Revealed: The former Israeli spies working in top jobs at Google, Facebook and Microsoft

Description

***MintPress* study has found that hundreds of former agents of the notorious Israeli spying organization, Unit 8200, have attained positions of influence in many of the world's biggest tech companies, including Google, Facebook, Microsoft and Amazon.**

The Israeli Defense Forces' (IDF) Unit 8200 is infamous for surveilling the indigenous Palestinian population, amassing kompromat on individuals for the purposes of blackmail and extortion. Spying on the world's rich and famous, Unit 8200 hit the headlines last year, after the Pegasus scandal broke. Former Unit 8200 officers designed and implemented software that spied on tens of thousands of politicians and likely aided in the killing of Saudi journalist Jamal Khashoggi.

GOOGLE

According to employment website LinkedIn, there are currently at least 99 former Unit 8200 veterans currently working for Google. This number almost certainly underestimates the scale of the collaboration between the two organizations, however. For one, this does not count former Google employees. Nor does it include those without a public LinkedIn account, or those who do have an account, but have not disclosed their previous affiliations with the high-tech Israeli surveillance unit. This is likely to be a considerable number, as agents are expressly prohibited from ever revealing their affiliation to Unit 8200. Thus, the figure of 99 only represents the number of current (or extremely recent) Google employees who are brazenly flouting Israeli military law by including the organization in their profiles.

Among these include:

Gavriel Goidel: Between 2010 and 2016, Goidel served in Unit 8200, rising to become Head of Learning at the organization, leading a large team of operatives who sifted through intelligence data to "understand patterns of hostile activists", in his own words, transmitting that information to superiors. Whether this included any of the over 1000 Gazan civilians Israel killed during their 2014 bombardment

of Gaza is unknown. Goidel was recently appointed Head of Strategy and Operations at Google.

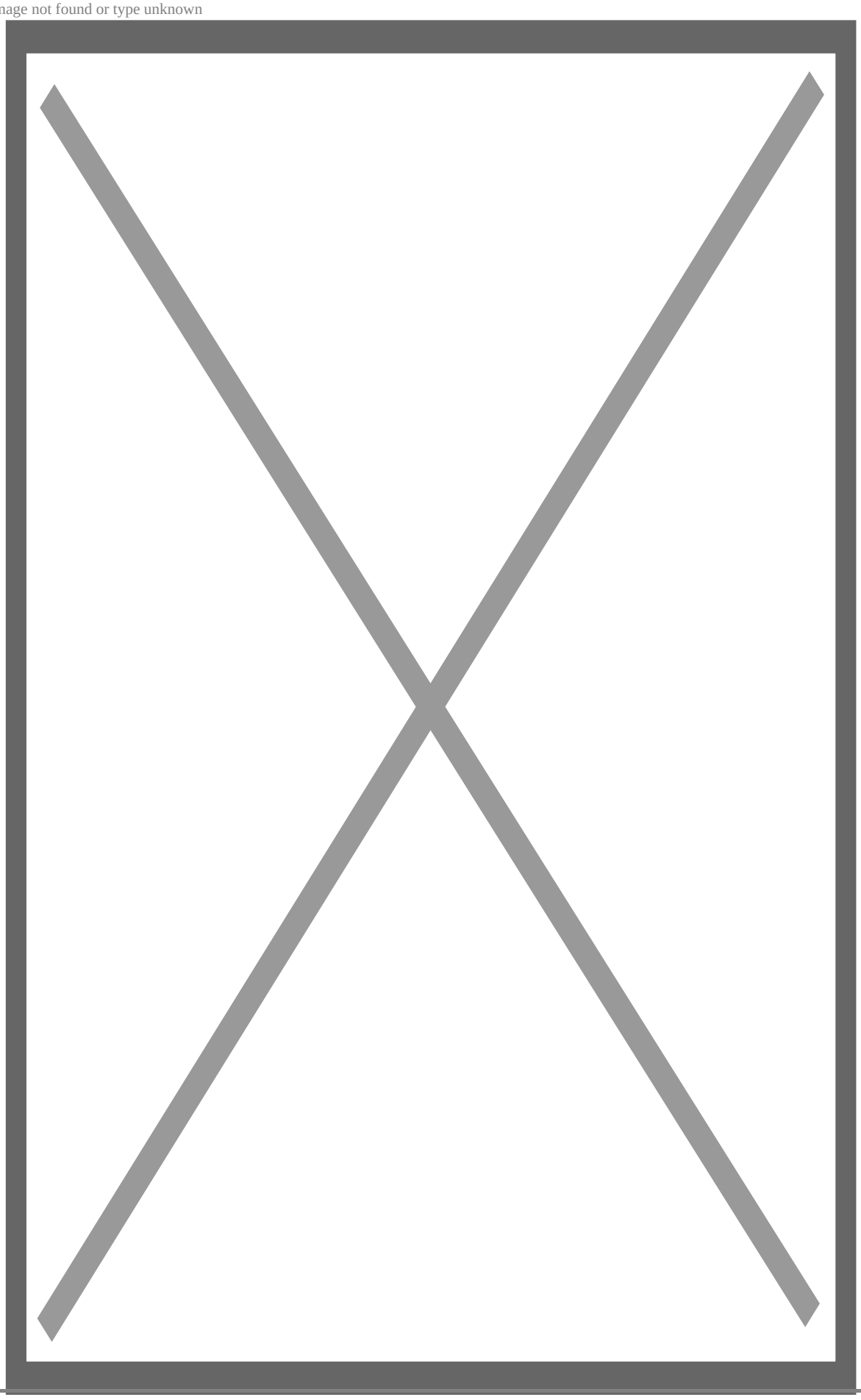
Jonathan Cohen: Cohen was a team leader during his time in Unit 8200 (2000-2003). He has since spent more than 13 years working for Google in various senior positions, and is currently Head of Insights, Data and Measurement.

