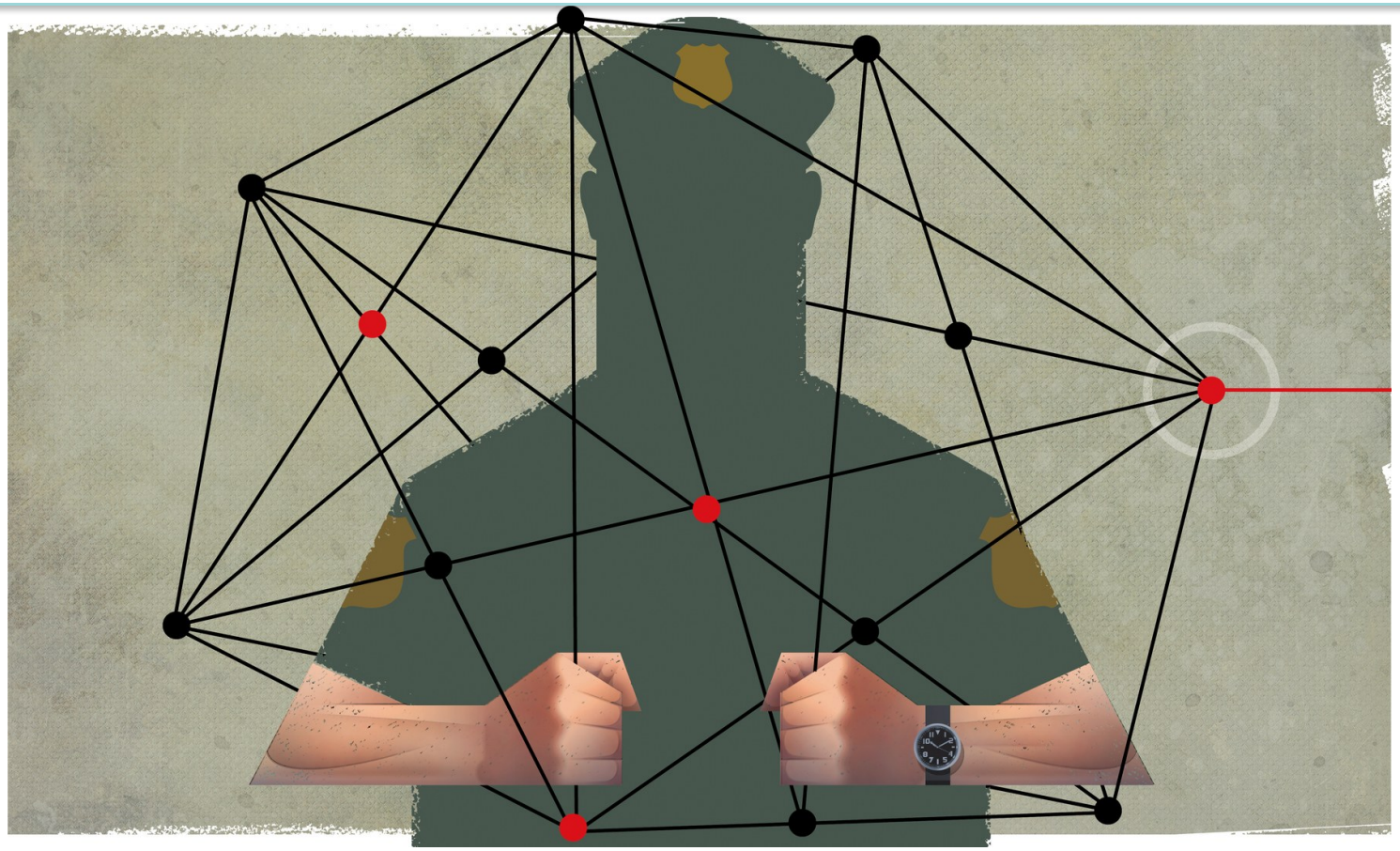


ILLUSTRATION BY VAL MINA

MARK HARRIS BACKCHANNEL 08.09.17 09:40 AM

HOW PETER THIEL'S SECRETIVE DATA COMPANY PUSHED INTO POLICING

When Sergeant Lee DeBrabander marked a case confidential in the Long Beach drug squad's Palantir data analysis system in November 2014, he expected key details to remain hidden from unauthorized users' eyes. In police work, this can be crucial—a matter of life and death, even. It often involves protecting vulnerable witnesses, keeping upcoming operations hush hush, or protecting a fellow police officer who's working undercover.

Yet not long after, someone working in the gang crimes division ran a car license plate mentioned in his case and was able to read the entire file. "Can you please look at this?" DeBrabander wrote to a Palantir engineer in an email, which was obtained by Backchannel in response to public records requests.

Palantir had been selling its data storage, analysis, and collaboration software to police departments nationwide on the basis of rock-solid security. "Palantir Law Enforcement provides robust, built-in privacy and civil liberties protections,

retention capabilities," its website reads.

But DeBrabander had a hard time getting Palantir to respond, emails show. Two weeks after he made his first complaint, his sensitive case was still an open book to other detectives at Long Beach PD. "I went over to Gangs and had them run the plate since they are not listed in our confidentiality group, and sure enough the plate was found within the narrative of the very report we want to keep tight control on," he complained in an email to Palantir. Four months later, his case was still visible to other officers, and he was still sending emails to Palantir to fix the problem.

Law enforcement accounts for just a small part of Palantir's business, which mostly consists of military clients, intelligence outfits like the CIA or Homeland Security, and large financial institutions. In police departments, Palantir's tools are now being used to flag traffic scofflaws, parole violators, and other everyday infractions. But the police departments that deploy Palantir are also dependent upon it for some of their most sensitive work. Palantir's software can ingest and sift through millions of digital records across multiple jurisdictions, spotting links and sharing data to make or break cases.

The scale of Palantir's implementation, the type, quantity and persistence of the data it processes, and the unprecedented access that many thousands of people have to that data all raise significant concerns about privacy, equity, racial justice,

BACKCHANNEL

Mark Harris is a freelance journalist reporting on technology from Seattle.

works, who is using it, and what their problems are. And neither Palantir nor many of the police departments that use it are willing to talk about it.

MORE FROM THIS EDITION

JESSI HEMPEL
How Baidu Will Win China's AI Race—and, Maybe, the World's

GABRIEL NICHOLAS
Ethereum Is Coding's New Wild West

SUSAN CRAWFORD
Jeff Bezos Should Put His Billions Into Libraries

SCOTT ROSENBERG
Bitcoin Makes Even Smart People Feel Dumb

In one of the largest systematic investigations of the company to date, Backchannel filed dozens of public records requests with police forces across America. When Palantir started selling its products to law enforcement, it also laid a paper trail. All 50 states have public records laws providing access to contracts, documents, and emails of local and government bodies. That makes it possible to peer inside the company's police-related operations in ways that simply aren't possible with its national security work.

