The "Independent" Internet Freedom Organization That Makes All Your Favorite Privacy Apps – is Staffed Full of Spies

By Alan Macleod

WASHINGTON – The Open Technology Fund (OTF) is one of the most influential and celebrated organizations in the hacking and internet freedom communities. Well over two billion people globally use OTF-produced software, including communications app Signal and web browser Tor, services that are specifically marketed to privacy-conscious consumers looking to circumvent government censorship and surveillance. Yet its close links to the U.S. national security state raise many worrying questions about whether the world is making a mistake by trusting the organization and its products.

Through its research and sponsorship, the OTF is responsible for apps and services that can boast a massive reach. It is estimated that more than two-thirds of all smartphones are equipped with OTF offerings, apps that brand themselves as the obvious choice for privacy-minded users.

The OTF describes itself as "an independent non-profit organization committed to advancing global Internet freedom," adding that it "supports projects focused on counteracting repressive censorship and surveillance, enabling citizens worldwide to exercise their fundamental human rights online."

There is strong evidence, however, to suggest that the Open Technology Fund is not what it claims to be: that it is neither independent nor truly committed to online freedom and privacy. First, while technically a private company, it is directly funded and controlled by the United States Agency for Global Media (USAGM), a government body responsible for overseeing U.S.-funded state media outlets overseas, including *Radio Free Europe/Radio Liberty*, *Voice of America* and *Radio* and *Televisión Martí*. The OTF derives essentially all of its funding from USAGM, which, in turn, receives money from Congress through the Department of State, Foreign Operations and Related programs ($808 million in 2019).

Secondly, until 2019, the OTF was officially a government project managed by the infamous *Radio Free Asia*. Together, *The New York Times* described these outlets as a "worldwide propaganda network built by the CIA." Even a brief look at their content suggests that this is essentially an accurate description, with USAGM brought into existence to manage CIA-created media outlets.

This alone would be enough to raise questions. However, the OTF's definition of freedom should sound even more alarm bells. In its most recently published annual report, it describes its mission as:

…Advanc[ing] internet freedom in repressive environments by supporting the research, development, implementation, and maintenance of technologies that provide secure and uncensored access to USAGM content as well as the

broader internet. This critical support helps to counter attempts by authoritarian governments to restrict freedom online.

Internet freedom, according to the OTF, is explicitly defined in relation to access to U.S. state propaganda arms. If individuals in a country have access to *Voice of America* and *Radio Free Asia*, then their internet is free. If not, they live in a totalitarian state. Internet freedom boils down to the freedom of the U.S. government to reach you. Any other understanding of the concept is, at best, an afterthought.

The report also states that the OTF exists primarily for two purposes: (1) to "[p]rovide unrestricted access to the internet to individuals living in information-restrictive countries to help ensure they are able to safely access USAGM content," and (2) to [p]rotect journalists, sources, and audiences from repressive surveillance and digital attacks to help ensure they are able to safely create and engage with USAGM content." This is unlikely to be the idea of freedom that many privacy-conscious users of Signal and Tor have in mind.

That this operation is pointed specifically at U.S. enemies is made clear on the fund's website, which states that "leading censors like China and Russia" are "exporting their censorship and surveillance tactics to like-minded regimes abroad," and that the OTF must "capitalize on its unique capability within the U.S. government to support internet freedom efforts," thereby positioning Washington as the unquestioned defender of liberty around the world.

Of course, China and Russia do indeed have very serious censorship concerns, but they are hardly alone in that regard. Thus, while the fund speaks in the language of privacy and social justice, its targets are overwhelmingly U.S. enemy states. Meanwhile American allies with equally poor or worse free speech environments (such as Saudi Arabia or Qatar) are quietly overlooked.

A board of state functionaries

Not only was the Open Technology Foundation created by the national security state, it continues to employ high government officials in key positions. Its five-person board consists entirely of important state functionaries:

- Karen Kornbluh was formerly U.S. ambassador to the OECD, Barack Obama's policy director, deputy chief of staff at the Treasury Department, and a senior figure at the FCC during the Clinton administration.
- Ben Scott was previously policy adviser for innovation at the Department of State, where, in the OTF's words, he crafted the government's 21st Century Statecraft agenda.
- Top Democratic fundraiser Michael Kemper served as the DNC's deputy finance chairman as well as deputy finance coordinator for President Obama. He also held a position on the White House Council for Community Solutions from 2010 to 2012.
- William Schneider is a Republican who was Ronald Reagan's under secretary of state for Security Assistance, Science and Technology. He

is also a member of the notorious neoconservative group, the Project for a New American Century. In 1998, he signed a letter to President Bill Clinton, urging him to attack Iraq. A science expert, he has consistently argued that the U.S. should use nuclear weapons as a standard part of its warfare.

- Even more central to the post-9/11 wars, however, is the fifth member of the board, Ryan Crocker. Crocker was United States ambassador to both Iraq (2007-2009) and Afghanistan (2011-2012). So important was he to the occupations that General David Petraeus, supreme commander of the occupation forces, said that he was merely Crocker's "military wingman." George W. Bush described him as "America's Lawrence of Arabia."

