Big Brother is being increasingly outsourced to Silicon Valley, says report

Immigrant and privacy activists are detailing the involvement of big tech–especially Amazon–with the military, ICE, and local law enforcement.

[Photo: Michael Aleo/Unsplash]

BY SEAN CAPTAIN 3 MINUTE READ

The federal and local governments have long relied on private companies for defense and law enforcement technologies, from Lockheed Martin

jetfighters to Booz Allen Hamilton data analysis. But increasingly, the government is expanding beyond the usual defense contractors to the company that also provides free shipping and online TV.

“The . . . thing that was shocking for me was to understand just how the federal authorizations are allowing Amazon to have such a monopoly over the storage of government information,” says Jacinta Gonzalez, field organizer for immigrant advocacy group Mijente. Along with the National Immigration Project and the Immigrant Defense Project, Mijente funded a new report entitled, “Who’s Behind ICE?: The Tech and Data Companies Fueling Deportations.”

Its findings are based on documents such as contracts, memoranda, and corporate financial reports–which are publicly available but take a lot of digging to decipher. (We’ve asked Amazon for feedback on the accuracy of the report, but have yet to receive a response.)

Related: How tech workers became activists, leading a resistance movement that is shaking up Silicon Valley

---

While Amazon plays the leading role, the report also details the involvement of companies including Peter Thiel's Palantir, NEC, and Thomson Reuters in storing, transferring, and analyzing data on both undocumented residents and U.S. citizens. The U.S. government is moving its databases from federal facilities to cloud providers, especially Amazon Web Services (AWS), raising concerns about accountability.

"There is a transfer of discretion and power from the public sector to the private sector in the form of these contracted technological services," says Shankar Narayan, director of the Technology and Liberty Project at the ACLU in Washington State, which was not involved in the report. Based in Seattle, Narayan tracks Amazon's growing role in law enforcement, such as its facial recognition tech of disputed accuracy, called Rekognition.

Groups like Mijente draw attention to the extent of data gathering used by federal Immigration and Customs Enforcement (ICE) and local law enforcement. “People on the ground have been more and more [saying to us] ‘How do they have information about my taxes?’ How do they have information about where I drive my car?'” says Gonzalez.

She’s also seen, and experienced, the gathering of biometric data in public. “When I was working in New Orleans back in 2013 and 2014 . . . ICE was stopping anyone that looks Latino,” claims Gonzalez. “And they were handcuffing them and fingerprinting them using mobile biometric devices.”

Gonzalez herself, a Mexico-born U.S. citizen, was transferred to immigration custody after being arrested at a March 2016 civil disobedience protest against then-candidate Donald Trump in Phoenix, where she now works. (She refused to provide information to authorities after her arrest to clarify her legal status.)

Last November, Mijente joined other organizations in a lawsuitdemanding that ICE provide information on its abandoned plans for a series of immigration raids in several US cities called “Operation Mega.”

ICE has a mandate to enforce US immigration law, but it’s faced widespread condemnation for tactics including the separation of families at the US border. Gonzalez charges hypocrisy in how ICE uses its substantial technological tools. “They have technologies to be able to surveil you,” she says. “But somehow they can’t keep track of your children when they’re being separated from you and ripped out of your arms.”

Mistrust of how governments use technology and data is exacerbated by a lack of transparency, say activists. “I think we’ve raised that concern, for example, around face surveillance,” says Narayan. “It’s remote, it’s undetectable, it could be ubiquitous, and the government doesn’t even have to really determine who they’re going to follow around in advance.” But there’s reason to fear that this surveillance will extend beyond

immigration enforcement and crime-fighting, he says, pointing to a history of political surveillance from civil rights leaders in the 1960s to New York City Muslim communities after 9/11.

Getting information is even harder now that the technology and data are in private hands, he claims. “That’s the dynamic that makes these technologies hard to even detect, let alone to put some standards of accountability around,” says Narayan. “You don’t get to crack open that black box, because these entities will use trade secret [protections], will use the Computer Fraud and Abuse Act to prevent entities from coming in and testing [their] products.”

“We’re really getting past the point of no return in terms of our ability to put safeguards in place to hold these large corporations accountable,” he says.

ABOUT THE AUTHOR

Sean Captain is a Bay Area technology, science, and policy journalist. Follow him on Twitter@seancaptain. More