Jonathan Cohen

Ori Daniel: Between 2003 and 2006, Daniel was a technical operations specialist with Unit 8200. After a stint with Palantir, he joined Google in 2018, rising to become Head of Global Self-Service for Google Waze.

Ben Bariach: For nearly five years between 2007 and 2011, Bariach served as a cyber intelligence officer, where he “commanded strategic teams of elite officers and professionals.”Since 2016, he has worked for Google. Between 2018 and 2020, he concentrated on tackling “controversial content, disinformation and cyber-security”. Today, he is a product partnership manager for Google in London.

Image not found or type unknown



Notably, Google appears to not only accept former Unit 8200 agents with open arms, but to actively recruit current members of the controversial organization. For example, in October 2020, **Gai Gutherz** left his job as a project leader at Unit 8200 and walked into a full time job at Google as a software engineer. In 2018, **Lior Liberman** appears to have done the same thing, taking a position as a program manager at Google after 4 years in military intelligence. Earlier this year, she left Google and now works at Microsoft.

SPYING ON PALESTINIANS

Some might contend that all Israelis are compelled to complete military service, and so, therefore, what is the problem with young people using the tech skills they learned in the IDF in civilian life. In short, why is this Unit 8200-to-Silicon-Valley-pipeline a problem?

To begin with, Unit 8200 is not a run-of-the-mill regiment. Described as “Israel’s NSA” and located on a gigantic base near Beer Sheva in the Negev desert, Unit 8200 is the IDF’s largest unit – and one of its most exclusive. The brightest young minds in the country compete to be sent to serve at this Israeli Harvard. Although military service is compulsory for Jewish Israelis, Arab citizens are strongly discouraged from joining the military and are effectively blocked from Unit 8200. Indeed, they are the prime targets of the apartheid state’s surveillance operations.

