Peter Thiel’s data-mining company is using 'War on Terror tools' as excuse to track American citizens. The scary thing? Palantir is desperate for new customers.

By Peter Waldman, Lizette Chapman, and Jordan Robertson

High above the Hudson River in downtown Jersey City, a former U.S. Secret Service agent named Peter Cavicchia III ran special ops for JPMorgan Chase & Co. His insider threat group—most large financial institutions have one—used computer algorithms to monitor the bank’s employees, ostensibly to protect against perfidious traders and other miscreants.

Aided by as many as 120 “forward-deployed engineers” from the data mining company Palantir Technologies Inc., which JPMorgan engaged in 2009, Cavicchia’s group vacuumed up emails and browser histories, GPS locations from company-issued smartphones, printer and download activity, and transcripts of digitally recorded phone conversations. Palantir’s software aggregated, searched, sorted, and analyzed these records, surfacing keywords and patterns of behavior that Cavicchia’s team had flagged for potential abuse of corporate assets. Palantir’s algorithm, for example, alerted the insider threat team when an employee started badging into work later than usual, a sign of potential disgruntlement. That would trigger further scrutiny and possibly physical surveillance after hours by bank security personnel.

Featured in *Bloomberg Businessweek*, April 23, 2018. Subscribe now.

Over time, however, Cavicchia himself went rogue. Former JPMorgan colleagues describe the environment as Wall Street meets*Apocalypse Now*, with Cavicchia as Colonel Kurtz, ensconced upriver in his office suite eight floors above the rest of the bank’s security team. People in the department were shocked that no one from the bank or Palantir set any real limits. They darkly joked that Cavicchia was listening to their calls, reading their emails, watching them come and go. Some planted fake information in their communications to see if Cavicchia would mention it at meetings, which he did.

It all ended when the bank’s senior executives learned that they, too, were being watched, and what began as a promising marriage of masters of big data and global finance descended into a spying scandal. The misadventure, which has never been reported, also marked an ominous turn for Palantir, one of the most richly valued startups in

Silicon Valley. An intelligence platform designed for the global War on Terror was weaponized against ordinary Americans at home.

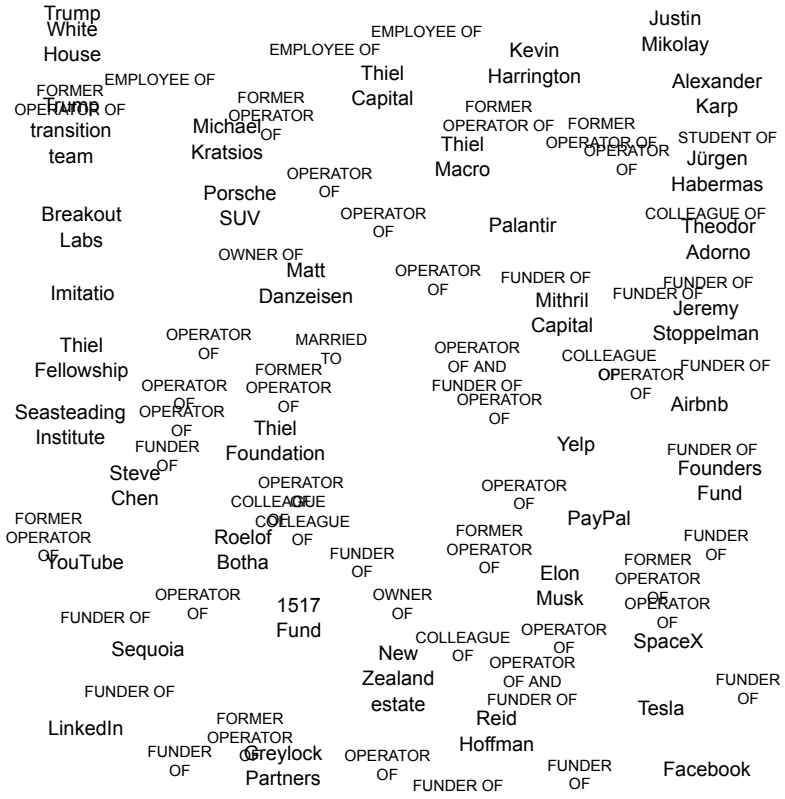
Founded in 2004 by Peter Thiel and some fellow PayPal alumni, Palantir cut its teeth working for the Pentagon and the CIA in Afghanistan and Iraq. The company's engineers and products don't do any spying themselves; they're more like a spy's brain, collecting and analyzing information that's fed in from the hands, eyes, nose, and ears. The software combs through disparate data sources—financial documents, airline reservations, cellphone records, social media postings—and searches for connections that human analysts might miss. It then presents the linkages in colorful, easy-to-interpret graphics that look like spider webs. U.S. spies and special forces loved it immediately; they deployed Palantir to synthesize and sort the blizzard of battlefield intelligence. It helped planners avoid roadside bombs, track insurgents for assassination, even hunt down Osama bin Laden. The military success led to federal contracts on the civilian side. The U.S. Department of Health and Human Services uses Palantir to detect Medicare fraud. The FBI uses it in criminal probes. The Department of Homeland Security deploys it to screen air travelers and keep tabs on immigrants.