For such a group of individuals, who have spent their lives dedicated to enhancing U.S. state power, it appears unlikely that freedom from state surveillance would be high on their list of priorities. Underlining that the Open Technology Fund's concern with privacy and freedom of speech goes only so far is its choice of CEOs, who have included the former director of programming for *Voice of America*, the former president of *Radio Free Asia*, and an ex-State Department and National Endowment for Democracy official.

Thus the OTF – a "private" company that was created by government agencies and was a government body itself until 2019 – is staffed by top U.S. officials who have been chosen by the USAGM. The veneer of independence actually serves two important purposes: it provides the U.S. government a modicum of plausible deniability if any misdeeds are exposed and ensures that the organization is not subject to Freedom of Information Act requests, making the OTF far harder to scrutinize. This semi-privatization technique is a new trend in U.S. statecraft. In recent years, the government has farmed out much of its most controversial clandestine work to NGOs and shadowy "private" companies that rely largely or solely on federal contracts. For example, NGOs like Creative Associates International have been employed to organize regime-change ops in Cuba or act as a front group for the CIA in Pakistan. Last year, a private American security firm was also responsible for a failed coup attempt in Venezuela.

OTF genesis

Radio Free Asia — the Open Technology Fund's former parent organization — was established by the CIA in 1951, in the wake of the American retreat from China. Between 1945 and 1949, the United States occupied mainland China in an attempt to support the nationalist Kuomintang forces and prevent Communist forces under Mao Zedong from coming to power. In this, they failed, and the Kuomintang fled to the island of Taiwan, just off China's coast. The powerful U.S. Navy prevented the Communists from pursuing them, allowing the Kuomintang to establish a one-party state on the island. This remains the basis of the current U.S.-China-Taiwan dispute.

During the 1950s, *Radio Free Asia* bombarded the mainland with anti-Communist propaganda in an attempt to weaken and, ultimately, unseat the

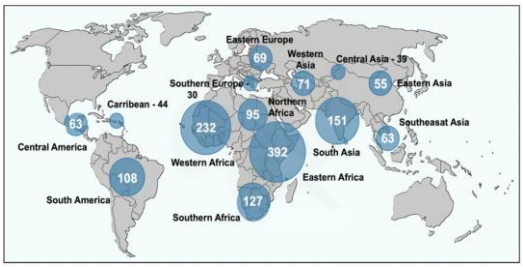
Communist Party. However, results were poor and the project was put on ice, returning only in the 1990s after the fall of the Soviet Union, when U.S. planners began to believe a total eradication of communist states was possible. Yasha Levine, an investigative journalist and author of "Surveillance Valley: The Secret Military History of the Internet," explained to *MintPress* that Beijing began blocking *Radio Free Asia*'s website almost as soon as it was launched in 1996. Consequently, its bosses began searching for a way of circumventing the Great Firewall of China. It was out of this project that the Open Technology Fund was born.

OTF's role in US-backed "pro-democracy" protests

The OTF has played a key role in U.S.-backed protest movements around the world. During the 2019-2020 Hong Kong protests, it was quietly channeling millions of dollars to protest leaders in an attempt to keep them going. It was also carrying out large-scale data-gathering operations on Chinese social media platforms Weibo and Wechat. CIA cutout organization the National Endowment for Democracy (NED) was engaged in similar activities.

For months, the Hong Kong protests dominated Western news media, with wall-to-wall positive coverage of the events. Yet locals themselves appeared to be far more split on the action. A poll conducted by *Reuters* showed that, by August 2020, only 44% of Hong Kongers supported the protest movement. The Open Technology Fund has also been crucial to Washington's activities in Cuba. There, it sponsored the development of Psiphon, an open-source tool that allows users to hide their identity and bypass government restrictions.

The NED had, for years, been spending big to build and train a network of activists across the island. When the time came, they were ready. "During the protest in July, Psiphon enabled over 2.8 million users to connect to the uncensored internet, allowing them to share their stories on social media and messaging apps," boasted the company's CEO, Michael Hull. "Giving [Cubans] those tools so they can talk to each other is the most important thing that we can do," a senior Biden administration official told *McClatchy*'s D.C. Bureau. "We're looking to further expand our support for the Open Technology Fund and those sorts of [operations]," they added. As with Hong Kong, worldwide media coverage of the Cuban protests was intense. Yet the demonstrations fell apart even quicker, as few Cubans had an appetite for regime change.



A map from a 2018 OTF report shows regions where so-called "Internet freedom communities" have applied for OTF assistance

The OTF is also known to have supported similar recent actions in Belarus, Iran and Venezuela. In Belarus, it trained the opposition to President Alexander Lukashenko, its agents carrying out ten separate tours of the country, holding meetings with representatives of what it deemed "independent mass media, human rights defenders and civil activists." In total, it conducted at least 225 consultations with Belarussian groups in 16 months during 2017 and 2018 alone. They also provided training sessions for these activists. Sure enough, widespread demonstrations followed, with the goal of removing Lukashenko. The leaders of the movement were "installed and maintained" by the OTF, according to *The Guardian*.