What's clear is that law enforcement agencies deploying Palantir have run into a host of problems. Exposing data is just the start. In the documents our requests produced, police departments have also accused the company, backed by tech investor and Trump supporter Peter Thiel, of spiraling prices, hard-to-use software, opaque terms of service, and "failure to deliver products" (in the words of one email from the Long Beach police). Palantir might

high cost, for both the police forces themselves and the communities they serve.

These documents show how Palantir applies Silicon Valley's playbook to domestic law enforcement. New users are welcomed with discounted hardware and federal grants, sharing their own data in return for access to others'. When enough jurisdictions join Palantir's interconnected web of police departments, government agencies, and databases, the resulting data trove resembles a pay-to-access social network—a Facebook of crime that's both invisible and largely unaccountable to the citizens whose behavior it tracks.

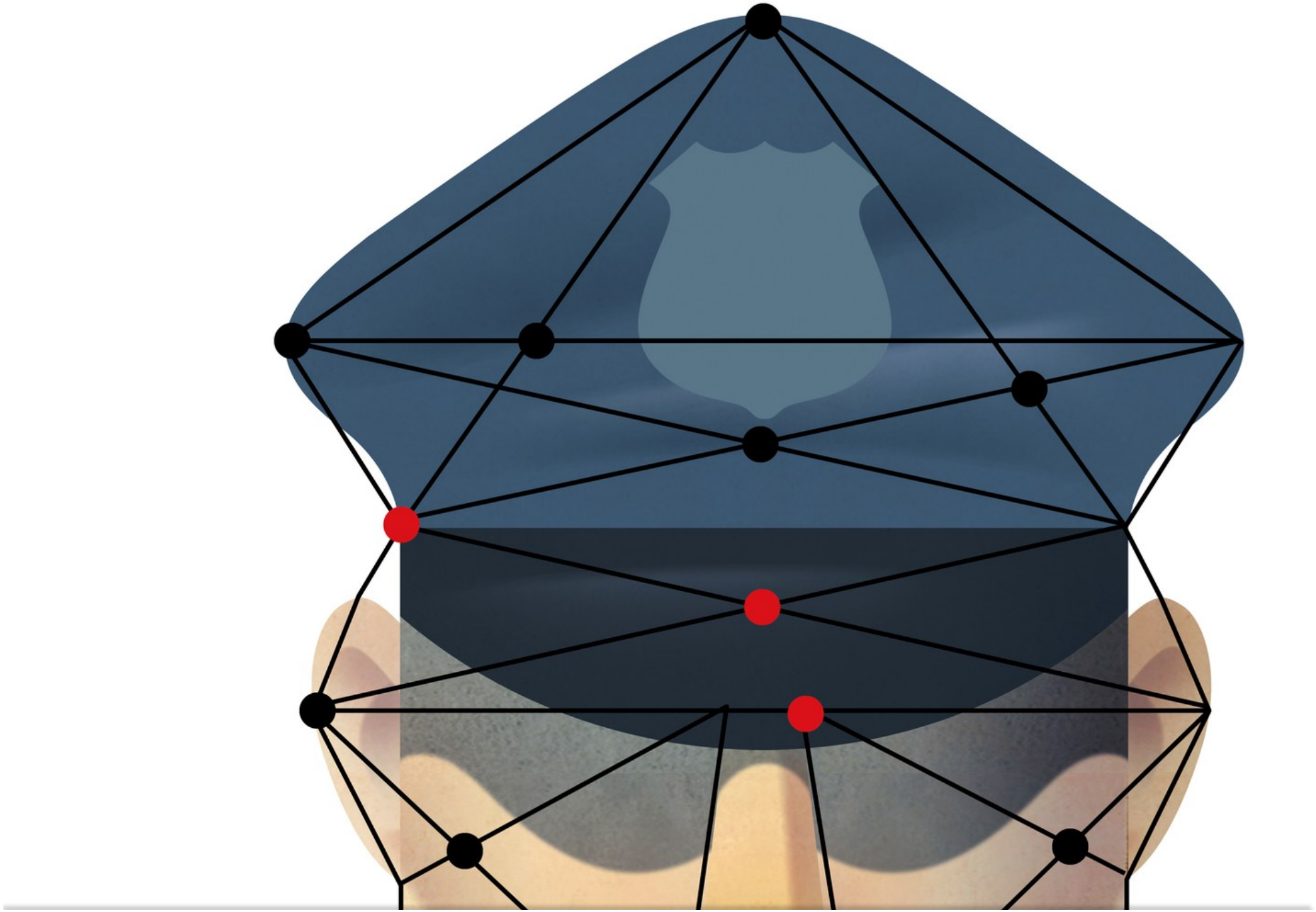
This is the story of how Palantir, despite the issues unearthed by Backchannel's investigation, came to quietly dominate the domestic law enforcement intelligence infrastructure of the US's most populous state—and how it could replicate that across the nation and around the world.

No one outside Palantir seems to know for sure how many police departments in America use its technology. (Despite multiple requests, Palantir declined to make anyone available for an interview, or to comment on any of Backchannel's findings.) The New York Police Department has certainly used it, as have Cook County sheriffs in Chicago, the Virginia State Police, the Metropolitan Police Department in Washington, D.C., and a dozen law enforcement agencies in Utah.

almost certainly paint an incomplete picture. However, they suggest that one state, California, accounts for many of the deployments—and perhaps close to 90 percent of the sales—of Palantir's systems to domestic law enforcement to date.

Palantir's software has been deployed by police departments in Los Angeles (LAPD), Long Beach (LBPD), and Burbank; sheriff's departments in Sacramento, Ventura, and Los Angeles Counties (LASD); the state's highway patrol; and homeland security "fusion centers" run by local departments in Orange County, San Francisco, Silicon Valley, San Diego and Los Angeles. Purchase orders and invoices show that these agencies have spent over $50 million with Palantir since 2009.

The first city in California to get involved was Los Angeles. In 2009, LAPD's then chief of police, Bill Bratton, wanted to test the real-time analysis and visualization of data. "We were looking for [a] tool to do a better job of visualizing our radio calls as they were coming out," remembers Sean Malinowski, then a captain but now a deputy chief at the LAPD. "Palantir partnered with us on [an] experiment to come up with [a] situational awareness tool."



