MEDC
Middle East
Democracy Center

control+alt+delete

The Exploitation of Meta Platforms to Silence Dissent in the Middle East

Yousuf Abdelfatah • Sara Mohamed

EXECUTIVE SUMMARY

This report examines the methods employed by authoritarian regimes in the Middle East and North Africa (MENA) to exploit Meta platforms in an effort to silence dissent and suppress opposition. Based on a series of semi-structured interviews with regional activists, journalists, legal experts, and technology specialists complemented by open-source research, the study reveals a comprehensive pattern of digital repression tactics including pervasive surveillance, coordinated censorship, systematic harassment, and the exploitation of vague legal frameworks to target activists both domestically and abroad.

Our research uncovered widespread surveillance by regional governments, including pervasive monitoring of social media accounts and private communications. These surveillance tactics are coupled with seemingly coordinated censorship efforts, including mass reporting campaigns to remove activist content, unexplained account shutdowns, and government reprisals. Activists also faced targeted harassment campaigns, with governments deploying "online armies" using fake accounts and bots to target human rights defenders and their families.

The effectiveness of these digital repression tactics is amplified by the abuse of legal frameworks, including vague cybercrime and counterterrorism laws that criminalize "false news" and criticism of government officials. These laws are increasingly being applied extraterritorially, affecting activists even in exile.

Meta's platform policies and practices have often fallen short in addressing these challenges. Interviewees consistently reported inadequate responses to harassment reports and fake accounts, limited transparency regarding government data requests, and insufficient direct communication channels for at-risk users. The platform's content moderation practices show concerning inconsistencies across languages, while security vulnerabilities in platform updates create additional risks for vulnerable users. Additionally, of particular concern to many of the activists we talked to was the apparent bias in content moderation affecting Arabic-language posts and the shadow banning of political and human rights-related content.

To address these challenges, Meta must implement comprehensive reforms across several key areas including but not limited to the following:

Prioritizing User Privacy and Security

- Implement robust encryption across all services
- Switch to opt-in rather than opt-out security features
- Strengthen protection of user metadata

Investing in More Effective Moderation

- Develop more robust language-specific moderation tools
- Implement mechanisms to identify and disrupt coordinated harassment campaigns
- Address uneven moderation across languages

Increasing Transparency

- Provide regular detailed reporting on government data requests
- Ensure clear communication about content removal decisions
- Create transparent appeals processes

Improving Responsiveness and Support For Activists

- Enhance response times to reports of harassment
- Establish more direct communication channels with human rights defenders and human rights organizations
- Develop expedited processes for urgent requests
- Create clear emergency protocols

These findings highlight the urgent need for Meta to address these challenges and implement systematic changes to better protect vulnerable users in the MENA region. Current platform policies and practices often inadvertently enable state-sponsored digital repression, requiring immediate attention and comprehensive reform to better safeguard human rights defenders and activists.

METHODOLOGY

This report's findings are primarily based on a series of 15 semi-structured interviews conducted with activists and experts from across the region. The interviewees included human rights activists, journalists, legal experts, and technology specialists with firsthand experience and knowledge of digital repression tactics and their impact on civil society.

The semi-structured interview format allowed for a flexible approach, enabling us to explore specific areas of expertise while also allowing interviewees to elaborate on their own experiences and offer their personal and professional perspectives. Each interview covered topics such as personal experiences with digital repression, observations of government tactics, interactions with Meta platforms, and recommendations for improving online safety for activists.

To protect the identities of our interviewees, given the sensitive nature of the topic and the potential for reprisals, all participants have been anonymized in this report. Their insights have been aggregated and synthesized to present a comprehensive overview of the challenges faced by activists and dissidents in the region.

To supplement the primary data gathered through interviews, we conducted open-source research to follow up on issues mentioned by our interlocutors. This included reviewing academic literature, analyzing reports from human rights organizations and think tanks, and examining relevant legislation and policy documents from MENA countries.

The combination of in-depth interviews and open-source research allowed us to triangulate information, verify claims, and provide a nuanced understanding of the complex landscape of digital repression in the MENA region. While our findings provide valuable insights into the challenges faced by activists and Meta's response, it's important to note that the rapidly evolving nature of digital technologies and government tactics means that ongoing research and monitoring will be necessary to stay abreast of new developments in this field.

OVERVIEW OF AUTHORITARIAN TACTICS

Authoritarian regimes in the MENA region utilize Meta platforms to carry out domestic and transnational repression, targeting dissidents, activists, and human rights defenders living abroad.[1] These tactics include surveillance, censorship, harassment, and the weaponization of vague cybercrime and counterterrorism laws. Social media platforms, once seen as tools for free expression and organizing, have become double-edged swords—offering activists a broader audience while simultaneously exposing them to significant risks of monitoring and arrest.

SURVEILLANCE

Our interviewees noted that the surveillance of activists in the MENA region has become increasingly pervasive, with social media platforms emerging as key enablers of this surveillance. One interviewee starkly characterized Facebook as having become "a major tool for repression," while another described feeling that they were constantly being watched, stating that "everyone knows that their social media accounts, their phones, their texts, even things like Instagram, and WhatsApp, and Snapchat, all of these platforms are surveilled." Similarly, a Tunisian activist that we spoke to noted that "the regime follows our moves and our activism on these platforms." A Saudi activist told us that—based upon court documents they had seen—they believe that "what the Saudi government does is that it keeps track of everyone posting even from abroad and once they go back to Saudi they get arrested."