While these operations are couched in the language of promoting democracy, it is clear at whom the OTF aims its tools. In its latest published yearly report, for example, the words "China" or "Chinese" appear 81 times, "Russia" or "Russian" 27 times, "Iran" 24 times and "Venezuela" 13 times. Yet Bahrain, Saudi Arabia and Qatar — three U.S. allies with particularly egregious media freedom records — are mentioned only once, in passing.

"An anarchist Lockheed Martin"

This long and sordid history certainly raises questions about the legitimacy and safety of the OTF's two most popular products, Signal and Tor. Between 2013 and 2016, the OTF channeled more than $3 million to Signal, while it gave twice that amount — more than $6 million — to Tor between 2012 and 2020. (Tor continues to be sponsored by a number of U.S. government agencies).

Certainly, all parties involved keep this information quiet. There is no mention of the OTF on Signal's website. Meanwhile, reading the three organizations' Wikipedia pages would barely clue an individual in on their connections. This is not a coincidence. Emails Levine obtained under the Freedom of Information Act show that Tor Project director and co-founder Roger Dingledine (who once interned at the NSA) was acutely aware of how bad the optics were.

"We also need to think about a strategy for how to spin this move in terms of Tor's overall direction. I would guess that we don't want to loudly declare war on China, since this only harms our goals?" he wrote to the director of OTF parent company USAGM. "But we also don't want to hide the existence of funding from [USAGM], since 'they're getting paid off by the feds and they didn't tell anyone' sounds like a bad *Slashdot* title for a security project. Is it sufficient just to always talk about Iran, or is that not subtle enough?"

The wording of this email suggests Dingledine views Tor as a U.S. government weapon aimed at its enemies, and not as a neutral and independent privacy project, but was searching for a way to present it as such. The director of USAGM reassured him, responding that his organization would, "do any spin you want to do to help preserve the independence of Tor."

Levine was highly critical of Tor's role in society. "Tor is a military contractor that makes software for the U.S. government. They're an anarchist Lockheed Martin; they give the U.S. government offensive capability on the internet. Of

course, they are not making missiles, but they are making cyber weapons for Washington," he told *MintPress*.

American agents use the browser to communicate. Ironically, the influx of new users actually helps them disappear into the crowd. Without the hackers, drug dealers, cyberpunks, crypto-enthusiasts, political activists and privacy-minded individuals using it, the identities and locations of U.S. agents would become obvious to foreign states monitoring online activities. In other words, when you use Tor, you're helping the CIA.

Does Tor or Signal's proximity to American intelligence mean that their products are fundamentally compromised? Enthusiasts point to their checkable, open source code as proof that they are secure. Even Levine does not challenge this. However, the enormous complexity of the operating systems they run on is a serious cause for concern. While many have checked Tor and Signal's source code, few except state actors pore over the countless billions of lines of code of the software on our phones or computers — and they are doing it to find ways to exploit or attack the millions of holes and backdoors in the operating systems. Big governments can ultimately find a way to get to the data before it is encrypted, Levine argued, meaning that:

Signal and Tor offer a false sense of security. It depends who you are trying to hide from. If it is your local police department and you are using Signal, it is probably good enough. But if you are engaged in some kind of political protest building, organizing and challenging state power on some level, I would not be dependent on Signal to do it."

Since at least 2014, the FBI has been closely monitoring Tor, assessing users' exit nodes (the false IP address that a server sees). Independent tests conducted by Columbia University found that researchers were able to identify over 81% of Tor users in real-world tests.

Ultimately, then, Signal and Tor could be compared to an expensive home security system. The product might be high quality and secure enough to stop petty thieves or even committed professional burglars. But if the FBI wants to enter your house, they will simply ram the door down. "On a fundamental level, I don't think that privacy exists," Levine said. "To think that, as a regular consumer, you can take on the state with some app that you download for free… It's just ridiculous. It's a joke."

A dubious endorsement

Unfortunately, both Signal and Tor have developed large and devoted followings, being used the world over and endorsed by groups like the Electronic Frontier Foundation (EFF) and high profile privacy advocates. "The problem with Signal is not the technology, it is the marketing behind it. It has this *cachet* of being radical anarchist software that is backed by people like Edward Snowden. It has cultural capital," Levine told *MintPress*; "They have created a cult of security around this app that does not exist. Not just for Signal, but for any other app."

Perhaps more worryingly, the Electronic Frontier Foundation has also heartily endorsed the OTF, stating that the organization has "earned trust over the years through its open source ethos, transparency, and a commitment to independence from its funder, USAGAM." "OTF's funding is focused on tools to help individuals living under repressive governments," EFF adds.

Unfortunately, the EFF is fundamentally intertwined with the national security state itself, with several of its staff serving on the OTF advisory council. In the 1990s, the EFF collaborated with the FBI to pass the so-called "Let's Just Wiretap Everyone Bill," rewriting the bureau's draft legislation to make it sound more palatable to the public. That bill became the basis for a great deal of the FBI's continuing invasive online surveillance. The OTF has also sponsored a number of EFF projects. *MintPress* contacted the EFF for comment, but did not receive a reply.