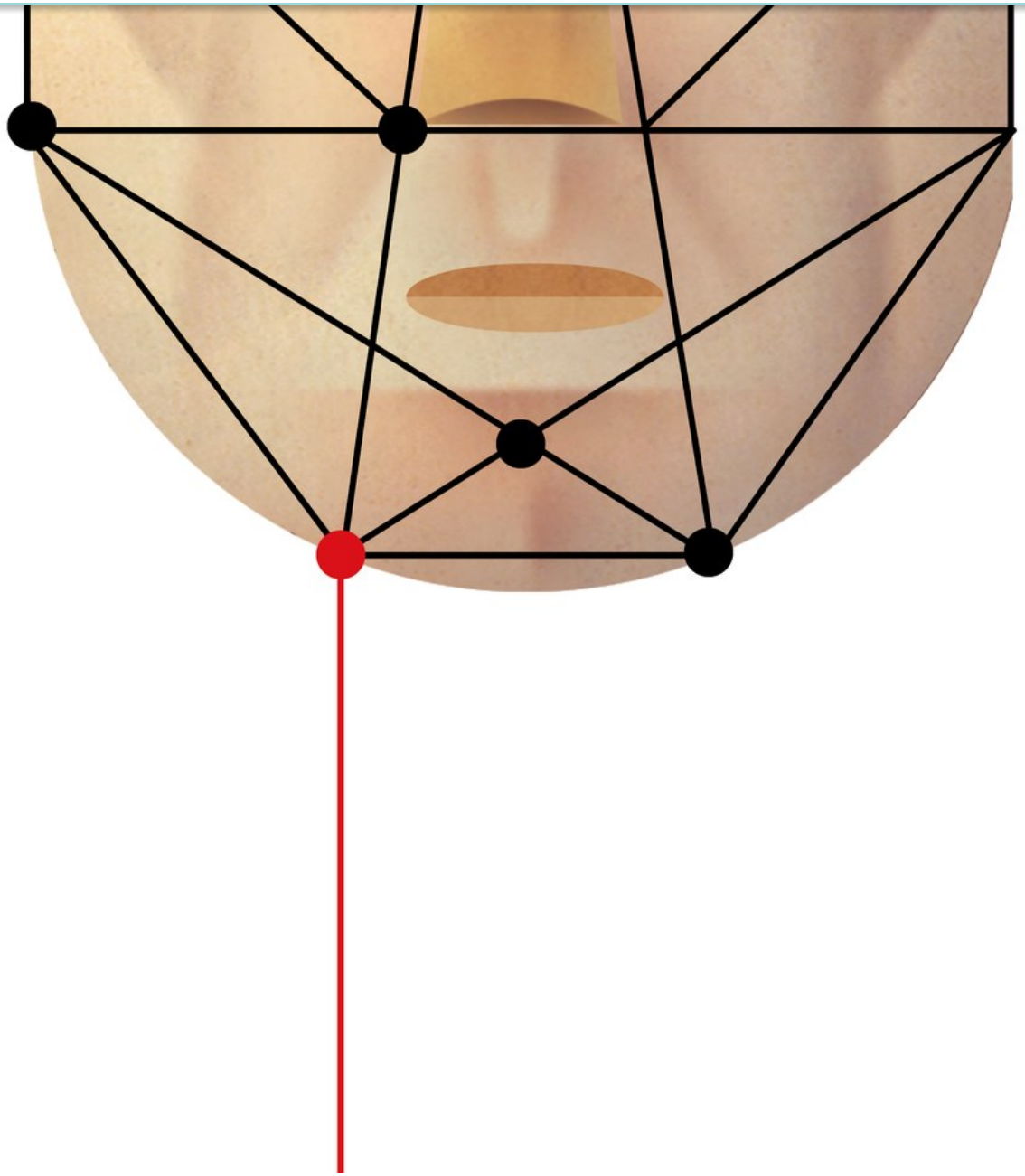


ILLUSTRATION BY VAL MINA

That pilot soon evolved into an investigative analysis platform that could access databases of crime reports and license plate information. Bratton even thought that Palantir might be just the tool for a far more ambitious program of predictive policing (the idea that historical data could provide clues to where crimes might occur in the future). He asked Craig Uchida, a consultant and researcher in data-driven policing, to draw up a plan.

"In LA, we started looking at what could be done with violent crime using data, to see where crime was emerging and what was causing it," says Uchida. "Back in 2009, the LAPD did not really focus on using data for those kinds of purposes. They had a lot of data, like all police departments do, but there wasn't a focus on how to use it and what to use it for."

Uchida was a big believer in hotspot policing: deploying officers on bike or foot to troubled areas in order to defuse tension and nip possible crimes in the bud. He proposed a project called Laser that would crunch six years of crime data to identify areas of the city with high levels of gun crime. These corridors and neighborhoods, code-named "Laser Zones," would then receive regular, high-visibility patrols.

The district chosen was Newton: nine square miles of South LA that are home to more than 40 gangs. Newton's notoriety for gun crime had earned it the nickname of "Shootin' Newton" and even a starring role in the gritty Jake Gyllenhaal cop movie *End of Watch*. In 2011, just before the Laser program began, Newton was ranked third in gun violence among LAPD's 21 divisions.

time officers stopped someone, they would fill out cards about the stop. These "field interview" cards would capture as much information as possible, from the person's name and address to the bike or car they were driving—even the tattoos they had. "Most of the time it didn't lead to anything, but it was...data that went into the system, and that's what I wanted: more data about what was happening, who they were stopping and why," says Uchida.

Back at base, analysts and officers would use that information to create so-called Chronic Offender Bulletins, identifying key individuals deemed "potential" or "probable" repeat offenders. These people then received extra attention from special units and patrols employing enhanced surveillance techniques, including license plate readers. Before Palantir, building each profile was a time-consuming job, taking about an hour for an analyst to tie together information from disparate sources. With officers in Newton stopping around 100 people each day, according to Uchida, the analysts could never keep up.

"This is where Palantir came into play," he says. Because Palantir could automatically integrate everything from citizen tips and crime incidents to field interviews and partial license plates, it dramatically accelerated the production of Chronic Offender Bulletins. What used to take an hour could be generated in three to five minutes. The analysts could now profile every single person stopped by police in Newton.