Police and sheriff's departments in New York, New Orleans, Chicago, and Los Angeles have also used it, frequently ensnaring in the digital dragnet people who aren't suspected of committing any crime. People and objects pop up on the Palantir screen inside boxes connected to other boxes by radiating lines labeled with the relationship: "Colleague of," "Lives with," "Operator of [cell number]," "Owner of [vehicle]," "Sibling of," even "Lover of." If the authorities have a picture, the rest is easy. Tapping databases of driver's license and ID photos, law enforcement agencies can now identify more than half the population of U.S. adults.

JPMorgan was effectively Palantir's R&D lab and test bed for a foray into the financial sector, via a product called Metropolis. The two companies made an odd couple. Palantir's software engineers showed up at the bank on skateboards. Neckties and haircuts were too much to ask, but JPMorgan drew the line at T-shirts. The programmers had to agree to wear shirts with collars, tucked in when possible.

As Metropolis was installed and refined, JPMorgan made an equity investment in Palantir and inducted the company into its Hall of Innovation, while its executives raved about Palantir in the press. The software turned "data landfills into gold mines," Guy Chiarello, who was then JPMorgan's chief information officer, told *Bloomberg Businessweek* in 2011.

The founder of Palantir is extremely well connected. Here's how his life might appear in the company's model.


Trump
White
House
EMPLOYEE OF
EMPLOYEE OF
Kevin
Harrington
Justin
Mikolay
EMPLOYEE OF
Thiel
Capital
Alexander
Karp
FORMER
OPERATOR OF
Trump
transition
team
FORMER
OPERATOR
OF
Michael
Kratsios
FORMER
OPERATOR OF
Thiel
Macro
FORMER
OPERATOR OF
OPERATOR
OF
STUDENT OF
Jürgen
Habermas
OPERATOR
OF
Porsche
SUV
Breakout
Labs
OPERATOR
OF
Palantir
COLLEAGUE OF
Theodor
Adorno
OWNER OF
Matt
Danzeisen
OPERATOR
OF
FUNDER OF
FUNDER OF
Mithril
Capital
FUNDER OF
Jeremy
Stoppelman
Imitatio
Thiel
Fellowship
OPERATOR
OF
MARRIED
TO
OPERATOR
OF AND
FUNDER OF
COLLEAGUE
OF
FUNDER OF
OPERATOR
OF
OPERATOR
OF
FORMER
OPERATOR
OF
OPERATOR
OF
Airbnb
Seasteading
Institute
OPERATOR
OF
Thiel
Foundation
FUNDER
OF
Yelp
FUNDER OF
Founders
Fund
Steve
Chen
OPERATOR
OF
COLLEAGUE
OF
COLLEAGUE
OF
OPERATOR
OF
PayPal
FORMER
OPERATOR
OF
Roelof
Botha
YouTube
FUNDER
OF
FORMER
OPERATOR
OF
FUNDER
OF
Elon
Musk
OPERATOR
OF
OPERATOR
OF
OPERATOR
OF
1517
Fund
FUNDER OF
OWNER
OF
Sequoia
COLLEAGUE
OF
OPERATOR
OF
SpaceX
New
Zealand
estate
OPERATOR
OF AND
FUNDER OF
FUNDER OF
FUNDER
OF
Tesla
LinkedIn
FORMER
OPERATOR
OF
Reid
Hoffman
FUNDER
OF
Greylock
Partners
OPERATOR
OF
FUNDER OF
FUNDER
OF
Facebook