A concealed weapon in the global cyberwar

While at face value Tor and Signal may be robust, the fact that significant parts of the internet freedom and anti-surveillance movement are intertwined with the U.S. national security state does seem an absurd contradiction. The NSA lied for years, even under oath, that it was not spying on Americans. In reality, it was collecting reams of data on just about everyone. The U.S. was even intimately surveilling its closest international allies, such as German chancellor Angela Merkel. Given such a history, what could possibly be done to assuage fears that a similar operation is not currently being executed?

While the OTF presents itself as independent internet freedom activists, their funding, staff, history and choice of targets all point to the conclusion that they are a digital weapon being used against Washington's enemies.

Thus, their talk of "freedom of information" is reminiscent of discussions about "free markets." Freedom of information is currently being championed by the government that dominates and controls the internet and is in a position to use that leverage to carry out its international ambitions. And while the U.S. talks piously about freedom of information, whenever foreign-owned communications companies begin to succeed — such as Chinese-owned Huawei or TikTok — there is a meltdown, followed by an all-out attack from Washington, which fears they will be weaponized in similar ways Washington has weaponized Silicon Valley.

A silent war is being waged for control of cyberspace. And in war, truth is always the first casualty.

Apple has made headlines in recent weeks for touting its commitment to privacy and human rights, rolling out tools to limit surveillance and spyware. But behind the corporate messaging lies a much darker reality.

The company has quietly brought in dozens of veterans from Unit 8200, Israel's shadowy military intelligence unit known for blackmail, mass surveillance, and targeted killings.

Many of these hires took place as Israel escalated its war on Gaza, and as CEO Tim Cook publicly expressed support for Israel while disciplining employees for pro-Palestinian expressions. Apple's deepening ties to Israel's most controversial intelligence raise uncomfortable questions, not only about the company's political loyalties, but also about how it handles vast troves of personal user data.

A MintPress News investigation has identified dozens of Unit 8200 operatives now working at Apple. The company's hiring spree coincides with growing scrutiny of its ties to the Israeli government, including its policy of matching employee donations to groups such as Friends of the IDF and the Jewish National Fund, both of which play a role in the displacement of the Palestinian people. The intense pro-Israel bias at the corporation has led many former and current employees to speak out.

This investigation is part of a series examining the close collaboration between Unit 8200 and Western tech and media companies. Previous investigations examined the links between Unit 8200 and social media giants like TikTok, Facebook and Google, and how former Unit 8200 spies are now responsible for writing much of America's news about Israel/Palestine, holding top jobs at outlets like CNN and Axios.

A Few (Dozen) Bad Apples

Israel's international reputation has taken a severe hit amid multiple spying scandals and ongoing attacks against its neighbors. During this same period, Apple has ramped up its recruitment of former Israeli intelligence personnel.

The Silicon Valley giant has hired dozens of former agents from the controversial Israeli intelligence outfit, Unit 8200, raising questions about the corporation's political direction.

Nir Shkedi is among the most prominent examples. From 2008 to 2015, he served as a commander and Chief of Learning at Unit 8200, leading a team of approximately 120 operatives who developed new artificial intelligence tools to perform rapid data analysis.

Unit 8200 is at the forefront of this technology, and is known to have used AI to auto-generate kill lists of tens of thousands of Gazans, including children. These tools helped the Israeli Defense Forces (IDF) bypass what it called human targeting, "bottlenecks," and strike huge numbers of Palestinians.

Shkedi has been a physical design engineer at Apple's Bay Area campus since 2022.

Noa Goor is another senior Unit 8200 figure turned Apple employee. From 2015 to 2020, Goor rose to become a project manager and head of cybersecurity and big data development team at Unit 8200, where she, in her own words, "invent[ed] creative technological solutions for high priority intelligence goals" and "manag[ed] two strategically important cyber projects" for the IDF.

One of the most important cyber projects Unit 8200 has launched in recent times is the September pager attack on Lebanon, an act that injured thousands of civilians and was widely condemned as an act of international terrorism, including by former CIA Director Leon Panetta. While Goor was not personally involved in that operation, Unit 8200 has spearheaded similarly nefarious actions for decades.

In 2022, Goor was hired by Apple as a system-on-chip design engineer.

Eli Yazovitsky, meanwhile, was directly recruited from Unit 8200. In 2015, he left a high-powered nine-year career as a manager in the military unit to join Apple, where he rose to become an engineering manager. He has since moved on to tech giant Qualcomm.

Unit 8200 is Israel's most elite—and most controversial—military intelligence unit. It serves as the backbone of both Israel's burgeoning tech sector and its repressive surveillance apparatus. The unit has developed cutting-edge technology like facial recognition and voice-to-text software to surveil, repress, and target Palestinians.

The vast amounts of data gathered on the Palestinian population, including their medical history, sex lives, and search histories, have been used for coercion and extortion. If a certain individual needed to travel across checkpoints for crucial medical treatment, permission could be suspended until they complied. Information about extramarital affairs or sexual orientation, especially homosexuality, is exploited as blackmail material. One former Unit 8200 agent recalled that he was instructed during his training to memorize different Arabic words for "gay" so that he could listen out for them in intercepted conversations.

