now that I checked your license, can I ask you a couple of questions? Where do you live? How long have you lived there? What’s your nationality?” And then as far as you would know, as the defense attorney, for example, to know that it did Thing A, so it goes back and does Thing B.

So, hypothetically, say the government has some very large database of phone records—as we know they have had, thanks to the Snowden revelations—and suppose they use those phone records to look at someone who they know is undocumented. They could then ask: “Who was that person in touch with? Who else might be undocumented?” Because they know that this might raise constitutional issues, they might ask a local officer to pull over the car that belongs to a person that interests them. And they don’t always tell the officer what they’re looking for. So, the officer follows the car, waits for it to drift over a line, or to not signal 20 feet before a turn. They pull the person over and then say, “Hey, now that I checked your license, can I ask you a couple of questions? Where do you live? How long have you lived there? What’s your nationality?” And then as far as you would know, as the defense attorney, for example, to know that it did Thing A, so it goes back and does Thing B.

So how might this work? The Intercept recently had an article about immigration enforcement in Texas, and how state troopers are starting to find people through traffic stops. And I thought, my gosh, when somebody gets pulled over for having windows that are tinted too dark, and then lo and behold! They have an immigration issue! That is kind of too happy for law enforcement to be a coincidence.

So, hypothetically, say the government has some very large database of phone records—as we know they have had, thanks to the Snowden revelations—and suppose they use those phone records to look at someone who they know is undocumented. They could then ask: “Who was that person in touch with? Who else might be undocumented?” Because they know that this might raise constitutional issues, they might ask a local officer to pull over the car that belongs to a person that interests them. And they don’t always tell the officer what they’re looking for. So, the officer follows the car, waits for it to drift over a line, or to not signal 20 feet before a turn. They pull the person over and then say, “Hey, now that I checked your license, can I ask you a couple of questions? Where do you live? How long have you lived there? What’s your nationality?” And then as far as you would know, as the defense attorney, for example, to know that it did Thing A, so it goes back and does Thing B.

So how might this work? The Intercept recently had an article about immigration enforcement in Texas, and how state troopers are starting to find people through traffic stops. And I thought, my gosh, when somebody gets pulled over for having windows that are tinted too dark, and then lo and behold! They have an immigration issue! That is kind of too happy for law enforcement to be a coincidence.

So, hypothetically, say the government has some very large database of phone records—as we know they have had, thanks to the Snowden revelations—and suppose they use those phone records to look at someone who they know is undocumented. They could then ask: “Who was that person in touch with? Who else might be undocumented?” Because they know that this might raise constitutional issues, they might ask a local officer to pull over the car that belongs to a person that interests them. And they don’t always tell the officer what they’re looking for. So, the officer follows the car, waits for it to drift over a line, or to not signal 20 feet before a turn. They pull the person over and then say, “Hey, now that I checked your license, can I ask you a couple of questions? Where do you live? How long have you lived there? What’s your nationality?” And then as far as you would know, as the defense attorney, for example, to know that it did Thing A, so it goes back and does Thing B.

So how might this work? The Intercept recently had an article about immigration enforcement in Texas, and how state troopers are starting to find people through traffic stops. And I thought, my gosh, when somebody gets pulled over for having windows that are tinted too dark, and then lo and behold! They have an immigration issue! That is kind of too happy for law enforcement to be a coincidence.

So, hypothetically, say the government has some very large database of phone records—as we know they have had, thanks to the Snowden revelations—and suppose they use those phone records to look at someone who they know is undocumented. They could then ask: “Who was that person in touch with? Who else might be undocumented?” Because they know that this might raise constitutional issues, they might ask a local officer to pull over the car that belongs to a person that interests them. And they don't always tell the officer what they're looking for. So, the officer follows the car, waits for it to drift over a line, or to not signal 20 feet before a turn. They pull the person over and then say, “Hey, now that I checked your license, can I ask you a couple of questions? Where do you live? How long have you lived there? What’s your nationality?” And then as far as you would know, as the defense attorney, for example, to know that it did Thing A, so it goes back and does Thing B.