Meanwhile, a nearby agency was putting Palantir to work on an even higher profile problem: terrorism. Fusion centers are "focal points" for collecting and sharing intelligence on domestic terrorism; there are 77 of them in the continental US, with

a high-tech command center run by and sharing an office building with a bureau of the LA Sheriff's Department (LASD). The JRIC would quickly become the nucleus of Palantir's largest network of local law enforcement agencies in the country, covering Los Angeles and six other counties—nearly 40,000 square miles and 18.5 million people. Its databases would ultimately stretch far beyond terrorism, including everything from parking tickets to maps of schools.

Palantir Technologies was founded in 2004 by a group of investors and technologists including its current CEO, Alex Karp, and Peter Thiel, a billionaire who co-founded PayPal and subsequently set up a hedge fund and venture capital firm. The CIA was an early investor in the company through its In-Q-Tel venture fund, and Palantir's advisors have included Condoleezza Rice and former CIA director George Tenet. Many of Palantir's early customers were intelligence agencies and information-gathering units of the military, and the company's technology is often said (although not confirmed) to have been used in the process of tracking and killing Osama bin Laden.

That history means the company's operations have always been the opposite of transparent. But as Palantir began to work with Los Angeles and other taxpayer-

politicians, oversight boards, and the public.

Palantir's law enforcement technology is based on its Gotham platform, a system it also sells to businesses and governments to organize and analyze unstructured data like spreadsheets, reports, and emails. (Palantir's other major platform, Metropolis, is aimed at the financial and investment industries.) A promotional video supplied by the company shows LAPD officers conducting geographical searches of a neighborhood to find crimes reported there, linking those crimes to suspects, seeing mugshots, visualizing networks of gangs, and even using augmented reality of a location during an arrest.

But that is only the tip of the iceberg. Palantir offers access to a universe of digital databases that are typically inaccessible to the general public. Precisely what kinds of information its tools grant access to has been largely unknown until now. Among the documents our investigation obtained is a contract between Palantir and the LA Sheriff's Department, signed in March 2016, that details a long list of applications and software—most previously unreported—built by Palantir for the JRIC fusion center between 2010 and 2015.

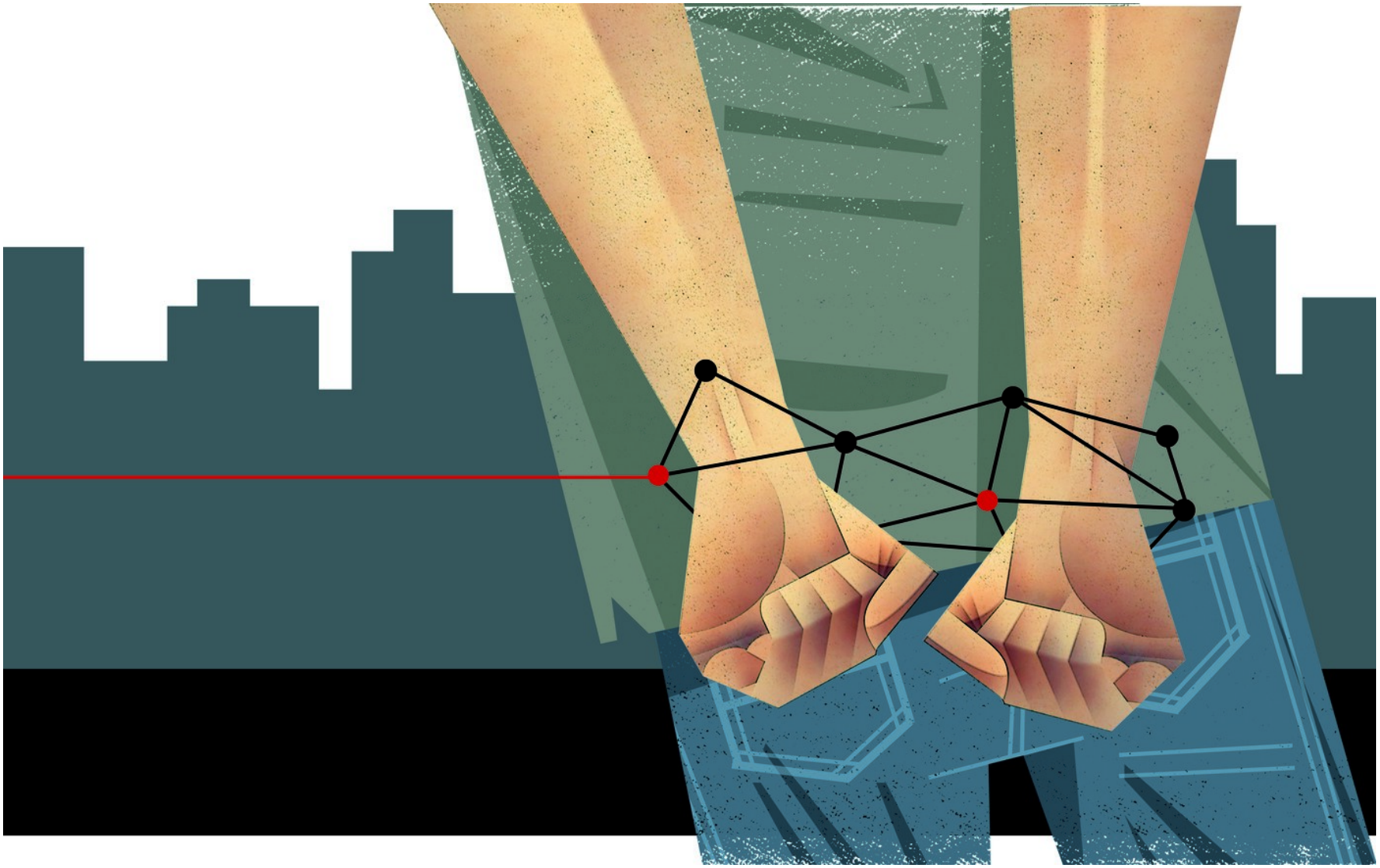


ILLUSTRATION BY VAL MINA

activity reports from across the many law enforcement agencies in the region, compare them against each other and all sources of intel...and identify links or patterns of suspicious behavior." The initial build also included instant access to millions of 911 call records, and a list of every officer on duty during every single police shift of every day.

The next year, Palantir added databases of regional crime data, field interviews, explosive-related incidents, and jail visitation records. These worked along the same lines as Palantir's intelligence tools for its military and national security customers. A much bigger change was the integration in 2011 of data from the California Law Enforcement Telecommunications System (CLETS).

CLETS used to be the primary digital tool for many officers in California. It contains criminal records and restraining orders, but also details of cars and drivers from the Department of Motor Vehicles in California and neighboring Oregon. That means that it includes millions of people outside the criminal justice system.