Internationally, Unit 8200 may be best known for its "former" agents who created the notorious Pegasus software, used by repressive governments around the world to spy on tens of thousands of prominent figures, including royals, heads of state, activists, and journalists.

Among them was Washington Post columnist Jamal Khashoggi, who was assassinated by Saudi operatives in Türkiye in 2018.

While military service is mandatory for Jewish Israelis, few end up in Unit 8200 by accident. Described as "Israel's Harvard," parents spend fortunes on STEM-based extracurricular lessons for their children in the hopes that they will be selected to join the IDF's most elite and selective unit. Those chosen are rewarded with lucrative careers in the tech industry upon completion of their service.

Given Unit 8200's documented history of violence, espionage, and surveillance, both domestically and internationally, it is worth asking whether tech giants should be hiring its alumni in such large numbers.

Shkedi, Goor, and Yazovitsky are the most high-profile examples, but they are from alone. A closer look reveals that dozens of other Unit 8200 veterans have also secured key roles at Apple.

Engineering and Hardware Design:

Natanel Nissan, formerly head of data analysis at Unit 8200, joined Apple's Tel Aviv office in 2022. Ofek Har-Even, a longtime officer and manager in the unit, has been a design verification engineer at Apple since 2022. Gal Sharon, a former intelligence systems operator and data analyst, has also worked as a physical design engineer since that same year.

Mayan Hochler and Shai Buzgalo, both former Unit 8200 analysts and instructors, hold roles in physical design and validation engineering, respectively.

Software and Cybersecurity:

Ofer Tlusty, who served nearly six years in Unit 8200 as a security and intelligence analyst, has worked as a software engineer at Apple since 2021. Ofek Rafaeli, who served between 2012 and 2016 and rose to project manager during Israel's 2016 assault on Gaza, became a software engineer at Apple in 2023.

Guy Levy, a former intelligence analyst, now also works as a software engineer.

AI, Machine Learning, and Validation:

Avital Kleiman, a six-year veteran of Unit 8200, is now a machine learning algorithm engineer at Apple. Niv Lev Ari, currently a validation engineer, notes in his LinkedIn profile that he received a letter of commendation from Unit 8200 commander Aviv Kochavi for his work in the unit.

Other Technical Roles:

Shahar Moshe, who worked as an intelligence specialist at Unit 8200 from 2012 to 2015, is now a design verification engineer. Gil Avniel, who spent over five years in the unit, currently serves as a network engineer.

An Apple Rots From the Core

The growing number of former Israeli intelligence operatives working at Apple does not seem to concern the company's senior management. CEO Tim Cook is known to hold strongly pro-Israel views and has spearheaded the Silicon Valley giant's collaboration with the Israeli state.

Apple has acquired several Israeli tech firms and now operates three centers in the country, employing around 2,000 people. In 2014, Cook invited Israeli Prime Minister Benjamin Netanyahu to the company headquarters in Cupertino, CA, where, in front of the cameras, the two openly embraced. The following year,

Cook accepted an invitation from President Reuven Rivlin to visit Israel. “It is a great privilege to host you and your team here,” Rivlin said, “Even for me, as one who prefers to write with a pen and paper, it is clear what a great miracle you have created when I look at my staff, and my grandchildren.”

Effusive praise for the Apple CEO has also come in the form of honors from pro-Israel organizations. In 2018, the Anti-Defamation League presented Cook with its inaugural Courage Against Hate Award at its Never Is Now Summit on anti-Semitism and Hate, where the organization described him as a “visionary leader in the business community.”

In the wake of the October 7, 2023, attacks, Cook sent out a company-wide email expressing his solidarity with Israel. “Like so many of you, I am devastated by the horrific attacks in Israel and the tragic reports coming out of the region,” he wrote, My heart goes out to the victims, those who have lost loved ones, and all of the innocent people who are suffering as a result of this violence.”

Yet, according to Apples4Ceasefire—a group of former and current employees opposing Israeli actions in Gaza—he has yet to say anything publicly about the mass devastation caused by the Israeli response to October 7.

Indeed, the Silicon Valley corporation has a policy of matching employee donations to groups such as Friends of the IDF, which raises money to buy equipment for IDF soldiers, and the Jewish National Fund, an organization that participates in the theft and destruction of Palestinian land.

Under Cook’s leadership, Apple employees have been disciplined or even fired for wearing pins, bracelets, or keffiyehs in support of the Palestinian people. Nevertheless, groups such as Apples4Ceasefire continue to speak out about what they describe as Apple’s complicity in genocide.

The Unit 8200 Tech Takeover

To be fair, Apple is far from the only tech or media company to hire large numbers of former Unit 8200 operatives. A 2022 MintPress exposé revealed hundreds of Israeli intelligence veterans working at Google, Facebook, Microsoft, and Amazon.