Yelp
Thiel Fellowship
YouTube
Breakout Labs
Seasteading Institute
Funder of
Operator of
Imitat
Operator of
Sequoia
Former operator of
Operator of
Funder of
Funder of
Jeremy Stoppelman
Funder of
Operator of
Thiel Foundation
Trump transition team
Former operator of
Steve Chen
Roelof Botha
LinkedIn
Former operator of
Employee of
Colleague of
Colleague of
Colleague of
Operator of
Matt Danzeisen
Michael Kratsios
Funder of
Former operator of
1517 Fund
Former operator of
Funder of
Married to
Operator of
Employee of
Greylock Partners
Operator of
Reid
Colleague of
Operator of
Thiel Capital
Operator of
Em
Funder of
Colleague of
Former operator of
Funder of
Funder of
Operator of
Thiel Macro
Operator of
Former operator of
Kevin Harrington
Elon Musk
Former operator of
PayPal
Funder of
Palantir
Funder of
Facebook
Tesla
Operator of
Operator of
Mithril Capital
Former operator of
Jus
SpaceX
Operator of
Operator of
Theodor Adorno
Miko
Funder of
Funder of
Alexander

Chart: Dorothy Gambrell

Cavicchia was in charge of forensic investigations at the bank. Through Palantir, he gained administrative access to a full range of corporate security databases that had previously required separate authorizations and a specific business justification to use. He had unprecedented access to everything, all at once, all the time, on one analytic platform. He was a one-man National Security Agency, surrounded by the Palantir engineers, each one costing the bank as much as $3,000 a day.

Senior investigators stumbled onto the full extent of the spying by accident. In May 2013 the bank's leadership ordered an internal probe into who had leaked a document to the *New York Times* about a federal investigation of JPMorgan for possibly manipulating U.S. electricity markets. Evidence indicated the leaker could have been Frank Bisignano, who'd recently resigned as JPMorgan's co-chief operating officer to become CEO of First Data Corp., the big payments processor. Cavicchia had used Metropolis to gain access to emails about the leak investigation—some written by top executives—and the bank believed he shared the contents of those emails and other communications with Bisignano after Bisignano had left the bank. (Inside JPMorgan, Bisignano was considered Cavicchia's patron—a senior executive who protected and promoted him.)

JPMorgan officials debated whether to file a suspicious activity report with federal regulators about the internal security breach, as required by law whenever banks suspect regulatory violations. They decided not to—a controversial decision internally, according to multiple sources with the bank. Cavicchia negotiated a severance agreement and was forced to resign. He joined Bisignano at First Data, where he's now a senior vice president. Chiarello also went to First Data, as president. After their departures, JPMorgan drastically curtailed its Palantir use, in part because "it never lived up to its promised potential," says one JPMorgan executive who insisted on anonymity to discuss the decision.

The bank, First Data, and Bisignano, Chiarello, and Cavicchia didn't respond to separately emailed questions for this article. Palantir, in a statement responding to questions about how JPMorgan and others have used its software, declined to answer specific questions. "We are aware that powerful technology can be abused and we spend a lot of time and energy making sure our products are used for the forces of good," the statement said.

Much depends on how the company chooses to define good. In March a former computer engineer for Cambridge Analytica, the political consulting firm that worked for Donald Trump's 2016 presidential campaign, testified in the British Parliament that a Palantir employee had helped Cambridge Analytica use the personal data of up to 87 million Facebook users to develop psychographic profiles of individual voters. Palantir said it has a strict policy against working on political issues, including campaigns, and showed Bloomberg emails in which it turned down Cambridge's request to work with Palantir on multiple occasions. The employee, Palantir said, worked with Cambridge Analytica on his own time. Still, there was no mistaking the implications of the incident: All human relations are a matter of record, ready to be revealed by a clever algorithm. Everyone is a spidergram now.

