theguardian

February 5, 2016

Meet Joe Simitian, Silicon Valley's surveillance technology watchdog

Danny Yadron in Palo Alto, California

The Californian has drafted the strictest proposal yet that would require police forces to get explicit permission for new surveillance tech

Joe Simitian, in his Palo Alto office, says that without state-level scrutiny of surveillance technology, the 'steady drip of the erosion of the right to privacy' would be even worse. Photograph: Danny Yadron/The Guardian

One of the broadest pushes to reel in America's surveillance state isn't in Congress, the White House or a courtroom; arguably it's in Joe Simitian's office in California's Santa Clara County government building.

Simitian – 63 and bespectacled - is a supervisor on the county board here. This winter he drafted a proposal for regulation that would require local law enforcement to justify each time they use any piece of surveillance technology – fake cellphone towers, computer hacks, license plate readers, GPS trackers, or anything else that helps cops track civilians.

(cont. next page)

The police aren't his biggest fans. Simitian has spent the past year trying to slow the sheriff's purchase of new gadgets, and describes the relationship as having a "healthy tension".

"I am perpetually the guy at our board meetings saying, 'I just want to be mindful of …'" he told the Guardian. "People talk about the importance of constitutional rights, but somehow this one just seems to have taken a back seat to others."

Privacy advocates say the Santa Clara regulation would be one of the broadest anti-surveillance measures being considered anywhere in the US. As Washington remains deadlocked over how to put a leash on an ever-growing list of surveillance technology used by state and local police departments, it will probably be up to city councils and county boards to play watchdog.

That can be a daunting task for local politicians who often have little technical experience and are more focused on dangerous intersections and village planning.

Based in Silicon Valley, Simitian might be a special case. He's been close to technology since his mother helped program computers with punched cards. At one point she worked at North American Aerospace Defense Command in Colorado Springs. He also has an interest in non-parochial issues. The bookshelf in his office includes treatises on recent foreign conflicts – With The Contras – and most of the autobiographies to come out of the Bush and Obama administrations.

If privacy is a passion, he doesn't show it verbally. In conversation and at board meetings he speaks in a steady, even cadence. He's also prone to unprompted anecdotes.

Like this one: just before he joined the state assembly in 2000, an employee at the local Microsoft campus asked him for his thoughts on privacy legislation. Simitian said his first response was that he thought that was something handled by Washington DC. The room laughed.

Since then, his policy efforts have donned a tin foil hat.

In 2001, he introduced what would become the first data breach disclosure law in the US where if hackers steal a company's data, the firm has to notify affected consumers. Since then, 46 states have followed suit.

Google was affected by his 2003 law that requires companies that collect personal data to clearly post a privacy policy. And thanks to him, California in 2008 became one of four states to outlaw the mandatory implantation of a radio frequency identity chip under someone's skin.

As he paged over a binder of county documents and news clippings related to privacy, Simitian acknowledged, "these issues seem a little abstract when you're in the middle of a recession".

But he said that someone has to remain on guard. If the electorate waits to care about privacy only after it's gone, it's probably too late, he said.

(cont. next page)

“This is not something that happens overnight,” Simitian said. “This is a steady drip of the erosion of the right to privacy.”

His efforts come as Congress and states have moved to regulate specific electronic surveillance methods, such as aerial drones, bulk telephone record collection, and devices that impersonate a cell tower to intercept calls.

But making laws takes a lot of time, and as new bits of spy kit continuously show up it can be hard to keep pace.

So Simitian’s draft ordinance would require the local sheriff or any county agency to get board approval if it wants to buy any new piece of surveillance technology or use an existing system in a new way. This applies to any “technological tool used, designed or primarily intended to collect … information specifically associated with, or capable of being associated with, any individual or group”.

The sheriff would then have to provide details for a public report that would explain what the technology is and how it would be used.

In Silicon Valley speak, the statute is, theoretically, future-proof.

Law enforcement also says it is overly burdensome.

“We want to be careful about tying the hands of police officers who are just trying to solve crimes and protect people,” said the Santa Clara County district attorney, Jeffrey Rosen. “It’s not as though we’re in a country where there are no laws about how law enforcement is supposed to act.”

Rosen said he has one-on-one chats with Simitian at least once a month. And he said he genuinely respects him, even if he disagrees. He did, however, note that when he talks with law enforcement counterparts in other cities, they don’t seem to have to debate with a Simitian. In an interview, the district attorney described the county supervisor as “unique”. Even in Santa Clara he can be an anomaly.