Once the Palantir system had incorporated the CLETS data, the floodgates opened. In 2012, Palantir added data from automated license plate readers, a download of Californian traffic citations, and links to an FBI database of terrorism-related reports. Cops could soon narrow license plate searches by area, follow inmates in custody, and even track diseases through jails—all from the mobile data terminals in their patrol cars.

"We started to sunset other applications in favor of Palantir because there wasn't another system out there that [could do] these kind of mission-critical analytic

much more.

MORE FROM THIS AUTHOR

MARK HARRIS
The Lawsuit That Could Pop Alphabet's Project Loon Balloons

MARK HARRIS
How My Public Records Request Triggered Waymo's Self-Driving Car...

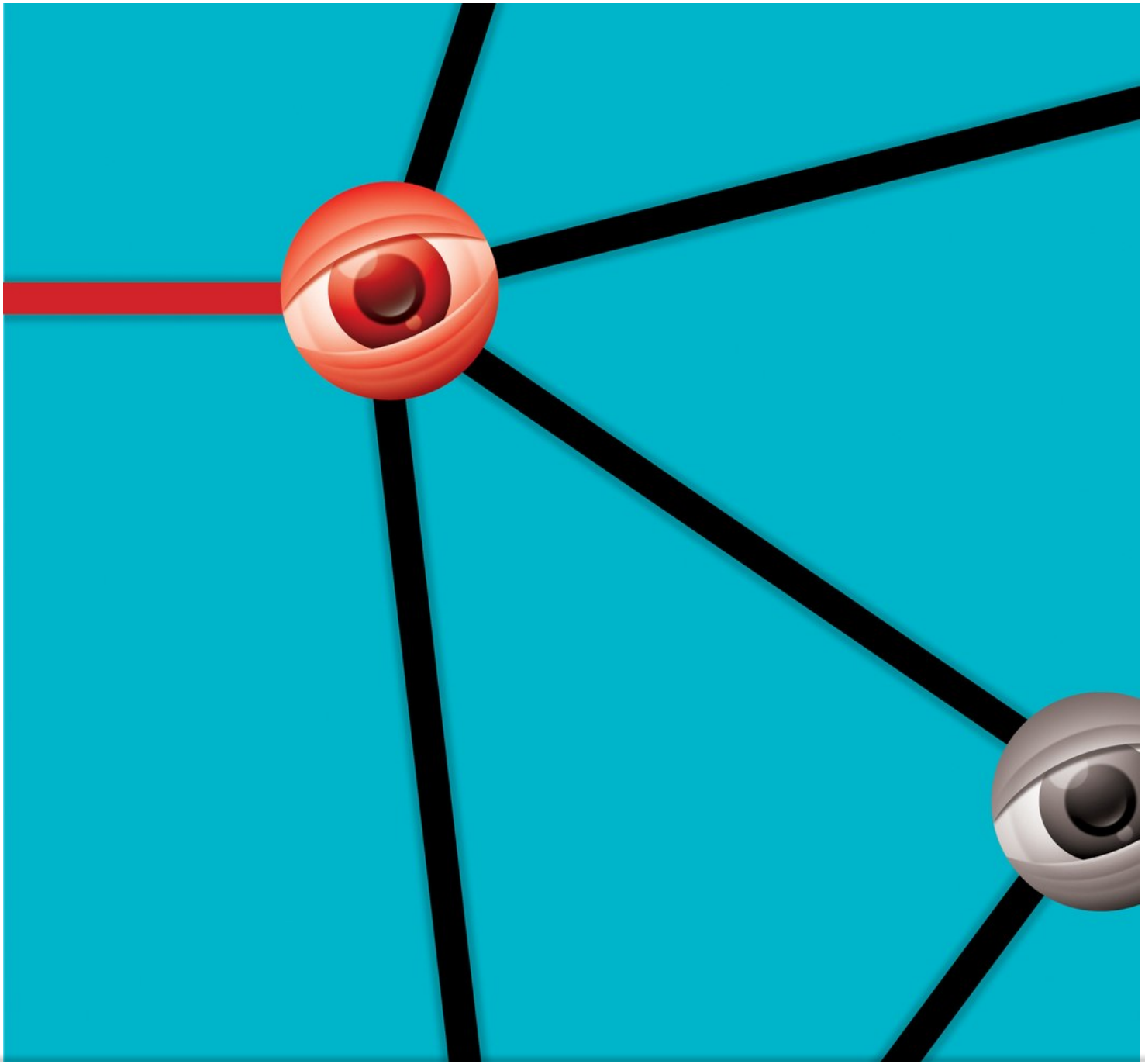
MARK HARRIS
How A Lone Hacker Shredded the Myth of Crowdsourcing