The Financial Times called Unit 8200 “Israel at its best and worst” – the centerpiece of both its burgeoning high-tech industry and of its repressive state apparatus. Unit 8200 veterans have gone on to produce many of the world’s most downloaded apps, including maps service Waze, and communications app Viber. But in 2014, 43 reservists, including several officers, sent a letter to Prime Minister Benjamin Netanyahu, informing him they would no longer serve in its ranks due to its involvement in the political persecution of Palestinians.

This consisted of using big data to compile dossiers on huge numbers of the indigenous domestic population, including their medical history, sex lives, and search histories, in order that it could be used for extortion later. If a certain individual needed to travel across checkpoints for crucial medical treatment, permission could be suspended until they complied. Information, such as if a person was cheating on their spouse or was homosexual, is also used as bait for blackmail. One former Unit 8200 man said that as part of his training, he was assigned to memorize different Arabic words for “gay” so that he could listen out for them in conversations.

Unit 8200

Image not found or type unknown

An award handed out to the IDF’s Unit 8200 for clandestine operations, June 24, 2020. Photo | IDF

Perhaps most importantly, the dissenters noted, Palestinians as a whole are considered enemies ofthe state. “There’s no distinction between Palestinians who are, and are not, involved in violence,” theletter read. It also claims that much intelligence was gathered not in service of Israel, but for powerfullocal politicians, who used it as they saw fit.

The letter, despite being intentionally vague and not naming anyone, was considered such a threat that Defense Minister Moshe Ya’alon announced that those who signed it would be “treated as criminals.”

In short, then, Unit 8200 is partially a spying and extortion organization that uses its access to data to blackmail and extort opponents of the apartheid state. That this organization has so many operatives (literally hundreds) in key positions in big tech companies that the world trusts with our most sensitive data (medical, financial, etc.) should be of serious concern. This is especially true as they do not appear to distinguish between “bad guys” and the rest of us. To Unit 8200, it seems, anyone is fair game.

PROJECT NIMBUS

Google already has a close relationship with the Israeli government. Last year, along with Amazon, it signed a $1.2 billion contract with Israel to provide military surveillance tech services – technology that will allow the IDF to further unlawfully spy on Palestinians, destroy their homes and expand illegal settlements.

The deal led to a staff revolt at both companies, with some 400 employees signing an open letter refusing to cooperate. Google forced one Jewish employee, Ariel Koren, out of the door for her part in resisting the deal. Koren later told *MintPress* that,

“Google systematically silences Palestinian, Jewish, Arab, and Muslim voices concerned about Google’s complicity in violations of Palestinian human rights – to the point of formally retaliating against workers and creating an environment of fear…in my experience, silencing dialogue and dissent in this way has helped Google protect its business interest with the Israeli military and government.”