So how might this work? The Intercept recently had an article about immigration enforcement in Texas, and how state troopers are starting to find people through traffic stops. And I thought, my gosh, when somebody gets pulled over for having windows that are tinted too dark, and then lo and behold! They have an immigration issue! That is kind of too happy for law enforcement to be a coincidence.

So, hypothetically, say the government has some very large database of phone records—as we know they have had, thanks to the Snowden revelations—and suppose they use those phone records to look at someone who they know is undocumented. They could then ask: “Who was that person in touch with? Who else might be undocumented?” Because they know that this might raise constitutional issues, they might ask a local officer to pull over the car that belongs to a person that interests them. And they don't always tell the officer what they're looking for. So, the officer follows the car, waits for it to drift over a line, or to not signal 20 feet before a turn. They pull the person over and then say, “Hey, now that I checked your license, can I ask you a couple of questions? Where do you live? How long have you lived there? What’s your nationality?” And then as far as you would know, as the defense attorney, for example, to know that it did Thing A, so it goes back and does Thing B.

So how might this work? The Intercept recently had an article about immigration enforcement in Texas, and how state troopers are starting to find people through traffic stops. And I thought, my gosh, when somebody gets pulled over for having windows that are tinted too dark, and then lo and behold! They have an immigration issue! That is kind of too happy for law enforcement to be a coincidence.

So, hypothetically, say the government has some very large database of phone records—as we know they have had, thanks to the Snowden revelations—and suppose they use those phone records to look at someone who they know is undocumented. They could then ask: “Who was that person in touch with? Who else might be undocumented?” Because they know that this might raise constitutional issues, they might ask a local officer to pull over the car that belongs to a person that interests them. And they don't always tell the officer what they're looking for. So, the officer follows the car, waits for it to drift over a line, or to not signal 20 feet before a turn. They pull the person over and then say, “Hey, now that I checked your license, can I ask you a couple of questions? Where do you live? How long have you lived there? What’s your nationality?” And then as far as you would know, as the defense attorney, for example, to know that it did Thing A, so it goes back and does Thing B.

So how might this work? The Intercept recently had an article about immigration enforcement in Texas, and how state troopers are starting to find people through traffic stops. And I thought, my gosh, when somebody gets pulled over for having windows that are tinted too dark, and then lo and behold! They have an immigration issue! That is kind of too happy for law enforcement to be a coincidence.
why it was so important to renew FISA Section 702, a major intelligence surveillance law. But that was not anywhere in the indictment, or any of the court records we’ve seen, and the prosecution claimed that this came from publicly available information.

If parallel construction is legal, does the Bill of Rights still have any meaning? If the government can do things that are constitutionally questionable, or that it should know are unlawful, and then simply never tell anyone, do those rights still have any meaning? I think this is very, very frightening.

CLARE GARVIE: I want you to imagine for a second that you’re home at night. It’s 8:00 p.m., and the police knock on your door and say there’s been a robbery in the neighborhood. They say, “Don’t worry, we think we have the person who did it in custody. However, we want you to come down to the station and stand in a lineup.”

I think a lot of us would say no. You might be thinking, I must look a lot like this guy. What if the witness points to me instead of the real suspect?

Well, the reality is, thanks to facial recognition, at least 53 percent of all American adults are now in what we call a “perpetual lineup.” This is not because they have had prior interaction with law enforcement, but because they have a driver’s license. The use of face recognition technology by law enforcement is far more pervasive and far more advanced than most people realize.