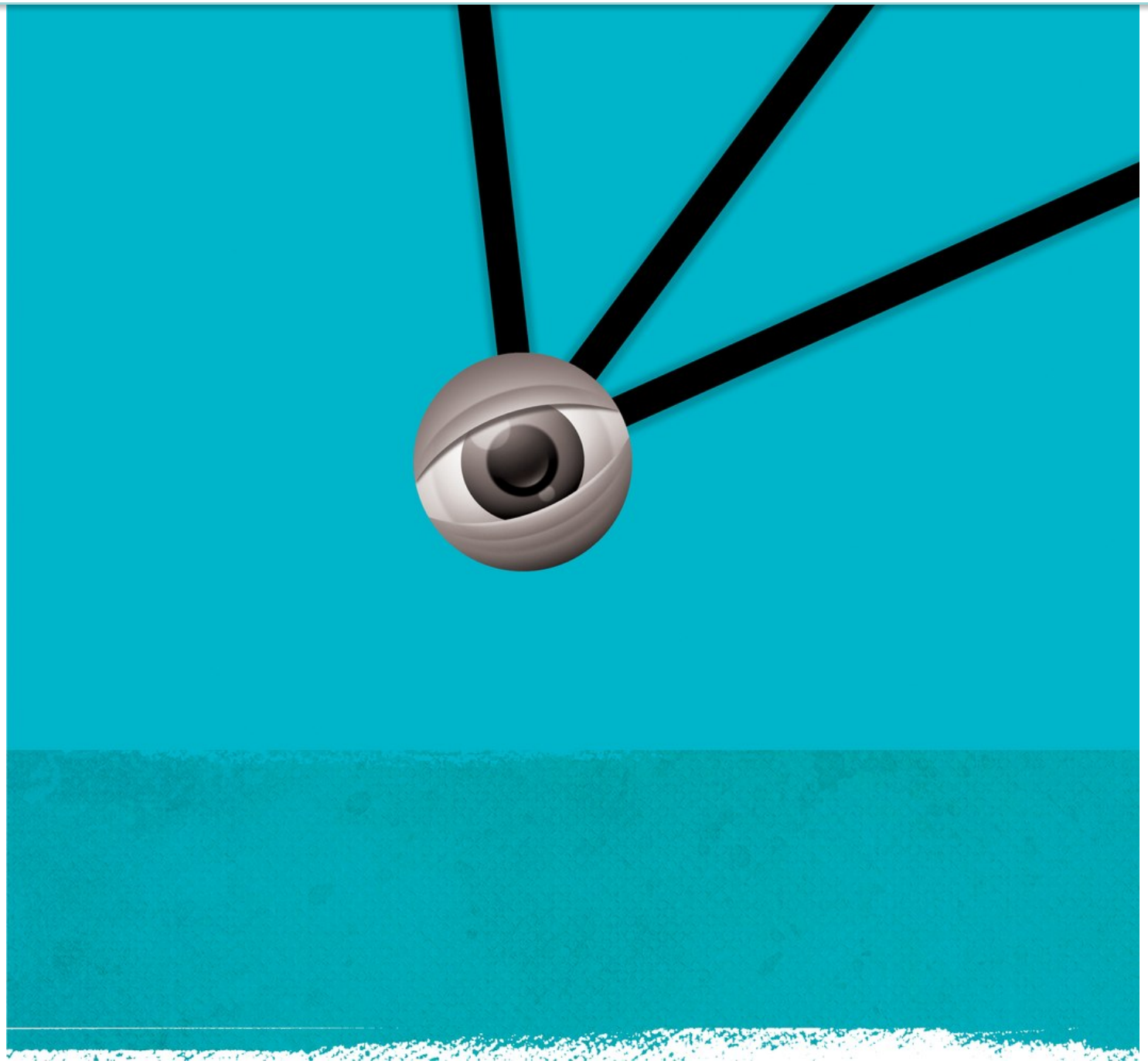
Of course, as police used Palantir more and more widely, the likelihood of screwups and misuse multiplied. In February 2013, JRIC was tasked with tracking down Christopher Dorner, an ex-LAPD officer who had embarked on a series of shootings targeting law enforcement officers. The effort involved dozens of agencies across the state. "We used Palantir extensively to address that [and] were active 24/7 until he was caught or killed," remembers Jackson. "We found that processing clues was a big challenge."

In fact, on two separate occasions, police shot at trucks misidentified as belonging to Dorner, injuring three civilians. "We said [to Palantir], 'We need an application that can span multiple units within an agency...multiple agencies within a county... and multiple counties within a state,'" says Jackson. "[They developed an application] based on lessons learned from Dorner." That application, called ClueMan, short for Clue Manager, has just gone live at JRIC.

Adding this much data to the Palantir system expanded the potential for misusing that information—as the record of other database systems suggests. With the

ex-partners, snooping on potential dates, and even trying to leak details of witnesses to the family of a convicted murderer. California's CLETS Advisory Committee reports that confirmed cases of misuse have been steadily climbing, reaching 177 in 2016. Palantir puts vastly more data than CLETS in the hands of a wider network of users.





By 2014, JRIC's system had digested so much data from so many sources (including the LAPD and LBPD) that Palantir added the ability to search by names, vehicles, keywords, locations—and even tattoos. JRIC's software platform had also ballooned: As of 2015, Palantir had built 29 applications, accessed by nearly 5,550 users at over 25 agencies. Jackson says JRIC's system now has around 12,000 users.

The applications vary in size, but some use massive data sets. An automated license plate reader database integrated into a Palantir system in a fusion center in Silicon Valley in 2012 could hold 50 million plates, with the expectation of scaling to 200 million records in the years ahead.

In fact, Palantir's systems now handle so much data that key analyses are being entirely automated. Two years ago, researchers at JRIC presented what they called a "Persistent Monitoring Feed" at a national Fusion Center training event. Their software collects data within certain geographical areas from multiple sources, and is used to provide regular, automatic intelligence updates on critical infrastructure sites—similar to how your Facebook feed scours hundreds of friends' pages to produce a rolling digest of what it thinks are the most interesting posts. With this kind of algorithmic filtering, no human need ever look at the actual raw intelligence data. But as any Facebook user knows, such filters can produce results of wildly variable quality. And in police work, bad data can be dangerous.

Even as Los Angeles and other California police departments started to become accustomed to the heady powers of Palantir's platform, they found themselves running into problems. Escalating costs would sometimes cause them to reconsider their dealings with the company. But backing away from Palantir would lead to another problem: Once you sign on with Palantir, it can be hard to sign off.

Cost containment was the biggest bone of contention. While the intelligence community's three-letter agencies typically have deep pockets to fund the Global War On Terror, domestic police departments tend to have much smaller budgets.

Early in 2015, a payment to Palantir of over $1 million rang alarm bells with LASD managers. The payment was legitimate but had been made retroactively, which was forbidden under department rules. Officials there asked its governing body, the LA County Board of Supervisors, to look into the department's relationship to Palantir. In August 2015, the Board's Auditor-Controller John Naimo produced his report, which has not previously been reported. It pulled no punches.

Naimo found that Palantir had originally been selected for a $250,000 pilot project in 2009 based solely on the recommendation of a former manager. "The Sheriff procured Palantir for JRIC without any...specifications or technical requirements describing JRIC's data analysis needs," reads his report. "As a result, we could not

needs.

According to LA County contracts, when JRIC committed to the full Palantir system in October 2011, the LASD paid around $122,000 each for 20 Palantir “cores”: packages of already-configured computer servers bundled with preinstalled software. That price was approximately $19,000 less per core than Palantir charged the federal government. According to paperwork for the pilot program, LASD received a “special discount because it [would] be the first in the LA basin to use this software.” Palantir staff indicated that the company provided JRIC a discount because it viewed working with the fusion center as a good partnership, Naimo′s report states.

Once the Palantir cores were in business, the police found themselves caught in an upgrade spiral. Naimo’s report says, “As additional law enforcement agencies… began to use the JRIC Palantir platform… and as additional data sources were added… it became necessary to purchase additional Palantir cores and servers to maintain intelligence data processing capacity and capability.” By 2016, Palantir had sold JRIC at least 115 cores, plus other services, for a total bill of just under $20 million.

John Naimo was also critical of the way Palantir sold its technology. “Palantir uses an opaque pricing model and does not discretely identify to customers the costs of software, hardware, equipment, and professional services,” he wrote. His report says that a company rep even claimed that detailed pricing information was Palantir’s “proprietary and trade secret information.” This made it virtually

they were being overcharged—especially when it came to support.