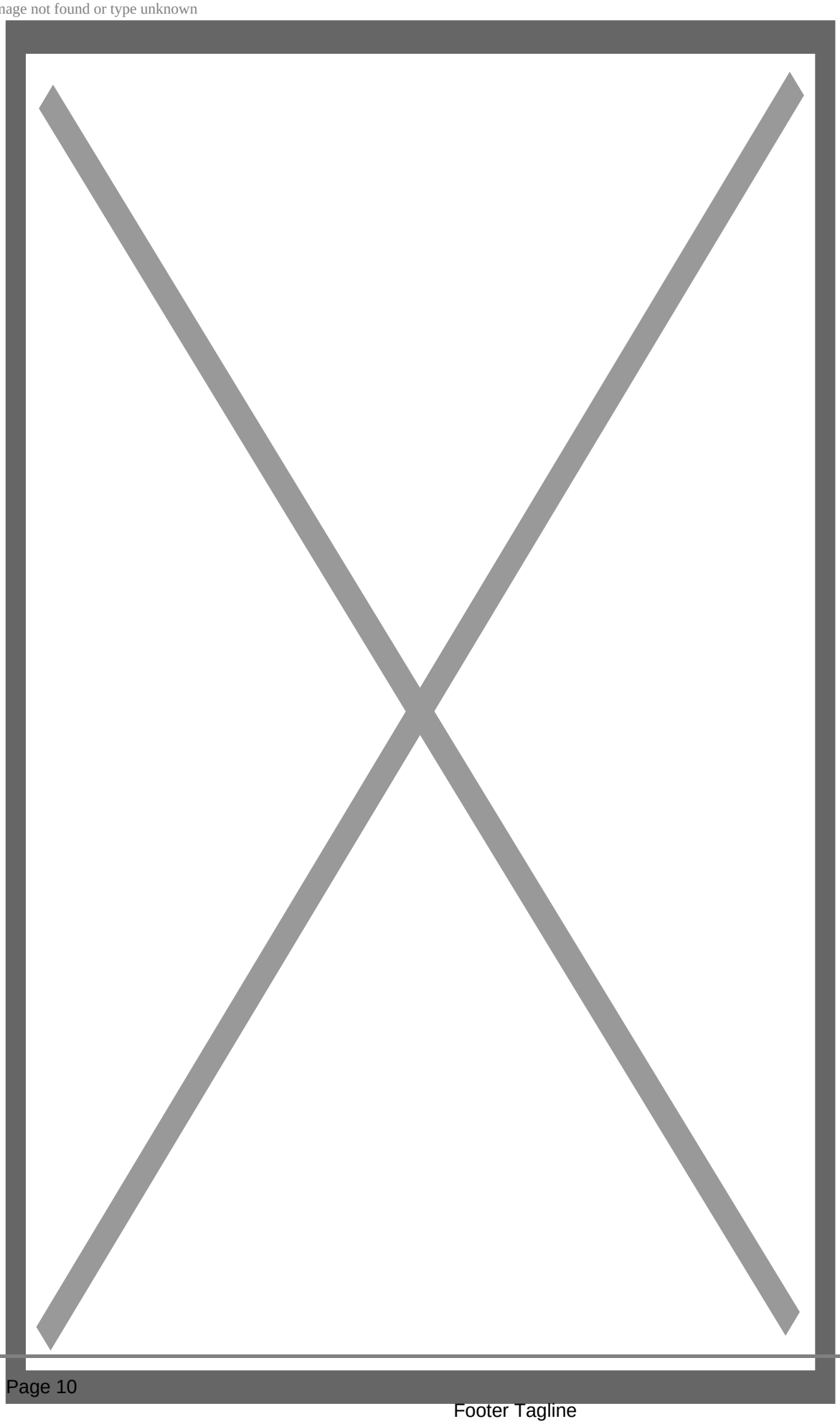
Another link between Google and the Israeli security state comes in the form of cybersecurity group Team8, a collaboration between former Google CEO and chairman Eric Schmidt, and three ex-Unit 8200 officers, including its former leader, Nadav Zafrir. Team8’s mission, according to a press release, is, “To leverage the offensive and defensive skills of veterans of Israel’s cyberwar efforts to build new security startups.”

META

Meta – the company that owns Facebook, Instagram and WhatsApp – has also recruited heavily from the ranks of Unit 8200.

Undoubtedly, one of the most influential people at Meta is Emi Palmor. Palmor is one of 23 individuals who sit on Facebook's Oversight Board. Described by Mark Zuckerberg as Facebook's "Supreme Court", the Oversight Board collectively decides what content to accept and promote on the platform, and what should be censored, deleted, and suppressed.

