

Silicon Valley

'They'll squash you like a bug': how Silicon Valley attacks those that displease it

Working for a tech company may sound like all fun and ping-pong, but behind the facade is a ruthless code of secrecy – and deadly retribution for those who break the secrecy or interfere with the Silicon Valley Cartel

 A former Facebook employee described his experience as the subject of an internal investigation: 'It's horrifying how much they know.'

▲ A former Facebook employee described his experience as the subject of an internal investigation: 'It's horrifying how much they know.' Photograph: Jeff Chiu/AP

Olivia Solon *in San Francisco*

 [@oliviasolon](#)  [Email](#)

Fri 16 Mar 2018 05.00 EDT



One day last year, John Evans (not his real name) received a message from his manager at [Facebook](#) telling him he was in line for a promotion. When they met the following day, she led him down a hallway praising his performance. However, when she opened the door to a meeting room, he came face to face with members of Facebook’s secretive “rat-catching” team, led by the company’s head of investigations, Sonya Ahuja.

The interrogation was a technicality; they already knew he was guilty of leaking some innocuous information to the press. They had records of a screenshot he’d taken, links he had clicked or hovered over, and they strongly indicated they had accessed chats between him and the journalist, dating back to before he joined the company.

Contact the Guardian securely



[Read more](#)

“It’s horrifying how much they know,” he told the Guardian, on the condition of anonymity. “You go into Facebook and it has this warm, fuzzy feeling of ‘we’re changing the world’ and ‘we care about things’. But you get on their bad side and all of a sudden you are face to face with [Facebook CEO] Mark Zuckerberg’s secret police.”


The public image of Silicon Valley’s tech giants is all colourful bicycles, ping-pong tables, beanbags and free food, but behind the cartoonish facade is a ruthless code of secrecy. They rely on a combination of Kool-Aid, digital and physical surveillance, legal threats and restricted stock units to prevent and detect intellectual property theft and other criminal activity. However, those same tools are also used to catch employees and contractors who talk publicly, even if it’s about their working conditions, misconduct or cultural challenges within the company.




While Apple's culture of secrecy, which includes making employees sign project-specific NDAs and covering unlaunched products with black cloths, has been widely reported, companies such as Google and Facebook have long put the emphasis on internal transparency.

Zuckerberg hosts weekly meetings where he shares details of unreleased new products and strategies in front of thousands of employees. Even junior staff members and contractors can see what other teams are working on by looking at one of many of the groups on the company's internal version of Facebook.

“When you first get to Facebook you are shocked at the level of transparency. You are trusted with a lot of stuff you don't need access to,” said Evans, adding that during his induction he was warned not to look at ex-partners' Facebook accounts.

“The counterbalance to giving you this huge trusting environment is if anyone steps out of line, they'll squash you like a bug.”

 The Google campus in Mountain View, California. The company has been sued for using overly broad confidentiality agreements and getting employees to spy on each other.

▲ The Google campus in Mountain View, California. The company has been sued for using overly broad confidentiality agreements and getting employees to spy on each other. Photograph: JasonDoiy/Getty Images   

During one of Zuckerberg's weekly meetings in 2015, after word of its new messaging assistant spread, the usually affable CEO warned employees: "We're going to find the leaker, and we're going to fire them." A week later came the public shaming: Zuck revealed the culprit had been caught and fired. [People at the meeting applauded.](#)

"Companies routinely use business records in workplace investigations, and we are no exception," said a Facebook spokeswoman, Bertie Thomson.

It's a similar story at Google. Staff use an internal version of Google Plus and thousands of mailing lists to discuss everything from homeownership to items for sale, as well as social issues like neoconservatism and diversity. With the [exception of James Damore's explosive memo](#) about gender and tech, most of it doesn't leak.

By and large, staff buy into the corporate mission in a happy-clappy campus which helps foster a tribal mentality that discourages treachery. Employees are also rewarded with annual allocations of restricted stock that can buy silence for years after leaving.

"You would never do something that screws up the company's chance of success because you are directly affected by it," said a former Googler Justin Maxwell, who noted the pressure to behave in a "Googley" way.

The search engine's former head of investigations, Brian Katz, highlighted this in 2016 in a company-wide email titled: "Internal only. Really."

“If you’re considering sharing confidential information to a reporter – or to anyone externally – for the love of all that’s Googley, please reconsider! Not only could it cost you your job, but it also betrays the values that makes [sic] us a community,” he wrote.

 Leaking isn’t ‘Googley’.

▲ Leaking isn’t ‘Googley’. Photograph: San Francisco Superior Court



This email came to light after another former employee sued Google for its overzealous approach to preventing leaks using overly broad confidentiality agreements and getting employees to spy on and report each other. The legal **complaint** alleges that Google’s policies violate labour laws that allow employees to discuss workplace conditions, wages and potential legal violations inside the company. Both parties are scheduled to enter mediation later this year.

James Damore, the software engineer who was fired from [Google](#) after writing a controversial memo questioning diversity programmes, suspects he was being monitored by the company during his final days.

He also described “weird things” happening to his work phone and laptop after the memo went viral. “All the internal apps updated at the same time, which had never happened before. I had to re-sign in to my Google account on both devices and my Google Drive – where the document was – stopped working.”

Damore said that much of the spying capabilities were outlined in his contract and that it was mostly “necessary” for a company that gives “everyone access to secret things”.

After he was fired, Damore stopped using his personal Gmail account in favour of Yahoo email out of fear that Google might be spying on him. “My lawyer doesn’t think they are above doing that,” he said.

It’s not implausible: Microsoft [read a French blogger’s Hotmail account](#) in 2012 to identify a former employee who had leaked trade secrets.