At a county board meeting last month, Simitian peppered sheriff’s department officials about their request to buy four GPS tracking devices for $3,000 – a small request given the county’s annual budget, and one that was eventually approved.

But Simitian had wanted to know what controls would be placed on who had access to data collected by the trackers. The department, which didn’t immediately respond to a request for comment, recently had several correctional officers accused of inappropriately accessing a database with inmate data.

Simitian asked if the sheriff’s department would accept data security advice from a county technology staffer. The sheriff’s department declined. “Captain, we’ve got legal liability as a county for any misuse or abuse of the system,” Simitian told the board.“I’m just baffled there isn’t some way you’d be open to stepping up the security of the system.”

The New York Times

March 16, 2015

A Police Gadget Tracks Phones? Shhh! It's Secret

By MATT RICHTEL

A powerful new surveillance tool being adopted by police departments across the country comes with an unusual requirement: To buy it, law enforcement officials must sign a nondisclosure agreement preventing them from saying almost anything about the technology.

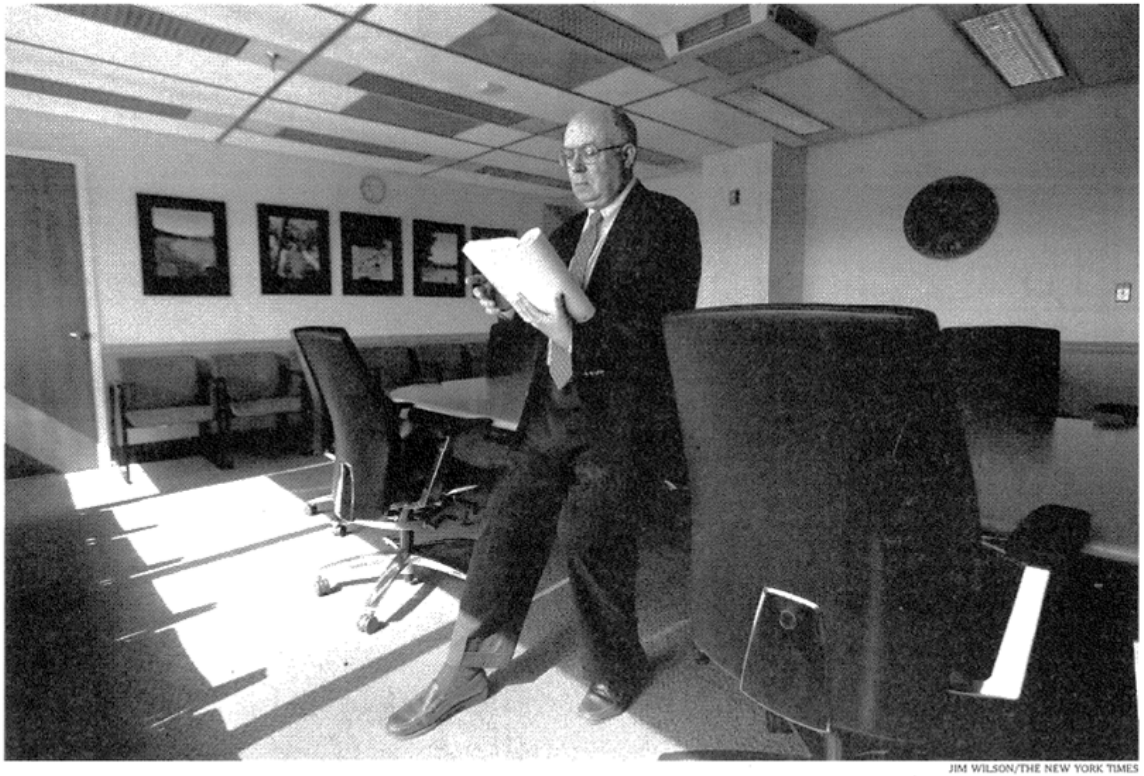
Any disclosure about the technology, which tracks cellphones and is often called StingRay, could allow criminals and terrorists to circumvent it, the F.B.I. has said in an affidavit. But the tool is adopted in such secrecy that communities are not always sure what they are buying or whether the technology could raise serious privacy concerns.