For instance, according to a letter from the LASD to the LA County Board of Supervisors in 2016, JRIC had told the LASD that all the Palantir servers were specially customized to operate its Gotham software. “The Department’s understanding was that only Palantir could provide continuous maintenance support of the hardware,” wrote Sheriff Jim McDonnell. “In late December 2015…the Department learned that all [Palantir’s hardware] is in fact comprised of standard, off-the-shelf…computer servers.”

From that point on, the letter continues, LASD took responsibility for its own hardware support. The department also requested that Palantir provide data to justify future software purchases, and threatened to bring in outside consultants to review the whole Palantir ecosystem. It might not have been able to follow through on that threat: According to a 2015 grant request by the San Diego fusion center for support of its Palantir installation, “Palantir Technologies, Inc. is the only vendor available to provide support and maintenance on Palantir’s Gotham software platform… [which] is proprietary to Palantir Technologies, Inc.”

Palantir’s customers must rely on software that only the company itself can secure, upgrade, and maintain. Although the letter noted Palantir had not provided JRIC with any of its requested (but unspecified) metrics by spring 2016, the company is set to receive annual maintenance payments of nearly $2.5 million from the fusion center through the spring of 2019.

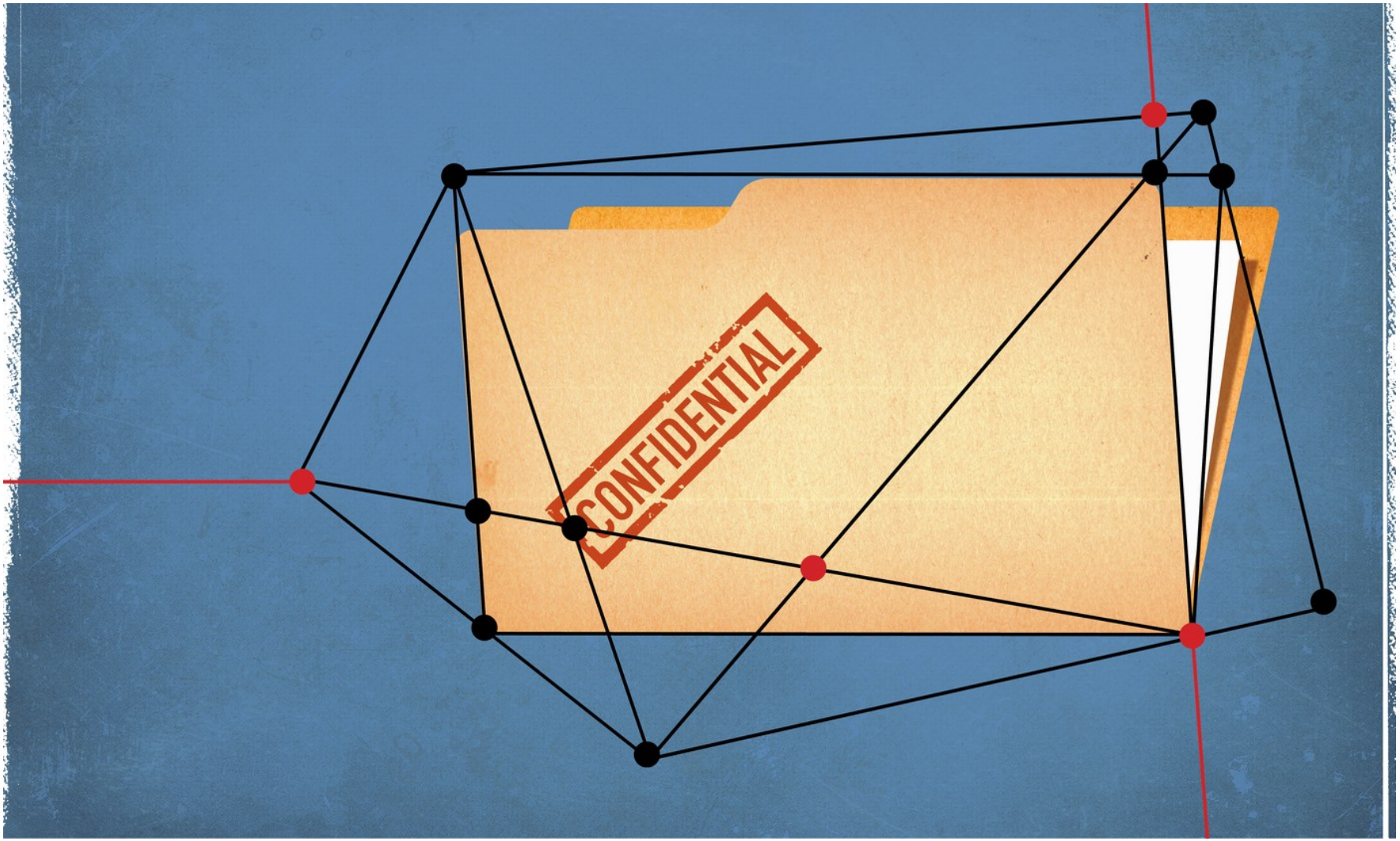


ILLUSTRATION BY VAL MINA

Other police departments have experienced similar problems, according to the minutes of a meeting between eight California law enforcement agencies and

dissatisfaction with the pricing model, reduction of services, lack of transparency, [and] failure to deliver products."

"There is a lot of conversation here about their pricing scheme getting out of hand," wrote Long Beach Chief of Police Robert Luna in an email that May. "Many agencies are unhappy (including LBPD) with the return on our... investment," replied his Administration Bureau Chief Braden Phillips. "Palantir is a powerful search tool, but is not user friendly." An analyst who formerly worked in law enforcement in New York goes further. "If you have never studied programming, it is impossible to learn Palantir in any reasonable timeline," says the analyst, who requested not to be named because they still work with agencies using Palantir. "They've built these extremely powerful [tools] that are essentially useless because [most] analysts don't have the technical background they need. Palantir is a great system for doing finance. I think it's really shitty if you're trying to save lives."

It all comes down to money. Many public agencies lack the funds to hire sought-after software engineers and analysts, especially after shelling out for a multi-million dollar Palantir system. "[Palantir] is very expensive," admits Craig Uchida. "[The LAPD] has been able to get grant funds... to bring it in but a lot of departments can't afford it and as a result, can't use it."

"The question should be asked, what else could we have gotten for this money?" argues Adam Schwartz, an attorney with the Electronic Frontier Foundation (EFF). "There are a lot of communities that would like to see police officers walking the beat more frequently. Unfortunately, that kind of conversation has not panned out

for high tech but do not pay for new patrols.