Perhaps the most notable of these is Emi Palmor, a former Israeli justice ministry official who sits on Facebook’s 21-person Oversight Board. Described by Mark Zuckerberg as his platform’s “supreme court,” the board ultimately decides what content is allowed or removed from the world’s largest social network. Facebook has worked closely with the Israeli government to censor or deplatform Palestinian content and accounts.

Even TikTok, often seen as a more open platform, has been hiring former Israeli spies to help manage its operations, according to a November investigation by MintPress. Reut Medalion, for example, served as a Unit 8200 intelligence commander and led its cybersecurity operations team.

In December 2023, during the peak of Israel's attack on Gaza, Medalion moved to New York City to accept a job as global incident manager for TikTok's trust and safety division. Considering the events going on in the world at the time, it's worth asking what sorts of "global incidents" she was brought in to manage.

After MintPress exposed Medalion's past to a worldwide audience, she deleted her entire digital footprint from the internet.

Former Israeli intelligence operatives have also found their way into American newsrooms, shaping coverage of the Middle East. A recent MintPress investigation uncovered a network of former Unit 8200 operatives working in some of the most influential newsrooms in the United States.

Among them is Axios correspondent Barak Ravid, whose Middle Eastern coverage won him the prestigious White House Press Correspondents' Award. Until at least 2023, Ravid was a member of Unit 8200. CNN has also hired at least two former agents to produce their news coverage, one of whom, Tal Heinrich, now serves as the official spokesperson for Prime Minister Netanyahu.

Given this pattern, Silicon Valley's partiality towards Israel should not come as no surprise. From tech giants like Google and Amazon to social media powerhouses like TikTok and Facebook, the field is filled with former Israeli spies. Apple is no exception, having hired dozens, if not more, Unit 8200 operatives to run its platforms and shape the company.

This investigation does not claim that the Israeli state is deliberately infiltrating Silicon Valley. However, what it does unquestionably suggest is that the outlook and general biases of these entities are strongly pro-Israel. What does it say about Silicon Valley's culture that individuals with well-documented ties to a controversial foreign spy agency are considered ideal hires?

It is unthinkable that former intelligence agents of Hezbollah, Iran's Ministry of Intelligence, or Russia's FSB or GRU would be hired en masse, and trusted with our most sensitive data. Yet, when it comes to Israel (or U.S. surveillance agencies), the answer is different. Many of these employees are not even "former" agents, and are directly recruited from Unit 8200 while still in active service, despite Israeli law explicitly prohibiting the group's members from identifying themselves or divulging their alliances.

Thus, in this light, it appears that those like Apples4Ceasefire struggling to end the company's double standards are fighting an uphill battle.

Google Helped Israel Spread War Propaganda to 45 Million Europeans

Internal ad records show Israel spent millions on YouTube propaganda targeting Europe, ads that breach Google's own rules and frame the war on Gaza as a defense of Western civilization.

While it continues its conflict with its neighbors, Israel is fighting another war just as intensely, spending gigantic amounts of money bombarding Europe with

messaging justifying their actions, and scaremongering Europeans that Iranian nuclear missiles will soon be turning their cities into rubble.

A MintPress study has found that, since it struck Iran on June 13, the Israeli Government Advertising Agency has paid for tens of millions of advertisements on YouTube alone. In clear breach of Google's policies, these ads justify and lionize the attack as a necessary defense of Western civilization, and claim that Israel is carrying out "one of the largest humanitarian missions in the world" in Gaza.

The countries most targeted by this campaign include the United Kingdom, France, Italy, Germany, and Greece.

Information War

"A fanatical regime firing missiles at civilians, while racing towards nuclear weapons. While Iran deliberately targets cities, Israel acts with precision to dismantle this threat." Thus starts one Israeli government ad that hundreds of thousands of YouTube viewers in Europe have been compelled to watch.

"Terror architects behind the elimination of Israel plan: eliminated. Israel targets only military and terror sites, not civilians. But the threat remains," the voiceover continues, over ominous music and high-tech graphics. "We will finish the mission for our people, for humanity. Israel does what must be done," it concludes.

"Iran's ballistic missile program isn't just a threat to Israel, it is a threat to Europe and the Western world," another, seen by 1.5 million viewers in just three weeks, claims. "Iran is developing missiles with ranges of approximately 4000 km. That places Europe within the regime's striking distance," it adds, as graphics show virtually the entire continent turning blood red, signifying a nuclear attack. "This isn't tomorrow's threat. It is today's reality. The threat posed by the Iranian regime must be stopped. Israel does what must be done."

Ominous messages like these, translated into multiple languages, have reached tens of millions of people across Europe. Other Israeli government ads take a different tack, attempting to present Israel as a virtuous victim and an unwilling participant in war. As one commercial notes:

Imagine this: you are holding your newborn in a hospital room. Then the air raid sirens go off. Iran fires ballistic missiles at hospitals, at innocent Israelis. Patients, doctors, newborn babies: deliberately targeted. While Iran aims at families and children, Israel responds with precision, striking military sites. This is not a war of choice. Those who target civilians and hospitals become the target."