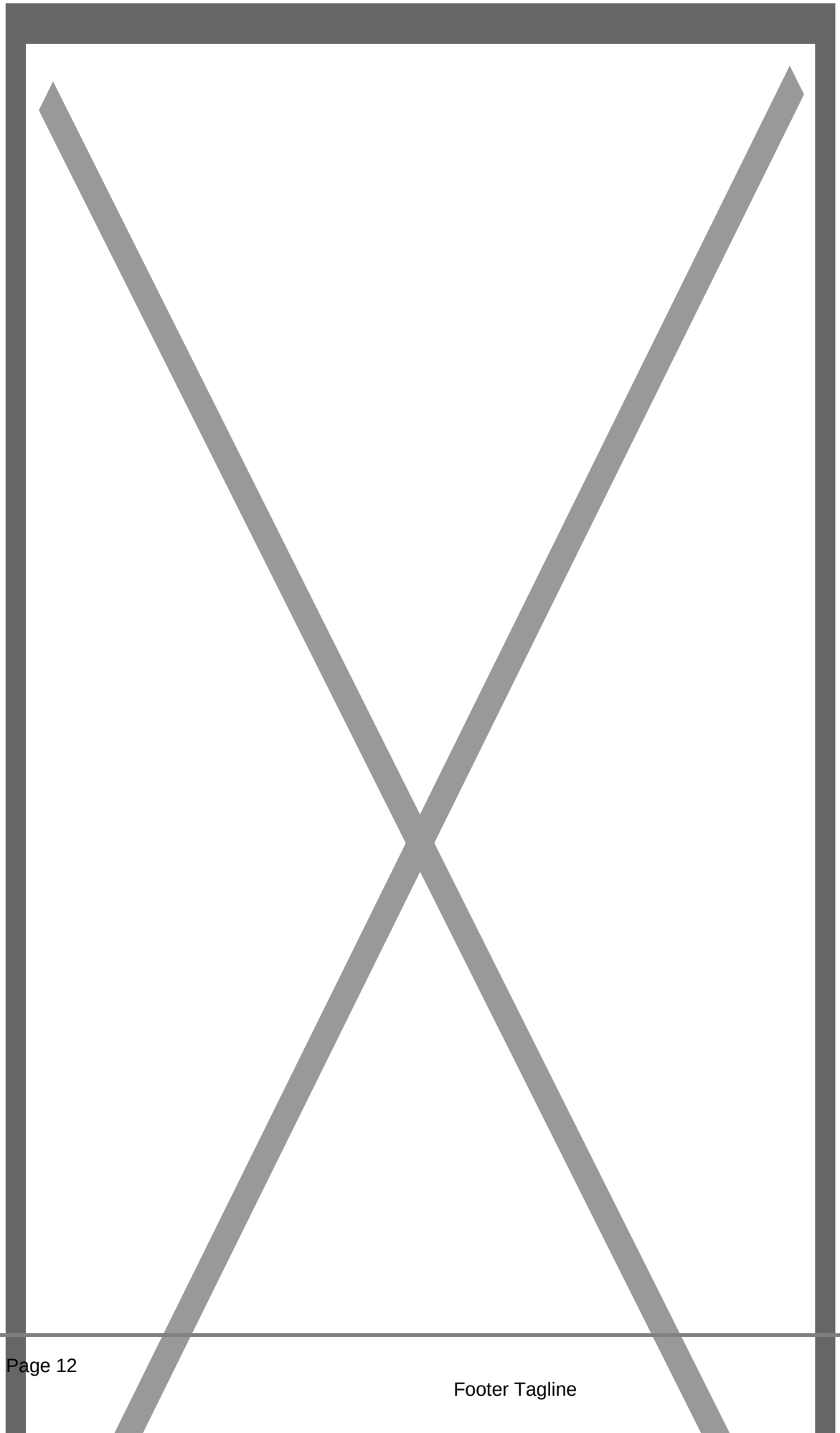
Image not found or type unknown



Palmor is a Unit 8200 veteran and later went on to become General Director of the Israeli Ministry of Justice. In this role, she directly oversaw the stripping away of Palestinian rights and created a so-called “Internet Referral Unit” which would find and aggressively push Facebook to delete Palestinian content on its platform that the Israeli government objected to.

