GEOLOCATION SURVEILLANCE ROUNDTABLE

SUMMARY

The University of Texas at Austin's Center for Media Engagement and the Surveillance Technology Oversight Project (S.T.O.P.) hosted a roundtable about mass surveillance in the age of mass protest. We analyzed how electronic surveillance is used to monitor political protest, mass gatherings, and how location tracking enables microtargeting of propaganda and political messaging. The roundtable took place under Chatham House Rules, thus quotes remain anonymous.

The event occurred in two sessions which took place on Feb. 11th, 2021, and were moderated by Joel Carter, Albert Fox Cahn, and Dr. Eleni Manis. Experts who participated came from various professional fields including, but not limited to: Surveillance, public policy, journalism, intelligence, law, technology, academia, digital activism, and human rights.

Q1: "What surveillance technologies are most concerning or top-of-mind and why?"

- *"Government use of facial recognition technology is the most concerning because of its bias against [people of color]."*

- *"High altitude aerial surveillance and how it is increasingly becoming a threat because it is becoming cheaper and more and more precise."*

- *"Any surveillance [that is] offered as a service for people, like Ring doorbells, and the scale it is done."*

- *"The fact that these facial recognition technologies and surveillance technologies are becoming normalized and integrated into society (like going to the doctor or entering buildings) is most concerning because they become no longer shocking."*

- *"Our data is collected in ways that create disparate impacts and track all our movements."*

- Persuasive technologies or those capable of tracking and changing human behavior.

- The partnering of government actors and private enterprises.

- Utilization of biometric data to predict search behavior or expose search history.

Q2: "Do you think the use of drones and other electronic surveillance tools at last summer's protests against police violence are a departure from historical norms?"

- *"Surveillance tools are used to maintain systems of power, and now we see them used in a more covert way."*

- *"Surveillance technology] has been used against marginalized communities for decades, but what changed is all of a sudden, groups not historically surveilled are [becoming] aware of this technology used to surveil them."*

- *"We did see a somewhat similar militarization of technologies being deployed to gather information en masse and to track participation, so it is not new."*

  - *"The amount of data being collected is frightening because we have seen how bad the abuses by the government can get."*

- *"[During the protests I thought] these helicopters are absolutely here to terrorize the people of this city right now. And having been part of some serious security apparatuses in my life, I was shocked by it to the point that I was like we get it, it's a show of force."*

- o *"I think one of the biggest problems is the lack of adequate checks and balances because the same tools in a certain set of political actors' hands could be used to protect and serve but at the same time are completely exploitable."*

- *"When you have agency heads, half of the time they blow off Congress and when they do show up, they provide misleading information, although it's a felony to lie to Congress – nothing happens. That should really worry a lot of us because it's quite a problematic situation to be in for our democracy and Congress has let it happen for a long time. So, they bear responsibility as well, not just the Executive branch."*

- *"Really, the only oversight we have of the intelligence community is Congress. There is the Inspector's General, but they aren't given the independence nor authority to be able to conduct tough oversight. Those agencies' mission is abuse, Congress is the one with the authority to look at [oversight]."*

  - o *"There's no enforcement mechanism, unfortunately. I think there are a lot of people in Washington who believe that Congress is not a co-equal branch of government."*

- Tactics employed by the Trump Administration, like the removal of the Inspector General, authorization of DEA to monitor protests, and the complete show of military aggression against protestors was new.

Q3: "What are the key levers of change for surveillance at the local, state, and federal level?"

- *"General transparency measures meant to protect us from government overreach and provide information to citizens are just simply disrespected. If we are going to allow the use of these technologies, we need to demand that accountability be urgent."*

  - o *"There should not be a cat and mouse game around [accountability] that's why legislation like the POST Act in New York is so important. But it strikes me that the government has to be accountable for us to trust it to any [surveillance technology]."*

- *"What are the [accountability] mechanisms other than Congress? [redacted] The most dreaded request was briefing Congress [redacted] because Congress was the leakiest organization – journalists protect information better than Congress does. So, I hear what you're saying [redacted] but going to Congress – you might as well be spilling your secrets publicly."*

- *"Congress is very leaky and I think part of the problem with that is not disclosing things to the public but [rather] the very politicized nature in which these disclosures take place -- it's so narrow. It's just to score a point against the [political] adversary and sometimes that can have the effect of disclosing secrets that shouldn't be necessary. How do we move away from this highly politicized system? [It's] a very systemic problem."*

    o *"Do we strengthen the Inspector's General? I have to say the Inspector's General is a kind of joke. The President picks them. Do you think the heads of agencies are going to dig into things that will be embarrassing to the administration? Of course not."*

    o *"FOIA is another [accountability] mechanism but it has no teeth, [so] there's really no oversight."*