The claims made in such videos are often highly questionable. For example, around 935 Iranians were killed in Israeli strikes, compared to just 28 Israelis, suggesting Israel is far less careful to avoid civilian deaths than its opponent. Indeed, since October 2023, Israel has repeatedly and deliberately targeted

hospitals. The World Health Organization has documented at least 697 Israeli strikes on medical facilities.

Ninety-four percent of Gaza's hospitals have been destroyed or damaged, and more than 1,400 medical personnel have been killed. This includes Dr. Adnan al-Bursh, head of orthopedics at al-Shifa Hospital, who was reportedly raped to death by Israeli prison guards. According to UNICEF, Israel has killed or injured over 50,000 Palestinian children. An American nurse who worked in Gaza told MintPress News that IDF soldiers regularly shoot boys in the genitals to prevent them from reproducing.

Despite this, Israeli advertising presents the country as the savior of the Palestinian people. One Ministry of Foreign Affairs video, set to epic, inspiring music, describes Israel as undertaking "One of the largest humanitarian operations in the world right now." "This is what real aid looks like. Smiles don't lie. Hamas does," it concludes.

Francesca Albanese, the United Nations special rapporteur on the Occupied Palestinian Territories, called the commercial "scandalous" and directly challenged YouTube: "How can this be allowed?" The video has been translated into Italian, French, German, and Greek, and has been viewed by nearly seven million people on YouTube alone.

Transparently Inorganic

All referenced videos appear in the Google Ads Transparency Center as paid content from the Israeli Government Advertising Agency, and there is strong evidence that few, if any, of their millions of views are organic. The five versions of the "Gaza Humanitarian Aid" video, for example, collectively have only a few thousand "likes"—barely 1% of what would be generally expected of videos with this amount of views—and only two comments in total.

The difference between organic and paid content is clearer in videos that Israel has not promoted. Other videos on Israel's Ministry of Foreign Affairs YouTube channel receive only tens of views per day, not millions, which strongly suggests that close to 100% of their traffic is paid advertising.

The scale of this public relations operation is difficult to overstate. Even as the Israeli government hikes taxes and slashes domestic spending, its foreign PR budget has grown by more than 2,000%, the Foreign Ministry receiving $150 million more for public diplomacy.

Much of that money is evidently being spent on ads. In the past month, the Israeli Ministry of Foreign Affairs has uploaded videos that have topped 45 million views on YouTube alone. The countries most targeted include the United Kingdom, France, Italy, Germany, and Greece.

Greece is a particularly noteworthy case. Over the past 12 months, the Israeli government advertising agency has funded 65 separate YouTube ad campaigns targeting the country.

The Greek version of a recent ad—titled “An efficient system is in place, delivering aid where it’s needed”—presents Israel as a benevolent bringer of life to Gaza and has garnered over 1 million views in just four days, equivalent to nearly 10% of Greece’s entire population. The video currently has no comments and fewer than 3,000 likes.

The Israeli Ministry of Foreign Affairs uploads its videos in English, French, German, Italian, and Greek. Countries that do not speak these languages—such as Slovakia, Denmark, and the Netherlands—are still targeted, though users there generally receive the English version.

Israel has avoided targeting nations whose governments have formally condemned its actions, such as Ireland or Spain, spending nothing to reach those populations. The Netanyahu administration, evidently, has decided to attempt to shore up support in allied countries, even as their populations increasingly turn against Israel.

While many of these figures might shock readers, this investigation only examined the advertising campaign of a single organization, the Israeli Government Advertising Agency, and on a single platform, YouTube. It does not include other Israeli government and non-governmental groups, nor the myriad organizations collectively comprising the pro-Israel lobby in the West.

Israel has also attempted to influence the debate on other platforms, including Facebook, Instagram, TikTok, and Twitter. What is presented here is merely the thinnest slice of a much broader operation.

Israel and Silicon Valley

Some videos the Israeli government has released attempt to portray Israel in a positive light, but instead perpetuate racist stereotypes about Western civilization and its supposed superiority. In one ad, Benjamin Netanyahu states (emphasis added):

I want to assure the **civilized** world, we will not let the world’s most dangerous regime get the world’s most dangerous weapons. The increasing range of Iran’s ballistic missiles would bring that nuclear nightmare to **the cities of Europe and eventually to America**.”

Thus, the Israeli prime minister implies that Iran’s threat matters only if it endangers the so-called “civilized world,” that is, Europe and North America. “Never again is now. Today, Israel has shown that we have learned the lessons of history,” Netanyahu continues, directly comparing the 12-Day War (which Israel started) to the Holocaust. “When enemies vow to destroy you, believe them. When enemies build weapons of mass death, stop them. As the Bible teaches us, when someone comes to kill you, rise and act first.”

Google’s advertising rules explicitly prohibit commercials that “display shocking content or promote hatred, intolerance, discrimination, or violence.” Yet many of the ads described here explicitly justify Israeli aggression.

MintPress News contacted Google to ask how much the Israeli government's advertising agency spent on ads, how many impressions those ads generated, whether the company had a response to Albanese's comments, and whether the videos violated its policies.