Other ex-Unit 8200 hold influential positions. For instance, Eyal Klein, the head of data science for Facebook Messenger since 2020, served for fully six years as a captain in the controversial Israeli military unit. Today, he is tasked with handling privacy issues for billions of users of Meta’s platforms.

Image not found or type unknown



Another former Unit 8200 leader now working in big tech in America is Eli Zeitlin. Two years after leaving Unit 8200, Zeitlin was employed by Microsoft and rose to become the corporation's senior development lead, becoming, in his own words, the "go to person in file processing and cloud protection" for the company. For the last six years, however, he has worked for Meta, where he leads the company in "prevent[ing] data misuse by third parties" – exactly the sort of operation that current Unit 8200 officers likely continue to carry out.

Other Unit 8200 veterans working in influential roles for Facebook include Tom Chet, head of activations and production for North American small business; Gilad Turbahn, a manager for Meta; engineering manager Ranen Goren; software engineers Gil Osher and Yoav Goldstein; security engineering manager Dana Baril; and software developer Omer Goldberg. Meanwhile, according to Yonatan Ramot's LinkedIn biography, earlier this year, he was simultaneously working for Meta while still an active duty manager in Unit 8200.

SPYING ON THE WORLD

Why is having former Unit 8200 officers in charge of security, development and software design at some of the world's most important communications companies a problem? To start with, one of the military unit's primary functions is to use their tech know how to carry out spying operations across the world. As Israeli newspaper *Haaretz* noted in an investigation, "Israel has become a leading exporter of tools for spying on civilians," selling invasive surveillance software to dozens of governments, many of them among the world's worst human rights abusers. In Indonesia, for instance, the software was used to create a database of gay people.

Unit 8200 also spies on Americans. Whistleblower Edward Snowden revealed that the NSA regularly passes on the data and communications of U.S. citizens to the Israeli group. "I think that's amazing…It's one of the biggest abuses we've seen," Snowden said.

The most well-known example of Israeli spyware is Pegasus, a creation of NSO Group, a technically private company staffed primarily by Unit 8200 veterans. The software was used to eavesdrop on more than 50,000 prominent people around the world. This included dozens of human rights defenders, nearly 200 journalists, several Arab royals, and over 600 politicians, including French president Emmanuel Macron, Pakistani prime minister Imran Khan and Iraqi President Barham Salih.

Meanwhile, Indian prime minister Narendra Modi used the software to dig up dirt on his personal opponents. Other members of his government hacked the phone of a woman accusing the Chief Justice of India of raping her.

Pegasus was also found installed on murdered *Washington Post* journalist Jamal Khashoggi, implying that NSO was collaborating with the Saudi government, aiding them to silence dissent and criticism.

Pegasus works by sending a text message to a targeted device. If a user clicks on the link provided, it will automatically download the spyware. Once infected, it is possible to track an individual's location and movements, take screenshots, turn on the phone's camera and microphone, retrieve messages and steal passwords.

But while the NSO's Pegasus made worldwide news, another firm, more worrying and dangerous, has flown under the radar. That firm is Toka, established by former Israeli defense minister and prime minister, Ehud Barak, with the help of a number of Unit 8200 officers. Toka can infiltrate any device connected to the internet, including Amazon echoes, televisions, fridges and other home appliances. Last year, Journalist Whitney Webb told *MintPress* that the company effectively acts as a front group for the Israeli government's spying operations.

A third private spy firm filled with Unit 8200 graduates is Candiru. The Tel Aviv-based company barely exists, officially. It does not have a website. And if you go to its headquarters, there is no indication that you are in the right place. Nevertheless, it is widely believed that Candiru was behind malware attacks observed in Saudi Arabia, the United Arab Emirates, Singapore, Qatar and Uzbekistan.

The company is named after a parasitic Amazonian fish that is said (apocryphally) to swim up human urine streams and enter the body via the urethra. It is an apt analogy for a firm that spends its time finding security flaws in Android and iOS operating systems and browsers like Chrome, Firefox and Safari, using this knowledge to spy on unsuspecting targets.