Thiel addresses the 2016 Republican National Convention. JIM WATSON/AFP/GETTY IMAGES

Thiel, who turned 50 in October, long reveled as the libertarian black sheep in left-leaning Silicon Valley. He contributed $1.25 million to Trump's presidential victory, spoke at the Republican convention, and has dined with Trump at the White House. But Thiel has told friends he's had enough of the Bay Area's "monocultural" liberalism. He's ditching his longtime base in San Francisco and moving his personal investment firms this year to Los Angeles, where he plans to establish his next project, a conservative media empire.

As Thiel's wealth has grown, he's gotten more strident. In a 2009 essay for the Cato Institute, he railed against taxes, government, women, poor people, and society's acquiescence to the inevitability of death. (Thiel doesn't accept death as inexorable.) He wrote that he'd reached some radical conclusions: "Most importantly, I no longer believe that freedom and democracy are compatible." The 1920s was the last time one could feel "genuinely optimistic" about American democracy, he said; since then, "the vast increase in welfare beneficiaries and the extension of the franchise to women—two constituencies that are notoriously tough for libertarians—have rendered the notion of 'capitalist democracy' into an oxymoron."

Thiel went into tech after missing a prized Supreme Court clerkship following his graduation from Stanford Law School. He co-founded PayPal and then parlayed his winnings from its 2002 sale to EBay Inc. into a career in venture investing. He made an early bet on Facebook Inc. (where he's still on the board), which accounts for most of his $3.3 billion fortune, as estimated by Bloomberg, and launched his career as a backer of big ideas—things like private space travel (through an investment in SpaceX), hotel alternatives (Airbnb), and floating island nations (the Seasteading Institute).

He started Palantir—named after the omniscient crystal balls in J.R.R. Tolkien's *Lord of the Rings* trilogy—three years after the attacks of Sept. 11, 2001. The CIA's investment arm, In-Q-Tel, was a seed investor. For the role of chief executive officer, he chose an old law school friend and self-described neo-Marxist, Alex Karp. Thiel told Bloomberg in 2011 that civil libertarians ought to embrace Palantir, because data mining is less repressive than the "crazy abuses and draconian policies" proposed after Sept. 11. The best way to prevent another catastrophic attack without becoming a police state, he argued, was to give the government the best surveillance tools possible, while building in safeguards against their abuse.

Legend has it that Stephen Cohen, one of Thiel's co-founders, programmed the initial prototype for Palantir's software in two weeks. It took years, however, to coax customers away from the longtime leader in the intelligence analytics market, a software company called I2 Inc.

In one adventure missing from the glowing accounts of Palantir's early rise, I2 accused Palantir of misappropriating its intellectual property through a Florida shell company registered to the family of a Palantir executive. A company claiming to be a private eye firm had been licensing I2 software and development tools and spiriting them to

Palantir for more than four years. I2 said the cutout was registered to the family of Shyam Sankar, Palantir's director of business development.

As shown in the pr
Facebook and Cambr
pressure to monet
companies is

I2 sued Palantir in federal court, alleging fraud, conspiracy, and copyright infringement. In its legal response, Palantir argued it had the right to appropriate I2's code for the greater good. "What's at stake here is the ability of critical national security, defense and intelligence agencies to access their own data and use it interoperably in whichever platform they choose in order to most effectively protect the citizenry," Palantir said in its motion to dismiss I2's suit.

The motion was denied. Palantir agreed to pay I2 about $10 million to settle the suit. I2 was sold to IBM in 2011.

Sankar, Palantir employee No. 13 and now one of the company's top executives, also showed up in another Palantir scandal: the company's 2010 proposal for the U.S. Chamber of Commerce to run a secret sabotage campaign against the group's liberal opponents. Hacked emails released by the group Anonymous indicated that Palantir and two other defense contractors pitched outside lawyers for the organization on a plan to snoop on the families of progressive activists, create fake identities to infiltrate left-leaning groups, scrape social

media with bots, and plant false information with liberal groups to subsequently discredit them.