Google did not answer the first three questions and reiterated that it has "strict ad policies that govern the types of ads we allow on our platform." "These policies are publicly available, and we enforce them consistently and without bias. If we find ads that violate those policies, we swiftly remove them," the company added, implying that it does not consider the ads a violation of its standards.

Few who have studied Google's connections to the Israeli government will be surprised that the Silicon Valley giant grants enormous leeway to the Netanyahu administration. Former CEO Eric Schmidt is known as one of Israel's most vocal supporters. Google has been financially invested in Israel since at least 2006, when it opened its first offices in Tel Aviv. In 2012, at a meeting with Netanyahu himself, Schmidt declared that "the decision to invest in Israel was one of the best that Google has ever made."

Company co-founder Sergey Brin has also come to the defense of Israel, denouncing the United Nations as "transparently anti-Semitic" and telling Google staff that using the word "genocide" to describe Israeli actions in Gaza is "deeply offensive to many Jewish people who have suffered actual genocides."

Earlier this year, with the Israeli economy in dire straits following its 18-month campaign against its neighbors, Schmidt's company came to the rescue, injecting billions into Israel in a record-setting acquisition. Google purchased local cybersecurity firm Wiz for $32 billion. The monumental sum paid—equivalent to 65 times Wiz's annual revenue and boosting the Israeli economy by 0.6%—left some analysts wondering if the deal had more to do with underwriting the Israeli economy than making a shrewd business investment.

It also raises questions about the safety of Google users' most sensitive personal data, given that Wiz was founded and continues to be staffed by former Israeli spies from the intelligence group, Unit 8200.

Google has a long history of working closely with Israeli intelligence. A 2022 MintPress News investigation identified at least 99 former Unit 8200 agents employed by Google.

Among them is Gavriel Goidel, head of strategy and operations for Google Research. Goidel joined Google in 2022 after a six-year career in military intelligence, during which he rose to become Head of Learning at Unit 8200. There, he led a large team of operatives who sifted through intelligence data to "understand patterns of hostile activists," according to his own account.

Google is far from the only tech giant recruiting Israeli spies to run their most politically sensitive departments. The same study found that hundreds of former Unit 8200 intelligence agents are employed at companies such as Meta

(formerly Facebook), Microsoft, and Amazon. And a significant amount of what America reads about the Middle East is also written by ex-Israeli spies.

A MintPress investigation from earlier this year uncovered a network of Unit 8200 alums working in top newsrooms across America.

Wikipedia is another key theater of war for the Israeli state. A project overseen by future Prime Minister Naftali Bennett deployed thousands of young Israelis to monitor and edit the online encyclopedia, removing troublesome facts and framing articles more favorably in Israel's favor. Those who made the most edits would receive rewards, including free hot air balloon rides.

The Ministry of Foreign Affairs has also launched a campaign to harass and intimidate American students, establishing a "task force" to carry out psychological operations aimed at, in its own words, "inflicting economic and employment consequences" against pro-Palestine protestors. While Foreign Minister Eli Cohen heads the task force, it stresses that its actions "should not have the signature of the State of Israel on it."

Amid mounting criticism, the Israeli government has sought to turn the tide by inviting influencers for direct talks with Netanyahu. In April, the Israeli prime minister met face-to-face with conservative internet personalities, including Tim Pool; Dave Rubin; Sean Spicer; Bethany Mandel; David Harris Jr.; Jessica Krause; Seth Mandel; and Mollie Hemingway, where they discussed how best to sell war with Iran to Western publics, and how to counter anti-Zionist sentiment online.

Other social media personalities report having been offered large sums of money in exchange for a few words of support for Israel.

In terms of turning the tide of European public opinion, Israel has its work cut out for it. A recent YouGov survey found the country was widely reviled across the continent. More than 20 times as many Italians, for instance, hold "very unfavorable" (43%) views of Israel than "very favorable" ones (2%).

Even in Germany, where popular support for Israel is highest, only 21% said they hold favorable opinions of the state (including only 4% highly favorable), with 65% displaying open opposition (including 32% who strongly dislike it).

A massive plurality of Britons, meanwhile, agreed with the statement: "Israel treats the Palestinians like the Nazis treated the Jews." Forty-eight percent answered in the affirmative, as opposed to just 13% who disagreed. This is despite European governments offering full-throated support to Israel, and even criminalizing pro-Palestine protests and persecuting journalists who oppose Western support for Tel Aviv.

The government of Israel is spending millions of dollars daily on gigantic advertising campaigns aimed at turning the tide of public opinion. To that end, it is developing a PR network as sophisticated as the advanced weapons systems it uses on its neighbors. On YouTube alone, its paid advertising, translated into

five languages, has reached at least 45 million people in the past month. Whether this strategy will ultimately prove effective remains unclear. After all, it is difficult to convince the public to support a genocide.

Alan MacLeod ***is Senior Staff Writer for MintPress News. After completing his PhD in 2017 he published two books: Bad News From Venezuela: Twenty Years of Fake News and Misreporting and Propaganda in the Information Age: Still Manufacturing Consent, as well as a number of academic articles. He has also contributed to FAIR.org, The Guardian, Salon, The Grayzone, Jacobin Magazine, and Common Dreams.***