Privacy Advocates Are Sounding Alarms Over Coronavirus Surveillance

Benjamin Powers

March 23, 2020

As the coronavirus pandemic spreads across Asia, nations leveraged significant surveillance networks to trace the virus's spread and forced governments around the world to weigh the trade-offs of public health and privacy for millions of people. Now, recent reports say the U.S. government is in talks with controversial surveillance and data gathering companies to enlist them in addressing the coronavirus crisis, signaling an escalation in the use of surveillance tools.

Last week the Wall Street Journal reported the Centers for Disease Control (CDC) enlisted Palantir, a data scraping and modeling behemoth that works with law enforcement and other government security agencies, to model outbreak data. Palantir and Clearview AI, the facial recognition startup that acquired billions of facial images through public web scraping, have been in contact with state governments about tracking people who came in contact with infected individuals.

See also: In Fight Against Coronavirus, Governments Face Trade-Offs on Privacy

The reports caused alarm among privacy advocates who, while noting the need to address the public health crisis, worry about the companies that are being pulled in to help.

"During times of crisis, civil liberties are most at risk because the normal balance of safety versus privacy becomes tilted toward safety," says Michele Gilman, a privacy lawyer and fellow at Data & Society, a think tank that studies the social impact of data-centric tech.

"A major concern is that new surveillance technologies deployed during the coronavirus crises will become the 'new normal' and permanently embedded in everyday life after the crisis passes. This can result in ongoing mass surveillance of the population without adequate transparency, accountability or fairness," she said.

There is a precedent for this, and from not long ago. The 9/11 terrorist attacks in 2001 led to an expansion of surveillance cameras and networks across the U.S. and the Patriot Act, a federal law that removed legislative guardrails to government surveillance and decreased transparency, accelerating the National Security Agency's intrusive and massive surveillance capabilities later revealed by whistleblower Edward Snowden. Despite the public backlash against the NSA's practices, lawmakers have yet to de-authorize it.

"AMBIGUOUS POLICIES AROUND WHAT HAPPENS TO THE DATA COLLECTED AFTER ITS INTENDED USE... RIP AWAY CONTROL AND TRANSPARENCY FOR PEOPLE."

“Many of the directives implemented as part of the Patriot Act led to the abuses that were exposed by Snowden,” says Steven Waterhouse, the CEO and co-founder of Orchid Labs, a privacy focused VPN company. “What abuses will we learn about later, after this crisis has passed? What legislation will be rammed through the government during this time of crisis?”

Things that may now be considered mundane, such as an abundance of surveillance cameras, being subjected to full body screens at the airport and the idea that we are constantly being observed, weren’t always the case. Often, public crises provide opportunities for surveillance architecture to move forward and become normalized fixtures of society. and create commercial opportunities for tech companies to provide new and ever more intrusive ways of tracking individuals.

That’s the case with Clearview AI, a facial recognition startup that claims to have scraped billions of public images off the web and created software that can identify a face within seconds. It markets itself to law enforcement within the U.S. but also targeted authoritarian regimes around the world with records of human rights abuses as part of a rapid expansion plan, according to documents obtained by Buzzfeed News. The company has also overstated the effectiveness of its technology, claiming police departments solved cases after using it when that was not the case. The company now faces legal challenges from other companies, and state governments.

“Clearview has a pretty consistent pattern of not being forthcoming about information but also intentionally misleading their clients in my view,” says Clare Garvie, senior associate at the Georgetown University Law Center's Center on Privacy and Technology. “Whatever means the government implements or various state and local governments implement to combat the spread of this virus must be the least intrusive means possible. What Clearview AI is proposing is not the least intrusive means possible.”

Extensive research shows facial recognition is not equally accurate on everyone.

“Facial recognition is notoriously inaccurate for women and people of color,” says Gilman. “Given this, why would we adopt such technologies to battle coronavirus? Moreover, we need much more information on how these technologies are effective in battling a global pandemic.”

China has facial recognition systems that detect elevated temperature, while South Korea has tracked people using cell phone data and locations of financial transactions.

Palantir, meanwhile, has extensive contracts with law enforcement and has little to no transparency about its practices unless you’re a customer. In a rare user manual for law enforcement obtained by Vice in 2019, the program Palantir Gotham is said to be in use at law enforcement centers that target data sources including day care centers, email providers and traffic accidents for data that builds profiles of suspects, and their friends, family and business associates.

The company was co-founded by Peter Thiel, the liberatarian billionaire who was also an early investor in Facebook. Privacy advocates have reason to fear his motives. In a 2009 essay for the Cato Institute, a libertarian think tank in Washington, D.C., Thiel wrote that “most importantly, I no longer believe that freedom and democracy are compatible.”

Public-Private

If privacy experts seem skeptical of companies like Clearview AI and Palantir, this is perhaps one reason why.

“Creating public-private partnerships to share sensitive data in times of crisis, such as a terrorism attack or a pandemic, brings short-term benefits but has an alarming impact on data privacy long after the emergency passes,” says Raullen Chai, CEO of IoTeX, a Silicon Valley company that develops privacy-protecting smart devices using blockchain.

“Ambiguous policies around what happens to the data collected after its intended use, as well as subjective triggers of ‘emergency-only’ practices, rip away control and transparency for people.”

Experts recognize the fundamental need to address immediate consequences of the coronavirus pandemic, but there is skepticism Clearview AI or Palantir would offer the required transparency and least intrusive approach.

Garvie worries about crisis profiteering. “It’s the use of fear to market surveillance tools,” says Garvie. “I just caution anyone considering contracting for these tools to make sure the decision is not being driven by the supplier, by the company, using the crisis to push through unnecessary surveillance mechanisms.”