As a preliminary, I want to briefly go through how face recognition is used by police today. The first use is what we call “stop and identify.” A handful of agencies across the country have face recognition applications on their phones, meaning that officers in the field, after they’ve stopped somebody, can actually look up that person’s identity with a face recognition application simply by taking their picture. This process takes about three seconds. Second, there’s “arrest and identify”—upon arrest in most jurisdictions that have a face recognition system, the person arrested, regardless of whether they’re charged or later convicted, will have their mugshot taken, and that photo will be searched against the existing database and enrolled into a face recognition database for future searches. The third is “investigate and identify.” Let’s say officers have a surveillance video of a bank robbery taking place, or a cell phone video of a theft. They can take that photo, and if there’s a good enough face in any of those stills, they can run that through a face recognition system and search for that individual against whatever database they have.

The fourth and most concerning application of face recognition that we’re seeing is real-time biometric surveillance. Increasingly, law enforcement agencies are expressing interest in using face recognition at the back-end of CCTV systems in real time to monitor who’s walking by those cameras.

The other component of face recognition that we need to talk about briefly is the fact that we’re seeing a disparate impact on African Americans. This is because of three factors. The first is illustrated by a
study in San Diego, which found that people
of color were between 1.5 and 2.5 times more
likely to be targeted than expected by their
presence in the population by advanced tech-
nology, specifically license plate readers and
face recognition. The second is that most face
recognition systems run on mugshots, and if
we look at arrests-to-population ratios,
African Americans are arrested at far greater
rates than their proportion of the population
would suggest. So African Americans are
overrepresented in the searches, the probe
photos, and in the databases themselves.

The third prong is the search itself. Tak-
ing a step back, face recognition is not very
accurate. A few years ago, the FBI ran a test
on the searches that they conduct and found
that they were about 86 percent accurate,
meaning that in six out of seven of the
searches they ran the suspect, who was in-
deed in the database, would show up in a list
of 2 to 50 possible candidates. One out of
seven searches would result in a list of com-
pletely innocent candidates, even though
the suspect was in their database. But com-
ounding this, the errors are not distributed
evenly. A 2012 study coauthored by an FBI
face recognition expert found that face
recognition algorithms are 5 to 10 percent
less accurate on African Americans, women,
and young people. More recent studies con-
tinue to demonstrate that these algorithms
perform differently depending on your de-
ographics, particularly race and gender.

Our third finding is that face recognition,
h owever pervasive or advanced it is, is not
under control. We found that there are no
comprehensive state or federal laws that gov-
ern the use of this technology by law en-
forcement. We then took a look at how the
agencies themselves are choosing to regulate
this and found that a very limited number of
agencies had policies to begin with. Very few
of those existing policies required individ-
ualized suspicion, limited the searches to cer-
tain crimes, required suspicion to begin with,
or prohibited searches on First Amend-
ment–protected activities. Many agencies
told us after our Freedom of Information Act
request that they didn’t have any rules gov-
erning how the technology is used—some
policies went even further than that, to say
that law enforcement is encouraged to use
this technology “whenever practical.” That
line is from the Pinellas County, Florida,
sheriff’s office policy. We talked to Sheriff Bob
Gualtieri there, in charge of operating the
longest-running system in the country. The
system has been used for about 16 years and
has never been audited, despite the fact that
about 8,000 searches are run on it every year.

This leads to one last question: Is there
any judicial control here? We went across the
street and spoke to Bob Dillinger, the public
defender for Pinellas County, and he said
never in his entire time running the public
defender’s office—and he’s been around for
the entire duration of the face recognition
program—has any case had face recognition
disclosed as Brady evidence. This is some-
thing one would expect, because face recog-
nition gives a list of possible candidates. Any
candidate who is listed by the algorithm who
was not the person charged would poten-
tially be exculpatory evidence that must be
turned over to the defense.

This technology may also be leading to
chilling free speech. After the death of Fredd-
ie Gray in police custody, the Baltimore
County Police Department reportedly used
Geofeedia in conjunction with face recogni-
tion to take photographs at public protests,
run them through face recognition, and
identify people at protest sites while the
demonstrations were going on. Law en-
forcement agencies themselves have said in
a 2011 report that this runs the risk of chilling
free speech, and yet that hasn’t stopped
them from using it with no limits.

