How Google Spies on Its Employees

Looking up COBRA health insurance costs. Screenshotting and using encrypted messaging apps at the same time. Google employees can attract scrutiny from the company's corporate security team through ordinary actions. Now a new trial is calling attention to the search giant's surveillance of staffers.

Illustration by Haejin Park

By Sarah Krouse

Sept. 23, 2021 6:00 AM PDT

At Google, a seemingly innocuous action can earn an employee the attention of the company's corporate security department.

For example, when Google wants to find out who has been accessing or leaking sensitive corporate information, the company often homes in on employees who are thinking about leaving it. In the past, its security teams have flagged employees who search an internal website listing the cost of COBRA health insurance—which gives workers a way to continue their coverage after leaving their employer—for further investigation, according to a person with direct knowledge of its tactics. Employees who draft resignation letters or seek out internal checklists that help workers plan their departures from Google have also faced similar scrutiny, the person said.

It has even looked at who has taken screenshots on work devices while running encrypted messaging services at the same time, according to current and former employees with knowledge of the practices. Bulk transfers of data onto USB storage devices and use of third-party online storage services can also raise eyebrows among Google's security staff.

> **THE TAKEAWAY**
>
> - Google leak hunts have focused on employees likely to leave
> - Viewing COBRA health information can attract suspicion
> - Google-backed open-source tool call Grr used for worker surveillance

Sure, Google knows a lot about the habits of the public through its all-seeing lens on internet searches and mobile phones. But the company also keeps a close eye on its employees through an extensive toolbox of digital surveillance techniques, many of which The Information is describing here for the first time. Google has even exported some of those tools outside the company so others can use them.

A company spokesperson said Google has "security policies that strictly protect user and customer data, as well as sensitive IP and trade secrets." Its security team "thoroughly investigates breaches," as other companies do.

The company says it does not monitor employee's personal devices. "We have literally zero desire to monitor our employees' personal data or activity," the spokesperson said.

U.S. employers have broad freedom to track their workers' activities, from logging keystrokes to taking screen grabs to digging through their emails. Some of them have no choice in the matter. For example, many financial services regulators require securities firms to record employee phone conversations, emails and chats related to trading activities as part of efforts to avoid potential market-rigging.

Silicon Valley companies aren't typically subject to that tight regulation, but have nevertheless focused on using digital surveillance tools—sometimes described pejoratively as bossware—to avoid the loss or misuse of intellectual property, client data and other confidential information at the hands of staff. Staffers who break those rules can be fired, disciplined and sued by their employers.

Apple CEO Tim Cook, for instance, recently warned employees in an email that the company is doing "everything in our power to identify those who leaked" **details** of an earlier all-hands meeting, **The Verge reported** on Wednesday. And Amazon has installed video cameras in its delivery vans to reduce distracted driving, tailgating and other unsafe behavior by its drivers, as The Information was first to report **earlier this year**.

"Everything you do is marked in your digital footprint," said Kon Leong, CEO of ZL Technologies, a data management company that helps employers detect compliance issues.

For its part, Google has snooped on employees for years, but its practices are now in the public spotlight in large part because they have collided with the employee activism that has buffeted Google in recent years. Last month, a trial began over a lawsuit the National Labor Relations Board filed against Google, in which the federal agency accused Google of illegally surveilling and firing several of those activist employees.

The company fired two of them, Sophie Waldman and Paul Duke, for accessing documents in 2019 related to work with U.S. Customs and Border Protection and sharing those documents with other Google employees in a petition that sought to discourage Google from pursuing an upcoming contract with the agency. Those employees, along with others involved in the NLRB suit, said the documents they accessed were easily found within Google's intranet, known as Moma. They testified that Google could have easily made the documents inaccessible to all Google employees or kept them off the intranet entirely.

Google's investigation of Waldman and Duke didn't appear to involve elaborate cloak-and-dagger techniques. Instead, the company saw through its digital records that the two had been involved in creating and distributing a petition, which linked to documents containing customer information they had accessed through Moma.

Attorneys for the former Google employees and the NLRB have said in legal filings that their actions were protected activities for the purpose of mutual aid and that Google selectively punished them. The employees were complying with a directive—included in Google's code of conduct—to speak up if they saw something they thought wasn't right, their attorney argued.

According to Duke, Google in 2019 changed its employee information policy to expand the scope of internal information that employees could be fired for accessing, a move that seemed to be designed to keep workers from protesting future projects.

Google executives are expected to testify in the NLRB trial in the coming weeks and the company has said it "strongly disagrees with" the agency's claims. The company says its investigation found individuals were involved in "systematic searches for other employees' materials and work, including distributing confidential business and client information."