After the emails emerged in the press, Palantir offered an explanation similar to the one it provided in March for its U.K.-based employee's assistance to Cambridge Analytica: It was the work of a single rogue employee. The company never explained Sankar's involvement. Karp issued a public apology and said he and Palantir were deeply committed to progressive causes. Palantir set up an advisory panel on privacy and civil liberties, headed by a former CIA attorney, and beefed up an engineering group it calls the Privacy and Civil Liberties Team. The company now has about 10 PCL engineers on call to help vet clients' requests for access to data troves and pitch in with pertinent thoughts about law, morality, and machines.

During its 14 years in startup mode, Palantir has cultivated a mystique as a haven for brilliant engineers who want to solve big problems such as terrorism and human trafficking, unfettered by pedestrian concerns such as making money. Palantir executives boast of not employing a single salesperson, relying instead on word-of-mouth referrals.

The company's early data mining dazzled venture investors, who valued it at $20 billion in 2015. But Palantir has never reported a profit. It operates less like a conventional software company than like a consultancy, deploying roughly half its 2,000 engineers to client sites. That works at well-funded government spy agencies seeking specialized applications but has produced mixed results with corporate clients. Palantir's high installation and maintenance costs repelled customers such as Hershey Co., which trumpeted a Palantir partnership in 2015 only to walk away two years later. Coca-Cola, Nasdaq, American Express, and Home Depot have also dumped Palantir.

Karp recognized the high-touch model was problematic early in the company's push into the corporate market, but solutions have been elusive. "We didn't want to be a services company. We wanted to do something that was cost-efficient," he confessed at a European conference in 2010, in one of several unguarded comments captured in videos posted online. "Of course, what we didn't recognize was that this would be much, much harder than we realized."

Palantir's newest product, Foundry, aims to finally break through the profitability barrier with more automation and less need for on-site engineers. Airbus SE, the big European plane maker, uses Foundry to crunch airline data about specific onboard components to track usage and maintenance and anticipate repair problems. Merck KGaA, the pharmaceutical giant, has a long-term Palantir contract to use Foundry in drug development and supply chain management.

Deeper adoption of Foundry in the commercial market is crucial to Palantir's hopes of a big payday. Some investors are weary and have

already written down their Palantir stakes. Morgan Stanley now values the company at $6 billion. Fred Alger Management Inc., which has owned stock since at least 2006, revalued Palantir in December at about $10 billion, according to Bloomberg Holdings. One frustrated investor, Marc Abramowitz, recently won a court order for Palantir to show him its books, as part of a lawsuit he filed alleging the company sabotaged his attempt to find a buyer for the Palantir shares he has owned for more than a decade.

As shown in the privacy breaches at Facebook and Cambridge Analytica—with Thiel and Palantir linked to both sides of the equation—the pressure to monetize data at tech companies is ceaseless. Facebook didn't grow from a website connecting college kids into a purveyor of user profiles and predilections worth $478 billion by walling off personal data. Palantir says its Privacy and Civil Liberties Team watches out for inappropriate data demands, but it consists of just 10 people in a company of 2,000 engineers. No one said no to JPMorgan, or to whomever at Palantir volunteered to help Cambridge Analytica—or to another organization keenly interested in state-of-the-art data science, the Los Angeles Police Department.

Screenshots of Palantir's Gotham program, from a promotional video. SOURCE: YOUTUBE

Palantir began work with the LAPD in 2009. The impetus was federal funding. After several Sept. 11 postmortems called for more intelligence sharing at all levels of law enforcement, money started flowing to Palantir to help build data integration systems for so-called fusion centers, starting in L.A. There are now more than 1,300 trained Palantir users at more than a half-dozen law enforcement agencies in Southern California, including local police and sheriff's departments and the Bureau of Alcohol, Tobacco, Firearms and Explosives.