- *"It's kind of like the War on Drugs, the extent to which unauthorized leaks are happening is a reflection of how much the formal channels have broken down and are not functioning. No leaker wants to put themselves at risk, they'd much rather go through the formal process and I've had so many people who have disclosed things who went through the formal process and it didn't work and [whistleblowing] is a last resort."*

- *"When I go to DC and I talk to insiders on privacy and surveillance they say, 'It's fine if Uncle Sam wants to spy on me, but those sociopaths in Silicon Valley would sell their mother for a nickel' and then I when I go to Silicon Valley, people say, 'Google just wants to show me better ads, who cares about that?'"*

    o *"You see from leaks from the Pentagon that they over-procured equipment so that it could be declared as surplus and delivered through the 1033 Program to local law enforcement. We ask ourselves, how is it that Orange County has all these planes and Dirtboxes just flying a pattern of Disneyland 24/7? It didn't come out of a tax raise; it came out of this model where money was effectively laundered from lobbyists in the defense industry."*

- *"Individual defensive measures will always be relied upon to combat surveillance even if surveillance gets more pervasive. People don't know how much they are being surveilled, but it's impressive how modern protesters are aware of what surveillance measures to take to protect themselves like leaving phones at home, wearing masks, etc."*

- Law enforcement guardrails – legislative bills should not dismiss facial recognition's impact on communities on color, their misidentification, or over-criminalization.

- Agency executives and their vendors are the only voices heard in making key decisions about whether certain technologies are appropriate for the community. So, it's important that policies are enforceable and that elected officials can be held accountable.

- Litigators have had luck with the 4th amendment in state court and there's optimism for corporate entities, like Apple, to instate measures aimed to protect consumers.

Q4: "What is your opinion of the 'Facial Recognition and Biometric Technology Moratorium Act of 2020?'"

- *"To me the biggest question, in terms of regulation and oversight is 'How do we get legislation that covers both of those groups, both public agencies within government and private industry?'"*

  - *"To me there isn't a huge distinction between these huge firms and what the federal government does because again, they staff each other, one is donating to the other to fund congressional runs."*

- *"We do support moratoriums, but they should be on the federal level with concrete enforcement mechanisms because if they don't, companies and law enforcement will get around them."*

- Agencies already have so much data on people so the effect would be minimal. Pressure needs to be placed on counties and police departments using facial recognition.

- The likelihood of a federal ban is low because Biden would be unwilling to sign the bill and because of gatekeeping at the federal level.

  - Privacy advocates will also put all their eggs into one basket with this legislation despite the ability of companies to leverage their money and influence to find loopholes. This adds to the challenge of banning the technology because the more common facial recognition becomes, the harder it will be to limit it.

Q5: "Does law enforcement surveillance vary based on the ideology and demographics of protesters?"

- *"The federal government's emphasis on BLM and left-wing protestors throughout the last year as opposed to extremists who sieged the Capitol on Jan. 6th makes clear the inequity in law enforcement focus or federal apparatus."*

- *"FBI or DHS will claim they don't monitor ideology, which is their standard talking point. What we saw over the last year is Bill Barr [and] Chad Wolf explicitly saying that we are going to monitor ideology."*

    o *'What's been challenging from an oversight perspective is that a lot of the answers people give aren't factually true … We haven't had a hearing about [the Capitol attack] but I'll bet my house on it that [law enforcement] will say they couldn't monitor ideology because of First Amendment's protections."*

- *"Some groups are more targeted and surveilled than others historically. The technology itself doesn't matter, but there will be a difference in volume."*

- *"There is hypocrisy and discrepancies between how slowly insurrectionists have been arrested vs how quickly action was taken against BLM protesters."*

Q6: "Should facial recognition play a role to identify Capitol attackers on January 6, 2021?"

- *"This is a really hard question, one I dealt with personally. I spent [redacted] hours reviewing [redacted], all publicly available video. The platform I was using to do it had some basic facial recognition technologies. Luckily for me, I wasn't forced with an ethical decision to use it because the platform wasn't set up for this type of video, but it was there."*

    o *"It's necessary to figure out who was involved in a crime; however, it strikes me that right now, we can't trust authorities to use these things because we can't trust that they'll be accountable for it."*

- Humans did more to identify individuals than did facial recognition technology by analyzing footage, capturing a face, and using tools to identify where else the face appears in the footage.