The utility of these technically private Israeli spy groups filled to the brim with ex-military intelligence figures is that it allows the government some measure of plausible deniability when carrying out attacks against foreign nations. As *Haaretz* explained, "Who owns [these spying companies] isn't clear, but their employees aren't soldiers. Consequently, they may solve the army's problem, even if the solution they provide is imperfect."

MICROSOFT

Data from LinkedIn suggests that there are at least 166 former Unit 8200 members who went on to work for Microsoft. In addition to those already mentioned, others include Ayelet Steinitz, Microsoft's former Head of Global Strategic Alliances, Senior Software Engineer Tomer Lev, and Senior Product Managers, Maayan Mazig, Or Serok-Jeppa and Yuval Derman.

Maayan Mazig

Image not found or type unknown

Notably, the Seattle-based giant also heavily leans on ex-Unit 8200 professionals to design and upkeep its global security apparatus. Examples of this phenomenon include Security Researchers Lia Yeshoua, Yogev Shitrit, Guni Merom, Meitar Pinto and Yaniv Carmel, Threat Protection Software Engineer Gilron Tsabkevich, Data Scientist Danielle Poleg, Threat Intelligence Officer Itai Grady and Security Product Manager Liat Lisha. In Merom, Carmel and Pinto's cases, they went straight from Unit

8200 into Microsoft’s team, again suggesting that Microsoft is actively recruiting from the regiment.

Lia Yeshoua

Image not found or type unknown

Other Microsoft security products such as Microsoft Defender Antivirus and Microsoft Azure secure cloud computing are also designed and maintained by ex-Unit 8200 individuals. These include former Senior Architect Michael Bargury, Principal Software Engineering Manager Shlomi Haba, Senior Software Engineering Managers Yaniv Yehuda, Assaf Israel and Michal Ben Yaacov, Senior Product Manager Tal Rosler, Software Engineer Adi Griever, and Product Manager Yael Genut.

Yaniv Yehuda

This is notable, as it was reported that malware likely produced by Unit 8200 was used to attack Microsoft products, such as its Windows operating system. It reportedly exploited loopholes it found to attack control systems, delete hard drives, and shut down key systems, such as the energy infrastructure of Iran.

BIG TECH, BIG GOVERNMENTS

None of this means that all or even any of the individuals are moles – or even anything but model employees today. But the sheer amount of people graduating from an organization such as Unit 8200 and going on to influence the world's largest communications companies certainly causes concern.

Unit 8200 certainly has a reputation for excellence in its field. The trouble is that their craft includes spying, extortion, gross violations of personal rights, and the hacking of exactly the tech companies that are now hiring them en masse. This does not appear to be a poacher-turned-gamekeeper scenario, however; there is no indication Silicon Valley is hiring whistleblowers.

Of course, Israel is far from the only country that attempts to spy on foes or manipulate the public. However, former spies from adversary countries such as Russia, Venezuela or Iran are not being hired in their hundreds to design, maintain and oversee the largest channels of public communication. In fact, this study could find no examples of ex-FSB (Russia) ex-SEBIN (Venezuela) or former agents from the Iranian Ministry of Intelligence working at Silicon Valley corporations.

MintPress has previously documented how, in recent years, big tech companies like Twitter, Facebook, Google, TikTok and Reddit have hired hundreds of spooks from the CIA, NSA, FBI, Secret Service, NATO, and other intelligence agencies. The fact that Unit 8200 is also a recruitment reserve underlines how strong an ally Israel is considered in the West.

However, it also highlights the increasing intersection between Silicon Valley and big government and further undermines any pretense that big tech companies are on our side in the fight to secure and maintain privacy online.

By Alan MacCleod

Category

1. Main
2. NWO-Deep State-Dictatorship-Tyrrany
3. Science-Tech-AI-Medical & Gen. Research

Date Created
11/22/2022