The LAPD uses Palantir's Gotham product for Operation Laser, a program to identify and deter people likely to commit crimes. Information from rap sheets, parole reports, police interviews, and other sources is fed into the system to generate a list of people the department defines as chronic offenders, says Craig Uchida, whose consulting firm, Justice & Security Strategies Inc., designed the Laser system. The list is distributed to patrolmen, with orders to monitor and stop the pre-crime suspects as often as possible, using excuses such as jaywalking or fix-it tickets. At each contact, officers fill out a field interview card with names, addresses, vehicles, physical descriptions, any neighborhood intelligence the person offers, and the officer's own observations on the subject.

The cards are digitized in the Palantir system, adding to a constantly expanding surveillance database that's fully accessible without a

warrant. Tomorrow's data points are automatically linked to today's, with the goal of generating investigative leads. Say a chronic offender is tagged as a passenger in a car that's pulled over for a broken taillight. Two years later, that same car is spotted by an automatic license plate reader near a crime scene 200 miles across the state. As soon as the plate hits the system, Palantir alerts the officer who made the original stop that a car once linked to the chronic offender was spotted near a crime scene.

The platform is supplemented with what sociologist Sarah Brayne calls the secondary surveillance network: the web of who is related to, friends with, or sleeping with whom. One woman in the system, for example, who wasn't suspected of committing any crime, was identified as having multiple boyfriends within the same network of associates, says Brayne, who spent two and a half years embedded with the LAPD while researching her dissertation on big-data policing at Princeton University and who's now an associate professor at the University of Texas at Austin. "Anybody who logs into the system can see all these intimate ties," she says. To widen the scope of possible connections, she adds, the LAPD has also explored purchasing private data, including social media, foreclosure, and toll road information, camera feeds from hospitals, parking lots, and universities, and delivery information from Papa John's International Inc. and Pizza Hut LLC.

The Constitutionality Question

Why the courts haven't ruled on whether Palantir's analytical tools are legal

Civil rights advocates say the compilation of a digital dossier of someone's life, absent a court warrant, is an unlawful intrusion under the U.S. Constitution. Law enforcement officials say that's not the case. For now, the question is unsettled, and that may be no accident. Civil liberties lawyers are seeking a case to challenge the constitutionality of Palantir's use, but prosecutors and immigration agents have been careful not to cite the software in evidentiary documents, says Paromita Shah, associate director of the National Lawyers Guild's National Immigration Project. "Palantir lives on that secrecy," she says.

Since the 1970s, the Supreme Court has differentiated between searching someone's home or car, which requires a warrant, and searching material out in the open or shared with others, which doesn't. The justices' thinking seems to be evolving as new technologies rise.

In a 2012 decision, *U.S. v. Jones*, the justices said that planting a GPS tracker on a car for 28 days without a warrant created such a comprehensive picture of the target's life that it violated the public's reasonable expectation of privacy.

Similarly, the court's 2014 decision in *Riley v. California* found that cellphones contain so much personal information that they provide a virtual window into the owner's mind, and thus necessitate a warrant for the government to search. Chief Justice John Roberts, in his majority opinion, wrote of cellphones that "with all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" Justice Louis Brandeis, 86 years earlier, wrote a searing dissent in a wiretap case that seems to perfectly foresee the advent of Palantir.

"Ways may someday be developed," Brandeis warned, "by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences."
—Peter Waldman

The LAPD declined to comment for this story. Palantir sent Bloomberg a statement about its work with law enforcement: "Our [forward-deployed engineers] and [privacy and civil liberties] engineers work with the law enforcement customers (including LAPD) to ensure that the implementation of our software and integration of their source systems with the software is consistent with the Department's legal and

policy obligations, as well as privacy and civil liberties considerations that may not currently be legislated but are on the horizon. We as a company determine the types of engagements and general applications of our software with respect to those overarching considerations. Police Agencies have internal responsibility for ensuring that their information systems are used in a manner consistent with their policies and procedures."

Operation Laser has made L.A. cops more surgical—and, according to community activists, unrelenting. Once targets are enmeshed in a spidergram, they're stuck.

Manuel Rios, 22, lives in the back of his grandmother's house at the top of a hill in East L.A., in the heart of the city's gang area. Tall with a fair complexion and light hair, he struggled in high school with depression and a learning disability and dropped out to work at a supermarket.