Google's employee surveillance also stands out because—in the eyes of some employees, at least—it seems to contradict the spirit of openness and virtue that attracted them to the company in the first place. During the NLRB trial, for example, current and former employees testified that they were drawn to Google because of its "don't be evil" founding mantra and their ability to see what others across the company were working on.

"Google was presenting itself as more than a company. It was this family, this identity, and a place that was better than all the rest of them and a really great place to work. And then this betrayal," said Margaret O'Mara, a history professor at the University of Washington who has studied the history of Silicon Valley. "When you get to a certain size, all secrets can't be shared."

Google's employee code of conduct warns staff that it may monitor, access or share their communications and other information to investigate suspected misconduct, when there is a business need or to secure its resources and property. Many of the tools it uses to catch internal threats also help detect cyberattacks, intellectual property theft and state-sponsored attacks.

'Google was presenting itself as more than a company. It was this family, this identity, and a place that was better than all the rest of them and a really great place to work.'

As a result, employees at times resort to tradecraft to avoid detection when they're breaking Google's rules. A couple years ago, one Google employee, who has since left the company, refused to talk to a reporter from his phone, which ran Google's Android operating system, insisting instead that the reporter call him on his teenager's iPhone.

Forensic Tools

Google has begun sharing more of its internal security and surveillance tools with other companies.

After Google announced in 2010 that it had detected a sophisticated attack, which originated in China and resulted in the theft of Google intellectual property, its engineers began developing an incident response system that the company later released as open-source software, as it has done with numerous coding projects in the past.

That software—known as Grr Rapid Response, after the expression of frustration Google security engineers uttered when using other security tools—lets companies access and regularly scan data on tens of thousands of work machines at once. Since then, Grr has evolved from an initial focus on detecting malware and other cyberattacks to different forms of employee monitoring, according to people with knowledge of the project's evolution, as well as updates to GitHub, a popular online repository for open-source projects.

Google itself has used the tool to catch people who share confidential information without permission.

When a screenshot of an upcoming Google product was leaked in 2015, for example, the company's security workers were able to use Grr to identify which employee computer was used to take the screenshot, said a former incident response employee. The tool helped the Google security team fetch the metadata of the image to determine things like the size of the computer display it was taken on, the screen resolution and the color profiles used on the device, the former employee said. Google identified an employee it suspected of leaking the information and fired that person.

Today, other companies in the tech industry use the system. Spotify previously relied on Grr for use in security investigations but no longer uses it, a spokesperson said.

At the same time, Google recently added features to its popular suite of online apps for businesses, Workspace, that are meant to thwart attempts by employees to leak corporate information outside their employers' systems. Google changed Workspace earlier this year to allow employers to block users from copying chat logs, documents and other data from their work accounts to their personal Google accounts.

The term “leaking” is a polarizing one, viewed in some circles as an expression that delegitimizes the sharing of confidential data outside a company. In some cases, people who release that information prefer the term whistle-blowers, which suggests they’re exposing wrongdoing by their employers. Someone anonymously filed a formal whistle-blower complaint against Google with the SEC earlier this year, alleging that the company could owe $100 million in back-pay to temporary employees, The New York Times **has reported**. It isn’t clear if the person is a Google employee. Google has said it is looking into the matter.

But defenders of the employee surveillance tactics used by Google and other tech companies say those tools are essential to preventing damaging loss of trade secrets.

One example of that threat was a 2016 incident in which Anthony Levandowski, an employee of what would become Google’s self-driving–car unit, Waymo, left to start a company that Uber bought soon afterward. Google sued Uber and Levandowski for theft of trade secrets, presenting records showing that he had downloaded thousands of confidential Google files onto his personal laptop before leaving the company.

Levandowski later pleaded guilty in a related criminal case and was **sentenced** to 18 months in prison, though **President Donald Trump pardoned him** before he served any time.

Still, despite such extreme examples, monitoring employees is a balancing act that can affect worker trust. The increased use of bossware, warned Ifeoma Ajunwa, associate professor of law at the University of North Carolina School of Law, brings greater opportunities for unlawful discrimination and the erosion of worker privacy.

“The employer certainly has a compelling interest in preserving its intellectual property interests,” said Ajunwa. “But that interest must be weighed against the human rights interest of privacy and personal autonomy for workers.”

Sarah Krouse (@bysarahkrouse) is a technology reporter for The Information. You can reach her via Signal at +1 (347) 436-5237.

Subscriber Comments

John Saddington