- *"From a democratic point of view, I think that language matters. One of the frustrations is that I've seen language saying 'this attack would have disrupted the peaceful transfer of power. The reality is that it did, and people should be talking about it that way. The impeachment trial was talking about that [and so should the public]."*

  - *"I think we're looking for technical solutions by asking these questions when we should be asking why the FBI hasn't found the people who planted bombs. Instead, we are asking if these technologies can help solve crimes."*

- *"The irony here is that we're talking about facial recognition to identify people who stormed the capitol, but it was all on social media. This wasn't surveillance from the government, it was surveillance from Facebook. It's amazing that I get a notification saying my face appeared in an image when it's [miniscule]."*

  - Is it considered law enforcement if Facebook's technology is being used to identify individuals?

- *"There is a private stakeholder that will lobby for [facial recognition] and there is a public stakeholder that will support those lobbying efforts. If we ask the question how facial recognition is able to be used by a dominant social media platform with 2.6 billion users, then how do we start the public private use of it? Maybe it's useful to rewind and say how did we sit back and watch a platform buy its way to 2.6 billion users and roll out a technology that has profound implications for privacy and democracy without so much as a hearing?"*

- *"Facial recognition wasn't necessarily the key in arresting people at the insurrection. The most evidence was from people posting on Facebook or Twitter."*

  - Facial recognition was crowdsourced, which is an inherent problem.

- The average person in Russia can use apps to scan faces and recognize people and it has led to malevolent usage.

  - Example of an anti-abortion group that would write down license plates and try to dox them. This could happen if facial recognition becomes available to everyone.

Q7: "How does surveillance facilitate targeted political messaging, campaigning, or geopropaganda?"

- *"None of this is new, whether domestic or foreign. The idea that the Russians would use the cheapest possible tools to engage in information warfare is not new. The fact that we've given these technologies so cheaply and with no oversight or transparency to any political operative because people want their Pepsi vs. Coca-Cola ads and don't care what it does to political discourse or voter suppression is terrifying."*

- *"This rise to conspiratorial vulnerability is more direct experience of actual conspiracy or corruption. Big tech makes it easy to find people who have been traumatized or target vulnerable people and does so using the same mechanism to target people who need to hear your message about why BLM or why gender is not a binary. That mechanism by which we formulate groups more cheaply is the motif of big tech."*

  - Material conditions make conspiracies attractive which experts believe needs to be addressed. Living through corruption or trauma ripens peoples' vulnerabilities to conspiracies because it creates material explanations which shapes the official mechanism by which we learn what is true.

  - In the mindset of Anti-vaxxers/conspiracists: Why trust the vaccine when big pharma, which is corrupt, has close ties to its regulators? I know this because I witnessed the Sachler family get richer than the Rockefellers from marketing OxyContin.

- *"I don't think we see so broadly at the moment in the next 1-3 years but certainly in the next 3-10 years. It seems to me a big problem potentially as language models like GPT-3 or other mechanisms to automatically generate very persuasive content that's hyper-targeted to individuals across any modality, whether sound or text."*

- *"Conspiracies have been around for a while, but the materials used to convince people are more apparent and more efficient – the technology has become advanced enough to make the message more direct and more immersive therefore making it more efficient."*

- *"Facebook was specifically recommending political groups after the platform said they wouldn't do that."*
    - Groups of people who didn't vote at all weren't receiving any recommendations.
    - Reinforcing system built on how much Facebook knows about a person.
- *"The Clinton campaign set up [PokeStop](#), where you pay people to go and it raises a point of location data being used to make people more politically involved."*
- *"The challenge is understanding the extent to which this creates vulnerabilities which is difficult to answer because policy is behind the innovation."*
- The point of protesting is to be public and legible to other people and political actors to say something matters. Unfortunately, the messaging is not legible to different actors in the same way.
    - Political actors receive BLM messaging differently than law enforcement does.

Q8: "Last thoughts or comments?"

- *"There needs to be a focus on how you shift power to find ways communities and individuals can empower themselves."*
- *"The responsibility of people in corporations is advocating for data minimization and privacy by design. You can't lose control of info you're not collecting and not retaining. It's important to understand what data you actually need to reach the goal you're trying to achieve."*
- *"It's important to consider the civil rights issues laid out in the use of these technologies, especially as they emerge and include People of Color at the table. Who is included in the design process? What are the individuals making the decisions to launch the technology?"*
- *"We cannot pick and choose when to apply technologies or have a wishy-washy approach because the cost is too high for communities that are already vulnerable."*
- Decentralization is both powerful and dangerous, and the internet showed us this.