He grew up surrounded by friends who joined Eastside 18, the local affiliate of the 18th Street gang, one of the largest criminal syndicates in Southern California. Rios says he was never "jumped in"—initiated into 18. He spent years addicted to crystal meth and was once arrested for possession of a handgun and sentenced to probation. But except for a stint in county jail for a burglary arrest inside a city rec center, he's avoided further trouble and says he kicked his meth habit last year.

In 2016, Rios was sitting in a parked car with an Eastside 18 friend when a police car pulled up. His buddy ran, pursued by the cops, but Rios stayed put. "Why should I run? I'm not a gang member," he says over steak and eggs at the IHOP near his home. The police returned and handcuffed him. One of them took his picture with a cellphone. "Welcome to the gang database!" the officer said.

Since then he's been stopped more than a dozen times, he says, and told that if he doesn't like it he should move. He has nowhere to go. His girlfriend just had a baby girl, and he wants to be around for them. "They say you're in the system, you can't lie to us," he says. "I tell them, 'How can I be in the hood if I haven't got jumped in? Can't you guys tell people who bang and who don't?' They go by their facts, not the real facts."

The police, on autopilot with Palantir, are driving Rios toward his gang friends, not away from them, worries Mariella Saba, a neighbor and community organizer who helped him get off meth. When whole communities like East L.A. are algorithmically scraped for pre-crime suspects, data is destiny, says Saba. "These are systemic processes. When people are constantly harassed in a gang context, it pushes them to join. They internalize being told they're bad."

In Chicago, at least two immigrants have been detained for deportation by Immigration and Customs Enforcement officers based on erroneous information in gang databases, according to a pair of federal lawsuits. Chicago is a sanctuary city, so it isn't clear how ICE found out about the purported gang affiliations. But Palantir is a likely link. The company provided an "intelligence management solution" for

the Cook County Sheriff's Office to integrate information from at least 14 different databases, including gang lists compiled by state and local police departments, according to county records. Palantir also has a $41 million data mining contract with ICE to build the agency's "investigative case management" system.

One of the detained men, Wilmer Catalan-Ramirez, a 31-year-old body shop mechanic, was seriously injured when six ICE agents burst into his family's home last March without a warrant. He'd been listed in the local gang database twice—in rival gangs. Catalan-Ramirez spent the next nine months in federal detention, until the city of Chicago admitted both listings were wrong and agreed to petition the feds to let him stay in the U.S. ICE released him in January, pending a new visa application. "These cases are perfect examples of how databases filled with unverified information that is often false can destroy people's lives," says his attorney, Vanessa del Valle of Northwestern University's MacArthur Justice Center.

When whole co
algorithmically scra
suspects, data

Palantir is twice the age most startups are when they cash out in a sale or initial public offering. The company needs to figure out how to be rewarded on Wall Street without creeping out Main Street. It might not be possible. For all of Palantir's professed concern for individuals'

privacy, the single most important safeguard against abuse is the one it's trying desperately to reduce through automation: human judgment.

As Palantir tries to court corporate customers as a more conventional software company, fewer forward-deployed engineers will mean fewer human decisions. Sensitive questions, such as how deeply to pry into people's lives, will be answered increasingly by artificial intelligence and machine-learning algorithms. The small team of Privacy and Civil Liberties engineers could find themselves even less influential, as the urge for omnipotence among clients overwhelms any self-imposed restraints.

Computers don't ask moral questions; people do, says John Grant, one of Palantir's top PCL engineers and a forceful advocate for mandatory ethics education for engineers. "At a company like ours with millions of lines of code, every tiny decision could have huge implications," Grant told a privacy conference in Berkeley last year.

JPMorgan's experience remains instructive. "The world changed when it became clear everyone could be targeted using Palantir," says a former JPMorgan cyber expert who worked with Cavicchia at one point on the insider threat team. "Nefarious ideas became trivial to implement; everyone's a suspect, so we monitored everything. It was a pretty terrible feeling." *—With Michael Riley*