The confidentiality has elevated the stakes in a longstanding debate about the public disclosure of government practices versus law enforcement's desire to keep its methods confidential. While companies routinely require nondisclosure agreements for technical products, legal experts say these agreements raise questions and are unusual given the privacy and even constitutional issues at stake.

"It might be a totally legitimate business interest, or maybe they're trying to keep people from realizing there are bigger

(cont. next page)

A Law Enforcement Surveillance Tool That Tracks Phones? Shhh! It's Secret



JIM WILSON/THE NEW YORK TIMES

Joe Simitian, a Santa Clara County, Calif., supervisor, pressed for more information about the StingRay surveillance device.

privacy problems," said Orin S. Kerr, a privacy law expert at George Washington University. "What's the secret that they're trying to hide?"

The issue led to a public dispute three weeks ago in Silicon Valley, where a sheriff asked county officials to spend $502,000 on the technology. The Santa Clara County sheriff, Laurie Smith, said the technology allowed for locating cellphones — belonging to, say, terrorists or a missing person. But when asked for details, she offered no technical specifications and acknowledged she had not seen a product demonstration.

Buying the technology, she said, required the signing of a nondisclosure agreement.

"So, just to be clear," Joe Simitian, a county supervisor, said, "we are being asked to spend $500,000 of taxpayers' money and $42,000 a year thereafter for a product for the name brand which we are not sure of, a product we have not seen, a demonstration we don't have, and we have a nondisclosure requirement as a precondition. You want us to vote and spend money," he continued, but "you can't tell us more about it."

The technology goes by various names, including StingRay, KingFish or, generically, cell site simulator. It is a rectangular device, small enough to fit into a suitcase, that intercepts a cellphone signal by acting like a cellphone tower.

The technology can also capture texts, calls, emails and other data, and prosecutors have received court approval to use it for such purposes.

Cell site simulators are catching on while law enforcement officials are adding other digital tools, like video cameras, license-plate readers, drones, programs that scan billions of phone records and gunshot detection sensors. Some of those tools have invited resistance from municipalities and legislators on privacy grounds.

The nondisclosure agreements for the cell site simulators are overseen by the Federal Bureau of Investigation and typically involve the Harris Corporation, a multibillion-dollar defense contractor and a maker of the technology. What has opponents particularly concerned about StingRay is that the technology, unlike other phone surveillance methods, can also scan all the cellphones in the area where it is being used, not just the target phone.

"It's scanning the area. What is the government doing with that information?" said Linda Lye, a lawyer for the American Civil Liberties Union of Northern California, which in 2013 sued the Justice Department to force it to disclose more about the technology. In November, in a response to the lawsuit, the government said it had asked the courts to allow the technology to capture content, not just identify subscriber location.

The nondisclosure agreements make it hard to know how widely the technology has been adopted. But news reports from around the country indicate use by local and state police agencies stretching from Los Angeles to Wisconsin to New York, where the state police use it. Some departments have used it for several years. Money for the devices comes from individual agencies and sometimes, as in the case of Santa Clara County, from the federal government through Homeland Security grants.

Christopher Allen, an F.B.I. spokesman, said "location information is a vital component" of law enforcement. The agency, he said, "does not keep repositories of cell tower data for any purpose other than in connection with a specific investigation."

A fuller explanation of the F.B.I.'s position is provided in two publicly sworn affidavits about StingRay, including one filed in 2014 in Virginia. In the affidavit, a supervisory special agent, Bradley S. Morrison, said disclosure of the technology's specifications would let criminals, including terrorists, "thwart the use of this technology."

"Disclosure of even minor details" could harm law enforcement, he said, by letting "adversaries" put together the pieces of the technology like assembling a "jigsaw puzzle." He said the F.B.I. had entered into the nondisclosure agreements with local authorities for those reasons. In addition, he said, the technology is related to homeland security and is therefore subject to federal control.

In a second affidavit, given in 2011, the same special agent acknowledged that the device could gather identifying information from phones of bystanders. Such data "from all wireless devices in the immediate area of the F.B.I. device that subscribe to a particular provider may be incidentally recorded, including those of innocent, nontarget devices."

But, he added, that information is purged to ensure privacy rights.

In December, two senators, Patrick J. Leahy and Charles E. Grassley, sent a letter expressing concerns about the scope of the F.B.I.'s StingRay use to Eric H. Holder Jr., the attorney general, and Jeh Johnson, the secretary of Homeland Security.

