FACTSHEET: THE DANGERS OF BIDEN'S TECH WALL

The Biden administration’s proposed U.S. Citizenship Act of 2021 aims to add DHS funding for border surveillance technology and infrastructure, both at and between ports of entry. This factsheet explains why “smart border” tech is an extension of the Trump administration’s border infrastructure buildup, not a break with it. And while the bill promises oversight and performance evaluations, the provisions fall far short of protecting the most vulnerable communities and continues the rapid expansion of the most dangerous federal agencies, including ICE and CBP.

I. Tech Wall May Be More Lethal and Expansive than a Physical Wall

At ports of entry, increased surveillance technology means more biometric collection, including expanded facial recognition and DNA collection, as well as experimental technologies like iris scanning at pedestrian border crossings. The ongoing DHS buildout of its new HART biometric database means that this biometric data will be accessible to all major federal law enforcement agencies and some foreign governments via information sharing agreements. The rapid expansion of license plate recognition technology used by CBP and other federal agencies is a major privacy concern.

Meanwhile, virtual wall technology between ports of entry is not a “humane” alternative to a physical wall. In fact, it has been shown to be even more dangerous, in a number of important ways:

- **Individuals detected by “smart” border technology, when apprehended by CBP or other law enforcement, find themselves caught up in the immigration enforcement dragnet, often in CBP and ICE jails that the United Nations has called out for inhumane conditions. The Biden administration already directed the Department of Justice to end private prison contracts, but privatized facilities are much more prevalent at immigration facilities, housing the majority of detainees.**

- **Increased border surveillance technology leads to more deaths, as migrants take longer, more dangerous routes to avoid detection. Peer-reviewed research has shown that there is “significant correlation between the location of border surveillance technology, the routes taken by migrants, and the locations of recovered human remains in the southern Arizona desert.” U.S. Border Patrol reported finding the remains of more than 250 migrants who died along the U.S.-Mexico border in 2020 alone.**
• The harms of border technology go far beyond the border and disproportionately impact Black, indigenous, and people of color communities, as demonstrated by CBP drones deployed on Black Lives Matter protesters last summer. Border enforcement policies have long served as a testing ground for military grade surveillance at the border and far into the interior.

II. The Tech-Border-Industrial Complex

Border surveillance is a for-profit industry. It is being pushed by companies with financial ties to both the Biden and former Trump administrations and clock thousands of lobby visits to Congress each year.¹ From FY 2017-20, CBP alone received $743 million from Congress for tech and surveillance.² In FY 2021, DHS received more than $780 million from Congress for the same. Below are examples of the technologies deployed by CBP:

• **Anduril Industries** builds mobile sentry towers. The company was founded by billionaire Trump donor Palmer Luckey with funding from Palantir’s Peter Thiel. The company was awarded a **contract** by CBP in July 2020 for a potential $250 million to set up over 200 mobile surveillance towers along the Southwest and Northern borders. These towers use sensors and AI software that distinguishes humans from animals, and relays data to drones and the CBP cloud. **Google AI** software is being used in relation to these surveillance towers. This technology forms the backbone of the new virtual wall.

• **Elbit Systems** is an Israeli company that builds and maintains the fixed surveillance towers along the U.S.-Mexico border under a contract worth up to $239 million through October 2022. Elbit Systems supplies the Israeli army with drones used in surveillance and attacks on Palestinians in Gaza. Pension funds in Norway, Holland, Sweden and the UK, as well as financial institutions like HSBC and AXA, have **divested** from the company in response to human rights concerns. The Biden administration’s border plan calls for investment in fixed towers, and CBP released a series of initial industry solicitations for the development of an updated system in 2022, along both the Southwest and Northern U.S. borders.

• **Venntel and mobile surveillance**: Venntel is a commercial data broker which stores and sells the **mobile location data** of millions of American’s cell phones. CBP uses software from Venntel for phone location tracking as well as mobile forensics software from Grayshift and Cellebrite to hack people’s phones including journalists, lawyers and activists. CBP conducts these invasive searches **without warrants**.

---


• **Drones** manufactured by Anduril, Lockheed Martin, FLIR Systems, AeroVironment and General Dynamics have also been used to patrol the border. **Autonomous drones** are currently in development as well, and Lockheed Martin has long provided surveillance blimps. Flir Systems has developed **thermal imaging technology**, and CBP purchases **sensor and camera systems** to complement the larger elements of the border surveillance system. Many of these companies contributed large amounts to both the Democratic and Republican presidential campaigns in 2020. During **Black Lives Matter protests** last year, CBP deployed these drones on marchers in multiple cities.