There is reason for optimism. The House
oversight committee did hold a hearing after
the launch of our report on the use of face
recognition technology in which they put
the FBI in the hot seat over its lack of trans-
parency and oversight. We’ve seen action in
Vermont, Maryland, and New York, includ-
ing an introduction of a comprehensive bill
in Maryland.

But so that we don’t end on too opti-
mistic of a note, I want to make two quick
points about where this technology is going.
Real-time face recognition used in conjunc-
tion with body cameras is coming—it’s al-
ready in use in the UK. The company who
deploys it in the UK has a contract here to
use it with dash cams. Think about this—
real-time face recognition where the final ar-
biter of the algorithmic match is not
somebody sitting behind a desk who has the
time and training to evaluate whether the
algorithm is right or not. It’s an officer in the
field with a weapon, who has a moment’s de-
cision to make on whether he’s faced with a
threat to public safety and to draw his gun.
What if the algorithm is wrong?

China is very aggressively deploying face
Continued on page 12
How the government is watching you—and what you can do about it

The Age of Surveillance

Most people believe that they have some fundamental right to privacy—but how can anyone achieve privacy in an age when people are constantly surveilled by ever-more-sophisticated technology, on phones, GPS devices, surveillance cameras, and more? At the 2017 Cato Surveillance Conference, experts, policymakers, technologists, and civil society advocates gathered to discuss the state of surveillance and what can be done to stop the erosion of Americans’ privacy. Rep. Ted Lieu (D-CA) delivered the opening remarks, recalling that his Taiwanese parents came to America precisely because America was a country where citizens had no need to fear their own government. Lieu warned that mass surveillance programs, such as those authorized by the Foreign Intelligence Surveillance Act’s controversial Section 702, which allows the government to intercept Americans’ communications, are endangering the American dream his parents came here in search of. A series of flash talks throughout the afternoon went in-depth into surveillance techniques and how the government shields them from the public eye—through the practice of parallel construction, for example, which Sarah St.Vincent of Human Rights Watch dubbed “one of the most frightening civil liberties issues that you may never have heard of.” (See page 9). Justin Hansford of Howard University delivered the lunch keynote address, in which he reviewed the FBI’s long history of surveilling civil rights activists under the guise of targeting “extremists.” A final panel discussed what self-defense strategies citizens can employ to shield themselves from surveillance. For example, Steve Bell previewed his venture Orchid Labs, which aims to build a totally decentralized, anonymous, and surveillance-free layer of the internet by allowing users to sell their bandwidth—this way, users in countries where internet use is heavily regulated and surveilled, such as China, can purchase bandwidth from freer countries in the West, increasing global freedom and thwarting government surveillance. 

Top: Professors Andrew Ferguson and Margaret Hu, reporter Justin Jouvenal, and John Grant of Palantir Technologies; bottom: Rep Ted Lieu (D-CA) and Justin Hansford of Howard University.

Continued from page 11

recognition technology on very minor crimes. They use it not only to shame jaywalkers, but also to report that crime to the police when it occurs. The Russian government is very actively using face recognition to crack down on anti-corruption and anti-government protesters. They publish protesters’ names online and subject them to harassment if not arrest and incarceration. And then a final note on real-time surveillance: China has 200 million cameras. They’re planning to implement 400 million more in the coming years. They have real-time face recognition in a lot of these cameras. The BBC just did a report on this where they had the system enroll the face of one of their correspondents, and he was found by the face recognition system within seven minutes of walking out the door. These systems are far more advanced than what we’re seeing in the United States today. But without restrictions, without laws in place to limit these systems, without transparency, without public knowledge about this, these systems are being deployed, and there are very few practical limitations on a U.S. agency deciding to purchase them.