The Harris Corporation declined to comment, according to Jim Burke, a company spokesman. Harris, based in Melbourne, Fla., has $5 billion in annual sales and specializes in communications technology, including battlefield radios.

Jon Michaels, a law professor at the University of California, Los Angeles, who studies government procurement, said Harris's role with the nondisclosure agreements gave the company tremendous power over privacy policies in the public arena.

"This is like the privatization of a legal regime," he said. Referring to Harris, he said: "They get to call the shots."

For instance, in Tucson, a journalist asking the Police Department about its StingRay use was given a copy of a nondisclosure agreement. "The City of Tucson shall not discuss, publish, release or disclose any information pertaining to the product," it read, and then noted: "Without the prior written consent of Harris."

The secrecy appears to have unintended consequences. A recent article in The Washington Post detailed how a man in Florida who was accused of armed robbery was located using StingRay.

As the case proceeded, a defense lawyer asked the police to explain how the technology worked. The police and prosecutors declined to produce the machine and, rather than meet a judge's order that they do so, the state gave the defendant a plea bargain for petty theft.

At the meeting in Santa Clara County last month, the county supervisors voted 4 to 1 to authorize the purchase, but they also voted to require the adoption of a privacy policy.

(Sheriff Smith argued to the supervisors that she had adequately explained the technology and said she resented that Mr. Simitian's questioning seemed to "suggest we are not mindful of people's rights and the Constitution.")

A few days later, the county asked Harris for a demonstration open to county supervisors. The company refused, Mr. Simitian said, noting that "only people with badges" would be permitted. Further, he said, the company declined to provide a copy of the nondisclosure agreement — at least until after the demonstration.

"Not only is there a nondisclosure agreement, for the time being, at least, we can't even see the nondisclosure agreement," Mr. Simitian said. "We may be able to see it later, I don't know."

sanjoseinside

November 14, 2014

Proposal: No New Surveillance Tools Without Public Input

*By **Jennifer Wadsworth** @jennwadsworth/ November 14, 2014*

San Jose police bought this drone without public input. (Image via Heli-world.com)

In response to growing concerns about government spying and personal privacy, Santa Clara County will study a proposal that would require public input before purchasing any surveillance tools.

According to a report released Wednesday by the American Civil Liberties Union, at least 90 law enforcement agencies in the state use surveillance technology, including license plate scanners, cameras and facial recognition software. Yet, those same agencies sought input only 14 percent of the time, the ACLU report states.

The study offers a glimpse of the tools that have transformed modern policing, such as cell phone trackers, body-worn cameras and drones. California agencies have spent upward of $65 million on 180 surveillance technology programs, the report states. Of that number, only 26 programs came up for public discussion.

The plan to regulate surveillance technology on the county level comes up for

(cont. next page)

consideration at Tuesday's Board of Supervisors meeting. The memo, signed by Supervisor Joe Simitian, asks for greater accountability in both acquiring surveillance equipment and managing the data it collects.

Simitian says the ACLU approached him several months ago to join in the project, which has enlisted the support of a broad coalition of elected officials. The group even provided a model ordinance to work with.

"We had worked together quite a bit when I was in the state legislature," Simtian said, noting that he served on the Select Committee on Privacy for both the State Assembly and State Senate.

"I've been working on these issues for the last decade and a half and what I've observed is an erosion of public privacy in an incremental fashion," Simtian said. "It's sort of drip, drip, drip."

"Just to be clear, do I think there's an appropriate use for license plate readers, closed circuit cameras and drone technology in the public arena? I absolutely do," he continued. "Do I think there are a series of questions that need to be asked and answered before we use that technology? Absolutely."

With enough public input, he says, the county can strike a balance.

"I don't think it's mutually exclusive," said Simitian. "I think we can protect and respect people's privacy."

In addition to law enforcement concerns, Simitian said his memo is part of larger plan to bring attention to raise privacy concerns about all county work, including hospital and tax records.

Simitian's memo asks for the county to draft a plan that would put in place more checks and balances before acquiring certain surveillance equipment. It would require all surveillance technology proposals to include an impact report, explaining the technology, its purpose, proposed deployment locations, monetary cost and potential impacts on civil liberties. It would also include a legally enforceable surveillance policy that limits when data can be accessed, who could see it and how long it's stored.

"Candidly, when I arrived at the county I was surprised at the failure to consider privacy implications in all of the work the county did," he said.