• **Palantir Technologies** operates key case management systems at ICE that were used in conjunction with CBP to **track down and prosecute families** of migrant children under the Trump administration. Palantir technology is also used by federal immigration authorities for ICE’s **tipline** and **workplace raids**. Palantir was founded by Peter Thiel, who remains its majority owner. Thiel was a major contributor to the 2016 Trump campaign and installed key people in the administration.

• Personal vehicles have become a subject of heightened surveillance at the border, airports, and beyond. CBP uses **automated license plate reader software** from **Vigilant Solutions**, which shares and compiles data from law enforcement across the country. Furthermore, the companies **MSAB** and Berla have partnered to provide **vehicle forensic software** that hacks cars’ infotainment systems to track “recent destinations, favorite locations, call logs, contact lists, SMS messages, emails, pictures, videos, social media feeds, and the navigation history of everywhere the vehicle has been.”

III. **Tech enforcement provisions of the U.S. Citizenship Act give DHS unlimited and unchecked resources to build a sprawling surveillance apparatus**

While Biden’s proposed immigration bill is in some ways a promising shift from the Trump administration’s racist policies, the bill’s surveillance technology provisions grant extreme latitude to DHS to construct a dangerous, unchecked, and unprecedented surveillance of the southern border region. ICE and CBP continue to operate as rogue agencies, and the Biden bill will push their massive expansion of surveillance technology into overdrive. Moreover, the bill provides little community accountability and oversight over the technology. We cannot trust that those agencies will show restraint or respect the privacy interests of residents, migrants, or anyone else in the southern border region and beyond.

Specifically, our concerns with the U.S. Citizenship Act bill include:

• **It allows the massive expansion of border surveillance technology in the U.S.** by using immigrants and border communities predominantly low-income and Latinx individuals as the test subjects and political justification for expanded government surveillance. This would extend the Trump Administration’s racist policy goals.
• The bill gives DHS a blank check, authorizing the agency to receive and spend any amount of money deemed necessary, without limits on spending.³

• The bill provides no definition for “smart border” technology and no limitation on the deployment of such technology. Given DHS’s existing practices, we can expect that DHS will take a broad definition of ports of entry as well as deploy such technology beyond ports of entry and far into the interior.

• The bill has a hollow oversight section.⁴ It provides for review by the DHS Office of the Inspector General, but does not authorize the OIG to block, interrupt, or order removal of invasive or wasteful technology. Evaluations of the privacy impacts, efficacy, and cost-effectiveness of authorized new technologies are so vague that they are meaningless; the Border Patrol is free to radically expand surveillance tech at any price as long as it relates to the murky goal of “situational awareness” at the border. Moreover, prior work of the OIG suggests a preference for tech enforcement solutions based on deterrence value and that the office may not be a proper oversight body.⁵

• The evaluation metrics throughout the border sections of the bill are stacked against tech privacy and human impact. Metrics focus on the “effectiveness” of border security operations, migrant deterrence, and cost-efficiencies, not the quality of life of border residents, civil rights abuses, or migrant safety. Such performance measures would reward exactly the wrong outcomes: DHS’s ability to make border crossings more difficult and dangerous, and the agency’s capacity to detain and deport more people.

• The bill requires no meaningful input from people who will be impacted by increased surveillance. Although border communities exposed to the dangers of new surveillance tech are mentioned as stakeholders to be “consulted”,⁶ the bill provides no meaningful opportunities for them to alter or limit new programs.

We call on the Biden administration to invest in border communities, not invasive tech and border militarization. Communities along the U.S.-Mexico border have some of the highest poverty rates in the country due to systemic disinvestment. They have already been the subject of extreme militarization and mass surveillance including interior checkpoints, drones, blimps, mobile and fixed surveillance towers, and other cameras and sensors placed in communities. Instead of pouring billions more into invasive surveillance and military technology that only harms immigrants and enriches private companies, the Biden administration should listen to the needs of border communities, address ongoing harms, and invest in communities.


⁴ U.S. Citz. Act § 2303.

⁵ Since at least 2017, DHS OIG has found that CBP fails to assess the efficacy of its technologies. Despite CBP’s continued failure to create metrics to evaluate tech, the OIG states that funding for CBP technology is too constrained. See supra 2, at 23; see also Angela Chan, “How Far Has Technology Come Since the Last ‘Smart Border’ Failed?,” The Verge, Feb. 22, 2019.

⁶ U.S. Citz. Act § 2303(3).