# Biometric Technology Center

8-10 minutes

---

Excerted from "First Platoon," Annie Jacobsen

Biometric Technology Center, Clarksburg, West Virginia

On April 10 , 2020 , the U.S . Department of Health and Human Services entered into a no-bid contract with Palantir Technologies to track the spread of the coronavirus. HHS is a cabinet-level, executive branch organization whose 2021 budget ($1.427 trillion ) is more than twice that of the Defense Deprtment ($705.4 billion ). The goal of the HHS Protect Now program, said its spokesman, is to " bring disparate data sets together and provide better visibility to HHS on the spread of COVID."

HHS confirmed the data that Palantir is now mining includes "diagnostic testing data; geographic testing data; [and] demographic statistics," meaning information about individual American citizens' health, location, family, and tribe. The initial HHS announcement said Palantir would be given access to 187 data sets. That number has since grown to 225. Unknowns abound: What data is going into the Palantir system, how is it shared, with whom, and for how long?

"Given how tight-lipped both HHS and Palantir have been over the program, we don't fully know," says Lauren Zabierek, executive director of the Cyber Project at Harvard Kennedy School's Belfer Center. Zabierek is a former U.S . Air Force officer who also served as a civilian analyst with the National Geospatial-Intelligence Agency, in three war zones, including in Kandahar in 2012. "I sincerely hope that HHS Protect Now will do nothing resembling finding and fixing certain entities," she says, using military nomenclature for locating and killing IED emplacers in the war zone. "I hope that [the data sets] will only be used to understand the spread of the virus in the aggregate."

As for Palantir, the privately held company seems to enjoy mythologizing the controversial nature of its work, its origins, and its founder, Peter Thiel. A large banner on the front page of the company website reads: "How a â€˜Deviant' Philosopher Built Palantir, a CIA-Funded Data-Mining Juggernaut," an homage to the title from a Forbes magazine article from 2013. For Americans, to

adopt a "nothing to hide, nothing to fear" mindset ignores the reality that HHS has previously shared sensitive, personal information with federal law enforcement agencies.

In 2018, HHS's Office of Refugee Resettlement allowed ICE to access confidential data files it had collected on migrant children, their family members, and potential sponsors after the federal government took the position that it needed this information to enforce the nation's immigration laws. To promote rule of law. Ten weeks into the Protect Now program, a group of lawmakers wrote to HHS Secretary Alex Azar to express concern. "Unfortunately, HHS data has been misused before by federal law enforcement officials ... We are concerned that, without any safeguards, data in HHS Protect [Now] could be used by other federal agencies in unexpected, unregulated, and potentially harmful ways."

In a separate letter, members of the Congressional Hispanic Caucus were a little more blunt: "We have valid concerns on whether the existing surveillance framework Palantir has created to track and arrest immigrants will be supplemented by the troves of potentially personal health information contained within the HHS Protect [Now] platform."

It is the merging of disparate government databases into a giant monolith that has privacy experts concerned." As nations enter into agreements to share biometric databases for military defense, foreign intelligence, and law enforcement purposes, the multinational cybersurveillance implications of biometric data collection and data analysis are likely to expand," warns Hu.

Shades of this merger are beginning to appear. Inaugurated in 2018, the Biometric Technology Center in West Virginia became the first joint biometric initiative between the Defense Department and the Justice Department to have its own physical building on U.S. soil. "With the opening of the BTC, the DoD and FBI will be able to work in collaboration to carry out operations and technical innovations to identify threatening or dangerous individuals," an army official said.

The DoD's Defense Forensics and Biometrics Agency covers one-sixth of the 360,000-square-foot biometrics center; five-sixths of the center belongs to the FBI. And it is here where so many of the government's big-data systems are housed. What does the ABIS machine actually look like? I wondered. This secretive behemoth, built of biometric data captured from millions of people in Iraq, Afghanistan, and elsewhere. Repeated requests to tour the facility, and to see ABIS with my own eyes, were denied.

I asked Tom Bush about ABIS and its almost mythical stature." Lockheed built ABIS from old parts in the basement, and it still sits in the basement of CJIS," said Bush. "Lockheed built it because they built us," he said, meaning the FBI's database. "But DoD is a mess. So many holes. There's no standard biometrics collection like with CJIS. There should be a CJIS [a Criminal Justice Information Services Division] at DoD. There is not. This is what we argued back in '05, in '06. DoD has [what] is called a biometric gap. No one can get through the labyrinth."

Gaps and labyrinths. Vacuum-like spaces and mazes into which critical information can fall. A database that so few have access to, and even fewer understand, with information that can be improperly used to influence a decision made by the president of the United States. These are dangerous areas of operation in the complex geospatial terrain known as rule of law.

As it stands now, in the criminal- justice system, individual humans are the backbone of the rule of law. In the systems of law enforcement, courts, and corrections, the humans still matter most. It is a human who commits the crime. A human who pulls the trigger or plants the IED. A human who finds the smoking gun. Automated machines do the grunt work, but humans solve the puzzle. The process itself is like a labyrinth.

Using science to solve crimes is thousands of years old, taking into account ancient autopsies and medieval toxicology reports. Using forensic biometrics to solve crimes has been part of the criminal justice system for 129 years, starting when Francisca Rojas left a bloody fingerprint on a doorway in 1892. The next twenty years of this century will almost certainly be transformative, taking leaps never before imagined.

A year 2020-2025 broad agency announcement, for advanced technology development programs for the army's Special Operations Command, provides a glimpse at what warfighting might be like in coming years. In this future operating environment, so-called hyper-enabled operators, or HEOs, will have systems on their bodies that allow for " persistent near- real-time collection" of biometric data to identify friend or foe. Fingerprint capture will be touchless, meaning the Pentagon's electronic systems will read people's ridges, whorls, and loops from "extended distances" without their awareness or consent. Soldiers will carry "rapid, portable, handheld DNA collection and processing [devices ] for matching against authoritative databases." Translation: Dr. Selden's microwave -size, rapid DNA system will soon be the size of an iPhone, allowing for on-the-spot DNA checks.

One technology being pursued gave me pause: a "handheld, manpackable [machine] with holographic capabilities." The Pentagon aims to have its hyper-enabled operators carry a device that has "the ability to project images that are not real but seem real, and have the ability to develop personalized message campaigns for the image to project." In other words, three-dimensional deepfakes, to trick the enemy in real time.

As it stands now, scientists have developed ways to identify what a person might look like from micrograms of captured DNA. Advances to build full-scale models of a person's probable identity from the gene up are ongoing. Add into the mix additional identity information from ear shape to vein pattern, voice, gait, and skeletal frame and this realistic-looking, soldier-projected hologram of a person is meant to be misinterpreted as the real person, the one with the true identity. How much further will it go? What will society become? Will humans still recognize who and what the real villains really are?

---