Mountain View VOICE

March 6, 2015

EDITORIAL
THE OPINION OF THE VOICE

Supervisors' action undermined the public process

Railing against the increasingly invasive use of high-tech tools to keep track of what we do, where we are, what we're reading and who might be coming over for dinner is a noble but often futile effort. Horse out of barn. Full gallop. Barn door closed. Alas.

The speed of technological development makes it unlikely if not impossible for a wired society to stay informed of the latest data-mining and other capabilities sneaked in by Google, Facebook and other private companies, and outpaces the ability of elected leaders to develop strategies to protect our privacy and due process rights, even when they care to try.

When a government agency, such as a police department or sheriff's office, introduces a plan for yet another potentially intrusive high-tech tool, the best we can do is thoroughly scrutinize the device and its capabilities, and put into place well-defined laws and strategies to protect the public from government overreach. And to do it *before* the agency is authorized to buy the equipment.

That's exactly what Supervisor Joe Simitian fought to do late last month when the Santa Clara County Board of Supervisors was asked to approve Sheriff Laurie Smith's request to buy a cellphone tracker. The sheriff wanted to spend nearly $503,000 from a Department of Homeland Security fund on a cellphone triangulation system that could be used to locate individuals. The tracking device would help the department find wanted criminals, suspects or people at risk, she told the board.

Sounds like an appealing proposition, right? Except that the device could also be used to keep track of any of us, compromising our rights to privacy and due process. When the sheriff presented her case for the cellphone tracker to the supervisors, there had been no open public review, and no policy on the device's use had been developed, much to Simitian's chagrin.

The supervisors did the public a disservice by authorizing the purchase, with Simitian casting the single "no" vote, prior to an open public review and the crafting of a policy to protect the public from abusive use of the tracking devise.

Simitian argued that the sheriff's request should be put on hold until a policy was developed — with public input — but his colleagues forged ahead. Why? Sheriff Smith argued that the funding could be withdrawn if her department didn't act soon to purchase the tracker, and the supervisors appeared to accept that premise. But the grant that includes funding for the device was approved in 2013, and the sheriff's office discussed buying the tracker at various times in 2014, at least as early as July. Why were elected officials and the public left in the dark all that time, only to be pressured in the final weeks to approve the purchase or lose the money? And why is the sheriff's office so vague about a policy for use after all these months of discussion?

The supervisors have rewarded the county's law enforcement agency for its lack of transparency and its end run to put undue pressure on them to rush through a process that requires rigorous scrutiny by them and the public. The caveat in approving the purchase is that the tracker cannot be put into use until a policy is discussed and approved. But what's missing in that way forward is another important aspect of the public process: an open discussion of whether the cellphone tracker is an item residents of Santa Clara County want their sheriff's office to have in its toolbox.

Simitian last year called for the development of a policy addressing the overall use of surveillance tools in the county. Such a policy would provide a framework to protect the public from abusive application of these high-tech tools that, like it or not, are here to stay. It's time to have a public discussion on such a policy, then act to put one firmly in place.

The Mercury News

June 7, 2016

Editorial

Simitian's surveillance rules needed

At the heart of Silicon Valley, Santa Clara County should be a pioneer in setting technology policy — including privacy rights, which increasingly are under attack by government agencies.

The Board of Supervisors on Tuesday should adopt Supervisor Joe Simitian's proposal to govern the use of surveillance technology. The cutting-edge ordinance will require that the board and the public be informed before any new surveillance technology is purchased by law enforcement officers and that a policy is in place governing how it can be used.

Critics, including District Attorney Jeff Rosen, worry that this might interfere with law enforcement's ability to catch criminals. He argues that the current proposal is too broad and that further discussion is needed to sharpen the ordinance.

Simitian's proposal will not block law enforcement from purchasing new technology or putting it to use. It will guarantee that the potential use of a new gadget first be discussed in public, policies for its use adopted and oversight established, including making it a misdemeanor for law enforcement agencies or individuals to disregard the policies.

The need for oversight became apparent last year when the county Sheriff's Office was given approval to purchase a cellphone tracking system for $500,000 without being able to fully explain to the supervisors how it works, let alone when and how it would be used. Supervisors were forced to rush to approve the request because of an imminent deadline

(cont. next pag

for winning a federal grant, although the purchase was never completed.