However, a Google spokeswoman said the company never reads personal email accounts and denied spying on Damore’s devices.

“I wouldn’t expect them to admit to it,” Damore said.

Since Damore’s memo, Google has become much leakier, particularly around [internal discussions](#) of racial and gender diversity.

“It’s a cry for help internally,” said another former Googler, who now runs a startup.

He said people at Google had for years put up with covert sexism, internal biases or, in his case, a manager with anger management problems. “No one would do anything until one day a VP saw the guy yelling at me in the hallway.

“People have been dealing with this stuff for years and are finally thinking ‘if Google isn’t going to do something about it, we’re going to leak it’.”

Everyone was paranoid. When we texted each other, we’d use code if we needed to talk about work

For low-paid contractors who do the grunt work for big tech companies, the incentive to keep silent is more stick than carrot.

What they lack in stock options and a sense of corporate tribalism, they make up for in fear of losing their jobs.

One European Facebook content moderator signed a contract, seen by the Guardian, which granted the company the right to monitor and record his social

media activities, including his personal Facebook account, as well as emails, phone calls and internet use. He also agreed to random personal searches of his belongings including bags, briefcases and car while on company premises. Refusal to allow such searches would be treated as gross misconduct.

Following [Guardian reporting](#) into working conditions of community operations analysts at Facebook’s European headquarters in Dublin, the company clamped down further, he said.

Contractors would be questioned if they took photographs in the office or printed emails or documents. “On more than one occasion

someone would print something and you'd find management going through the log to see what they had printed," said one former worker.

Security teams would leave "mouse traps" – USB keys containing data that were left around the office to test staff loyalty. "If you find a USB or something you'd have to give it in straight away. If you plugged it into a computer it would throw up a flare and you'd be instantly escorted out of the building."

"Everyone was paranoid. When we texted each other we'd use code if we needed to talk about work and meet up in person to talk about it in private," he said.

Some employees switch their phones off or hide them out of fear that their location is being tracked. One current [Facebook employee who recently spoke to Wired](#) asked the reporter to turn off his phone so the company would have a harder time tracking if it had been near the phones of anyone from Facebook.

 [James Damore stopped using his personal Gmail account after being fired, due to fears Google was spying on him.](#)

▲ James Damore stopped using his personal Gmail account after being fired, due to fears Google was spying on him. Photograph: Winni Wintermeyer for the Guardian



Two security researchers confirmed that this would be technically simple for Facebook to do if both people had the Facebook app on their phone and location services switched on. Even if location services aren't switched on, Facebook can infer someone's location from wifi access points.

“We do not use cellphones to track employee locations, nor do we track locations of people who do not work at Facebook, including reporters,” said Thomson.

Companies will also hire external agencies to surveil their staff. One such firm, Pinkerton, counts Google and Facebook among its clients.

Among other services, Pinkerton offers to send investigators to coffee shops or restaurants near a company's campus to eavesdrop on employees' conversations.

Big data for the people: it's time to take it back from our tech overlords



[Read more](#)

“If we hear anything about a new product coming, or new business ventures or something to do with stocks, we'll feed that information back to corporate security,” said David Davari, a managing director at the firm, adding that the focus is usually IP theft or insider trading.

Facebook and Google both deny using this service.

Through LinkedIn searches, the Guardian found several former Pinkerton investigators to have subsequently been hired by Facebook, Google and Apple.

“These tools are common, widespread, intrusive and legal,” said Al
Gidari, consulting director of privacy at the Stanford Center for
Internet and Society.

“Companies are required to take steps to detect and deter criminal
misconduct, so it’s not surprising they are using the same tools to
make sure employees are in compliance with their contractual
obligations.”

● *Contact the author: olivia.solon@theguardian.com / Signal +1
(650) 797 2472 or [find out more about how to contact the Guardian
securely](#).*

Topics



[Silicon Valley](#) /



[Google](#) /



[Facebook](#) /



[Alphabet](#) /



[Social networking](#) /



[Surveillance](#) /



[features](#) /

'It's horrifying how much they know': A Facebook employee explained what it's like to go face to face with Mark Zuckerberg's 'secret police'



An anonymous Facebook employee [has explained in a new interview with The Guardian](#) what it's like to be under investigation by Facebook's internal investigations

Facebook founder and CEO
Mark Zuckerberg Thomson Reuters

team.

FB Facebook-A

183.84 -0.26 (-0.10 %)

The anonymous employee said that they received a

Disclaimer

[Get real-time FB charts here »](#)

message from their manager saying they would receive a promotion. They said their manager walked them down a corridor, praising their work, and then directed them into a meeting room.

Inside the meeting room were several members of Facebook's internal investigations team, The Guardian reported. The investigators accused the employee of leaking information to a journalist, and the employee said they had records of screenshots, links clicked, and potentially the conversation with a journalist.

"It's horrifying how much they know," the anonymous employee told The Guardian, "you go into Facebook and it has this warm, fuzzy feeling of 'we're changing the world' and 'we care about things'. But you get on their bad side and all of a sudden you are face to face with Mark Zuckerberg's secret police."

The employee went on to say that "the counterbalance to giving you this huge trusting environment is if anyone steps out of line, they'll squash you like a bug."

It's not unusual for technology companies to have internal investigation teams that try to root out leaks. [But the full feature by The Guardian](#) illuminates how widespread it is and how it works. Facebook did not immediately respond to a request for comment.



Fa

Facebook bans Britain First pages (bbc.co.uk)

submitted 2 days ago by [generate](#) to [news](#) (+30|-0)



1 comment