Palantir sells its technology to police forces on the basis that it breaks down silos, connects databases, and enables sharing between jurisdictions, saving everyone time and resources. The promise, however, comes with one big catch: You don't get that benefit unless other agencies are also using Palantir.

Sacramento's fusion center, the Central California Intelligence Center (CCIC), found this out the hard way when it wanted to share data with the local Sheriff's Department and other agencies in 2014. "The contracted software and support services recommended herein are highly specialized and proprietary to Palantir Technologies," it wrote in a proposal. "All other fusion centers in California have implemented the Palantir system. The only way to share intelligence with the other fusion centers within California is to upgrade to the Palantir system."

Palantir had even managed to make its closed platform the only updated server for the California State Threat Assessment System (STAS) intelligence centers, which produce and share criminal and terrorist activity data statewide. "In order to maintain connectivity with STAS intelligence centers the CCIC needs to purchase Palantir systems. Palantir is the only unique system that will allow for the CCIC to have connectivity with the other intelligence centers," reads the fusion center's

approved the $1.2 million contract.

A similar problem applies if you try to leave Palantir's world. According to Buzzfeed News, the New York Police Department (NYPD) is canceling its contract with Palantir after five years, in order to move to in-house technology that it hopes will be cheaper and easier to use. But when the NYPD requested copies of Palantir's analyses, Palantir declined to provide software that would let the NYPD access them in a standard format, saying that doing so would expose its intellectual property, according to Buzzfeed. The NYPD did not respond to requests for comment.

The ultimate effect, in California at least, is that Palantir has achieved the holy grail of Silicon Valley startups: a network effect with some lock-in power. You can't leave Facebook because the data you want—updates on family and friends—is only to be found there. And if you cancel your Spotify subscription, you can't take the music with you.

For law enforcement, the network effect is nigh-on irresistible. "You just don't know what little tidbit might prevent us from experiencing the next terror attack," says Peter Jackson of JRIC. "We found that the more data [Palantir] touches, the more powerful and relevant and useful it becomes."

That's the seductive logic of information: More is always better. California's cops have become accustomed to the adrenaline rush of data and analysis that Palantir provides, and the more departments that join, the more addictive its products.

Malinowski. "My feeling is that the more layers you have in there, the better the information you get." Los Angeles expanded Uchida's Laser program to 12 LAPD divisions this year and plans to roll it out citywide by the end of 2019. The LAPD also now has many hundreds of officers trained to use Palantir, according to Malinowski.

Police departments in Milwaukee and Toledo have expressed interest in trying out similar projects; a fusion center in Virginia has already invested in Palantir; and domestic law enforcement agencies in Canada and Australia are also using its technology.

That is not to say that police chiefs are complacent about concentrating so many resources on a single vendor. "I don't feel like the whole organization would grind to a halt, but it certainly would make it less efficient if we did not have access to Palantir," says Malinowski. "It would impair our ability to identify trends and follow up on investigations in a timely manner."

In the spring of 2015, just as Palantir was cementing its dominance of California, some senior officers speculated that because the state had come to rely so heavily on Palantir, the company might be equally reliant on California. Four of Palantir's biggest customers in the Los Angeles region—the LAPD, LASD, LBPD and JRIC—planned to confront the company in a make-or-break meeting about pricing, service levels, and data access. Braden Phillips of the LBPD outlined their strategy in an email to the other departments: "The collective bargaining power of the LA Region may be enough to get Palantir to make some changes. The loss of this area

outcome.

That meeting took place in June 2015. Soon afterwards, Long Beach PD temporarily discontinued its use of Palantir while it upgraded aging technology, citing high costs, but the department says it plans to resume using Palantir once that upgrade is complete. Despite the discussion of cost containment, the combined spend by the four regional players on Palantir products in 2016 was around $15 million—its highest level ever.

For researchers like Craig Uchida, the smart policing that Palantir enables is all about results. After a year of more frequent patrols and Chronic Offender Bulletins in Newton, 70 percent of the identified chronic offenders had been arrested at least once, violent crime had fallen by about 15 percent, and homicides had dropped 59 percent, he says. “This was the biggest decline citywide. To have that kind of impact was a real strong message about how you can use data and make a difference.”

However, he acknowledges that there is no way to tell whether that impressive reduction was due to the hotspot policing, the bulletins, or some unconnected trend. And though one of the LAPD’s reasons for adopting Uchida’s data-driven approach was to move away from profiles based on race or gang affiliation, new technology risks codifying old prejudices.

overrepresented in arrests and other aspects of criminal justice," says the Electronic Frontier Foundation's Schwartz. "So if you use arrests, convictions, or field interviews as the training data, you are going to get a prediction that is contrary to reality. It's going to have the appearance of objective computer truth [but] is just perpetuating an old racial injustice."

The avalanche of personal data means that individuals themselves now carry digital labels that may be impossible to escape. Once people are labelled as chronic offenders, they will receive additional police attention. This raises the chance that they will be stopped for minor infractions that might be overlooked in others, especially outside the hotspot zones.

"A lot of this data is garbage," says Schwartz. "People end up getting over-investigated because ...information in these databases is false or misleading. There isn't a way for people to... get the bad information out, or put their own side of the story in."

There is growing awareness that uniquely powerful technologies like Palantir's require special supervision and oversight. California already has rules that govern

MORE BACKCHANNEL INVESTIGATIONS

LAUREN SMILEY
Mike Rothenberg's VC firm was young, splashy, and loaded with cash. Now it's a...

JESSICA PISHKO
The Drone Company That Fell to Earth

MARK HARRIS
How Otto Defied Nevada and Scored a $680 Million Payout from Uber

considering SB-21, a law supported by the EFF that would require police departments to put new surveillance technologies through a public approvals process before use. They would also have to publish transparency reports detailing how often the technology was deployed, the kind of data it collected, any abuses, and how many cases they helped to close. A similar law is making its way through New York's legislature.

Working under the radar has been good for Palantir. Working under a spotlight could turn out to be both less comfortable and less profitable. But the public sector works for the people, not Palantir. If these bills pass, they could level the playing field between the company and the public, giving citizens more of the visibility into Palantir's operations that the company already has into their own lives.

This story received support from MuckRock, which provided assistance with public records requests but had no editorial input. You can find many of the primary documents on the author's MuckRock page.

#BACKCHANNEL #PALANTIR #POLICE #FREEDOM OF INFORMATION ACT #PETER THIEL