The device impersonates a cellphone tower and can capture conversations, emails and texts of users in the area. In theory, it would be used only to track specific cellphone numbers, but the potential for abuse is high. At a time when the National Security Agency, FBI and other agencies are trying to broadly collect Americans' private data, "Trust us" just doesn't cut it.

Take drones, for example. They can save lives. Drones were used in the hunt for the suspects in Thursday's attack on police officers in Fremont. They can be helpful in search and rescue operations, hostage situations and bomb threats. But they can also be abused — snooping over people's backyards, for example. Elected officials need to set boundaries. Law enforcement should encourage this to keep the public trust. Otherwise, negative reactions to abuses could lead to voter-approved bans.

Tech advances constantly are producing new law enforcement tools. That's great, but nearly all need some constraints attached. Because this proposal is an ordinance and not etched in stone by voters, the supervisors can revisit and adapt it as technology and social norms change.

Simitian's ordinance provides transparency and accountability to this emerging field. The board should adopt it, and other counties should view it as a model. Eavesdropping gadgets may emerge from Silicon Valley, but they for sure don't stay here.

ars technica

June 8, 2016

Silicon Valley county passes new law requiring approval before cops buy spy kit

"The question is whether or not we have the wisdom to use the technology appropriately."

CYRUS FARIVAR - 6/8/2016, 2:00 AM

Dawn Endico

A Silicon Valley county has become the first in the United States to vote in a new law that requires "continued oversight and regular evaluation" for law enforcement agencies prior to the acquisition of surveillance technology.

The ordinance, which was unanimously approved by the Santa Clara County Board of Supervisors on Tuesday, requires that the county sheriff's and the district attorney's offices seek board approval before those agencies even begin the process of obtaining new snooping gear. The agencies are not required to immediately notify the board in exigent circumstances, but they must do so within 90 days.

Agencies must also submit a usage policy to the county government and, notably, an "Annual Surveillance Report," which should describe what data the device captures, how the agency deals with information collected about people not suspected of any wrongdoing, and whether the gear has been effective, among other requirements.

"The ordinance doesn't prohibit the acquisition of any surveillance technology," Supervisor Joe Simitian, a longstanding local privacy advocate and former state senator, told Ars. "It says if you're going to acquire any surveillance technology, let's talk about privacy and due process rights."

(cont. next page)

"The issue is not the technology. The question is whether or not we have the wisdom to use the technology appropriately," he added.

Catherine Crump, a law professor at the University of California, Berkeley, said that she was not aware of any county nationwide to implement such a law, but she noted that Seattle has a similar municipal law.

"It's particularly important that a tech savvy jurisdiction in the heart of Silicon Valley model how we can achieve the benefits of surveillance technology without abandoning people's privacy rights," she e-mailed Ars. "It seems likely that other counties and cities will use what Santa Clara has done as a model and feel more comfortable creating ground rules in this area."

Similarly, Elizabeth Joh, a law professor at the University of California, Davis, also said she didn't know of any similar county-level ordinances.

"If secrecy breeds suspicion, openness encourages oversight," she e-mailed Ars. "In the post-Snowden era, communities want to know *how* the police are doing what they do, not just that they are achieving data-driven results."

A delicate balance

In the 10-page ordinance, the Board acknowledged California's right to privacy, which is enshrined in the state constitution, but also noted that:

…surveillance technology may also be a valuable tool to bolster community safety and aid in the investigation and prosecution of crimes. To balance the public's right to privacy with the need to promote and ensure community safety, the Board finds that any decision to use surveillance technology must be judiciously balanced with an assessment of the costs to the County and the protection of privacy, civil liberties, and civil rights.

The Santa Clara Board made headlines over a year ago when it refused to approve the purchase of cell-site simulators, better known as stingrays. Simitian led the charge in trying to pierce the veil of secrecy when the county sheriff tried to acquire stingrays using federal grant money—ultimately the board rejected the sheriff's efforts.

Civil liberties groups, including the American Civil Liberties Union of California, lauded Tuesday's vote.

"When law enforcement gets to conceal the use of surveillance tools, they also get to conceal the misuse and abuse of these technologies," Nicole Ozer, a director at the ACLU of California, said in a statement. "Law enforcement in Silicon Valley has attempted secret drone purchases, lobbied to buy invasive cell phone trackers, and used social networking software to target Black, Asian-American, and Muslim protesters, so there certainly was a need for greater transparency and oversight."