The new way police are surveilling you: Calculating your threat ‘score’

By Justin Jouvenal January 10, 2016 at 8:13 PM, Wall Street Journal

FRESNO, Calif. — While officers raced to a recent 911 call about a man threatening his ex-girlfriend, a police operator in headquarters consulted software that scored the suspect’s potential for violence the way a bank might run a credit report.

The program scoured billions of data points, including arrest reports, property records, commercial databases, deep Web searches and the man’s social- media postings. It calculated his threat level as the highest of three color-coded scores: a bright red warning.

The man had a firearm conviction and gang associations, so out of caution police called a negotiator. The suspect surrendered, and police said the intelligence helped them make the right call — it turned out he had a gun.

As a national debate has played out over mass surveillance by the National Security Agency, a new generation of technology such as the Beware software being used in Fresno has given local law enforcement officers unprecedented power to peer into the lives of citizens.

Police officials say such tools can provide critical information that can help uncover terrorists or thwart mass shootings, ensure the safety of officers and the public, find suspects, and crack open cases. They say that last year’s attacks in Paris and San Bernardino, Calif., have only underscored the need for such measures.

But the powerful systems also have become flash points for civil libertarians and activists, who say they represent a troubling intrusion on privacy, have been deployed with little public oversight and have potential for abuse or error. Some say laws are needed to protect the public.

In many instances, people have been unaware that the police around them are sweeping up information, and that has spawned controversy. Planes outfitted with cameras filmed protests and unrest in Baltimore and Ferguson, Mo. For years, dozens of departments used devices that can hoover up all cellphone data in an area without search warrants. Authorities in Oregon are facing a federal probe after using social media-monitoring software to keep tabs on Black Lives Matter hashtags.

“This is something that’s been building since September 11,” said Jennifer Lynch, a senior staff attorney at the Electronic Frontier Foundation. “First funding went to the military to develop this technology, and now it has come back to domestic law enforcement. It’s the perfect storm of cheaper and easier-to-use technologies and money from state and federal governments to purchase it.”

Few departments will discuss how — or sometimes if — they are using these tools, but the Fresno police offered a rare glimpse inside a cutting-edge $600,000 nerve center, even as a debate raged in the city over its technology.

An arsenal of high-tech tools

Fresno's Real Time Crime Center is the type of facility that has become the model for high-tech policing nationwide. Similar centers have opened in New York, Houston and Seattle over the past decade.

Fresno's futuristic control room, which operates around the clock, sits deep in its headquarters and brings together a handful of technologies that allow the department to see, analyze and respond to incidents as they unfold across this city of more than 500,000 in the San Joaquin Valley.

Fresno police are using software that has given law enforcement powers to peer into the lives of citizens. (Nick Otto/For The Washington Post)

On a recent Monday afternoon, the center was a hive of activity. The police radio crackled over loudspeakers — "subject armed with steel rod" — as five operators sat behind banks of screens dialing up a wealth of information to help units respond to the more than 1,200 911 calls the department receives every day.

On 57 monitors that cover the walls of the center, operators zoomed and panned an array of roughly 200 police cameras perched across the city. They could dial up 800 more feeds from the city's schools and traffic cameras, and they soon hope to add 400 more streams from cameras worn on officers' bodies and from thousands from local businesses that have surveillance systems.

The cameras were only one tool at the ready. Officers could trawl a private database that has recorded more than 2 billion scans of vehicle licenses plates and locations nationwide. If gunshots were fired, a system called ShotSpotter could triangulate the location using microphones strung around the city. Another program, called Media Sonar, crawled social media looking for illicit activity. Police used it to monitor individuals, threats to schools and hashtags related to gangs.

Fresno police said having the ability to access all that information in real time is crucial to solving crimes.

They recently used the cameras to track a robbery suspect as he fled a business and then jumped into a canal to hide. He was quickly apprehended.

The license plate database was instrumental in solving a September murder case, in which police had a description of a suspect's vehicle and three numbers from the license plate.

But perhaps the most controversial and revealing technology is the threat-scoring software Beware. Fresno is one of the first departments in the nation to test the program.

As officers respond to calls, Beware automatically runs the address. The searches return the names of residents and scans them against a range of publicly available data to generate a color-coded threat level for each person or address: green, yellow or red.

Exactly how Beware calculates threat scores is something that its maker, Intrado, considers a trade secret, so it is unclear how much weight is given to a misdemeanor, felony or threatening comment on Facebook. However, the program flags issues and provides a report to the user.

In promotional materials, Intrado writes that Beware could reveal that the resident of a particular address was a war veteran suffering from post-traumatic stress disorder, had criminal convictions for assault and had posted worrisome messages about his battle experiences on social media. The "big data" that has transformed marketing and other industries has now come to law enforcement.

Fresno Police Chief Jerry Dyer said officers are often working on scant or even inaccurate information when they respond to calls, so Beware and the Real Time Crime Center give them a sense of what may be behind the next door.

Fresno Chief of Police Jerry Dyer inside the Fresno Police Department's crime center. (Nick Otto/For The Washington Post)

"Our officers are expected to know the unknown and see the unseen," Dyer said. "They are making split-second decisions based on limited facts. The more you can provide in terms of intelligence and video, the more safely you can respond to calls."

But some in Fresno say the power and the sheer concentration of surveillance in the Real Time Crime Center is troubling. The concerns have been raised elsewhere as well — last year, Oakland city officials scaled back plans for such a center after residents protested, citing privacy concerns.

Rob Nabarro, a Fresno civil rights lawyer, said he is particularly concerned about Beware. He said outsourcing decisions about the threat posed by an individual to software is a problem waiting to happen.

Nabarro said the fact that only Intrado — not the police or the public — knows how Beware tallies its scores is disconcerting. He also worries that the system might mistakenly increase someone's threat level by misinterpreting innocuous activity on social media, like criticizing the police, and trigger a heavier response by officers.

“It’s a very unrefined, gross technique,” Nabarro said of Beware’s color-coded levels. “A police call is something that can be very dangerous for a citizen.”

Dyer said such concerns are overblown, saying the scores don’t trigger a particular police response. He said operators use them as guides to delve more deeply into someone’s background, looking for information that might be relevant to an officer on scene. He said officers on the street never see the scores.

Lt. Dave Ramos of the Fresno Police Department checks his computer after responding to a disturbance call that came in through the crime center. (Nick Otto/For The Washington Post)

Still, Nabarro is not the only one worried.

The Fresno City Council called a hearing on Beware in November after constituents raised concerns. Once council member referred to a local media report saying that a woman’s threat level was elevated because she was tweeting about a card game titled “Rage,” which could be a keyword in Beware’s assessment of social media.

Councilman Clinton J. Olivier, a libertarian-leaning Republican, said Beware was like something out of a dystopian science fiction novel and asked Dyer a simple question: “Could you run my threat level now?”

Dyer agreed. The scan returned Olivier as a green, but his home came back as a yellow, possibly because of someone who previously lived at his address, a police official said.

“Even though it’s not me that’s the yellow guy, your officers are going to treat whoever comes out of that house in his boxer shorts as the yellow guy,” Olivier said. “That may not be fair to me.”

He added later: “[Beware] has failed right here with a council member as the example.”

An Intrado representative responded to an interview request seeking more information about how Beware works by sending a short statement. It read in part: “Beware works to quickly provide [officers] with commercially available, public information that may be relevant to the situation and may give them a greater level of awareness.”

Calls for ‘meaningful debate’

Similar debates over police surveillance have been playing out across the country, as new technologies have proliferated and law enforcement use has exploded.

The number of local police departments that employ some type of technological surveillance increased from 20 percent in 1997 to more than 90 percent in 2013, according to the latest information from the Bureau of Justice Statistics. The most common forms of surveillance are

cameras and automated license plate readers, but the use of handheld biometric scanners, social media monitoring software, devices that collect cellphone data and drones is increasing.

Locally, the American Civil Liberties Union reports that police in the District, Baltimore, and Montgomery and Fairfax counties have cellphone-data collectors, called cell site simulators or StingRays. D.C. police are also using ShotSpotter and license plate readers.

The surveillance creates vast amounts of data, which is increasingly pooled in local, regional and national databases. The largest such project is the FBI's $1 billion Next Generation Identification project, which is creating a trove of fingerprints, iris scans, data from facial recognition software and other sources that aid local departments in identifying suspects.

Law enforcement officials say such tools allow them to do more with less, and they have credited the technology with providing breaks in many cases. Virginia State Police found the man who killed a TV news crew during a live broadcast last year after his license plate was captured by a reader.

Cell site simulators, which mimic a cellphone tower and scoop up data on all cellphones in an area, have been instrumental in finding kidnappers, fugitives and people who are suicidal, law enforcement officials said.

But those benefits have sometimes come with a cost to privacy. Law enforcement used cell site simulators for years without getting a judge's explicit consent. But following criticism by the ACLU and other groups, the Justice Department announced last September that it would require all federal agencies to get a search warrant.

The fact that public discussion of surveillance technologies is occurring after they are in use is backward, said Matt Cagle, an attorney for the ACLU of Northern California.

"We think that whenever these surveillance technologies are on the table, there needs to be a meaningful debate," Cagle said. "There needs to be safeguards and oversight."

After the contentious hearing before the Fresno City Council on Beware, Dyer said he now wants to make changes to address residents' concerns. The police chief said he is working with Intrado to turn off Beware's color-coded rating system and possibly the social media monitoring.

"There's a balancing act," Dyer said.