1. The Freedom Initiative, "In the Shadow of Authoritarianism: Egyptian and Saudi Transnational Repression in the U.S.," April 17, 2023, https://mideastdc.org/publication/in-the-shadows-of-authoritarianism/; Ahmed Shaheed and Benjamin Greenacre, "Binary Threat: How Governments' Cyber Laws and Practice Undermine Human Rights in the MENA Region," Project on Middle East Political Science, 2021, https://pomeps.org/binary-threat-how-governments-cyber-laws-and-practice-undermine-human-rights-in-the-mena-region; United Nations Human Rights – Office of the High Commissioner, "Online Protection and Digital Security of Syrian Women Human Rights Defenders," May 10, 2023, https://romena.ohchr.org/en/node/356; 1. Access Now, "How Journalists and Human Rights Defenders Are Targeted Online: A Detailed Report on the Middle East and North Africa," June 2019, https://www.accessnow.org/wp-content/uploads/2019/06/MENA-report.pdf; 1. Human Rights Watch, "'We Will Find You': A Global Look at How Governments Repress Nationals Abroad," February 22, 2024, https://www.hrw.org/report/2024/02/22/we-will-find-you/global-look-how-governments-repress-nationals-abroad

Some interviewees expressed concern even about ostensibly end-to-end encrypted platforms such as WhatsApp. One interviewee noted that Signal was banned in the United Arab Emirates (UAE), Oman, Qatar, and Egypt due to regimes having difficulty monitoring it, leading to some concerns regarding the safety of WhatsApp, especially in countries where calls are blocked but not messages.[2] The interviewee, an Emirati activist in exile, provided what they called "very clear examples" of private WhatsApp conversations being monitored in the UAE, citing the case of two Jordanian siblings who were detained for discussing the Yemen war in a private WhatsApp chat.[3] The interviewee believes this surveillance is widespread, stating, "we all expect that this is the same case with us."

In addition to the monitoring of accounts, our interviewees discussed several other sources of surveillance employed in the MENA region. These include spyware used to hack into activists' phones and track their communications;[4] network surveillance, where states with advanced technical capabilities like Israel can intercept data to deduce communication patterns on platforms like WhatsApp without accessing message content;[5] government requests for user data from social media platforms;[6] and device confiscation to extract data, even without the user's passcode. Notably, many of these tactics can and are used not just against activists in the country but also those outside.

An Egyptian activist described to us how the government uses IP tracking to identify and locate individuals who post critical content online. The same interviewee referenced a private case in which ostensibly private WhatsApp messages were used as evidence of support for an opposition political candidate and used to justify his arrest. Another interviewee noted that activists in their network expect that their phones are being monitored with spyware, highlighting the pervasive nature of this surveillance. Another, without making specific reference to spyware, seems certain that the messenger app was compromised, specifically stating, "They can easily access our account. They can easily see what we are writing on Messenger. So there is no security for activists."

> **Facebook Messenger was one of the most common vehicles by which to deliver spyware and other malicious content.**

Echoing this concern, a digital security expert told us that Facebook Messenger was one of the most common vehicles by which to deliver spyware and other malicious content. Similarly, an interview with a group of Tunisian activists working together in a Tunisian civil society organization revealed that they had similar concerns about whatsapp, stating, "We only communicate on Signal. . . . We don't have trust in [WhatsApp] since the conspiracy case . . . since it was revealed that the conversations between politicians were on the WhatsApp application."[7]

2. Maria Xynou and Arturo Filastò, "How Countries Attempt to Block Signal Private Messenger App Around the World," Open Observatory of Network Interference, October 21, 2021, https://ooni.org/post/2021-how-signal-private-messenger-blocked-around-the-world/

3. A profile of the brothers can be found here: MENA Rights Group, "Jordanian Brothers Tortured and Sentenced to Ten Years in Prison in UAE," January 20, 2023, https://menarights.org/en/caseprofile/jordanian-brothers-tortured-and-sentenced-ten-years-prison-uae

4. Frank Bajak, "Journalists, Lawyers and Activists Hacked with Pegasus Spyware in Jordan, Forensic Probe Finds," Associated Press, February 1, 2024, https://apnews.com/article/jordan-hacking-pegasus-spyware-nso-group-99b0b1e4ee256e0b4df055f926349a43

5. Tahrir Institute for Middle East Policy, "TIMEP Brief: Use of Surveillance Technology in MENA," October 23, 2019, https://timep.org/2019/10/23/timep-brief-use-of-surveillance-technology-in-mena/

6. Alina Bîzgă, "Meta Received Over 450,000 Government Requests for User Data in 2022," Bitdefender, June 30, 2023, https://www.bitdefender.com/en-us/blog/hotforsecurity/meta-received-over-450-000-government-requests-for-user-data-in-2022

7. Amnesty International, "Tunisia: Release and Drop Charges Against Opposition Activists Arbitrarily Detained for a Year," February 23, 2024, https://www.amnesty.org/en/latest/news/2024/02/tunisia-release-and-drop-charges-against-opposition-activists-arbitrarily-detained-for-a-year/

CENSORSHIP

Several of our interviewees expressed that they believed that Meta and/or regional governments are able to censor online content — restricting or removing content critical of the regime. A Tunisian activist interviewed stated that they have to constantly delete and block accounts because they are targeted by a barrage of negative comments from fake accounts. Their account is flooded with comments such as, "you're a traitor," "we don't want your democracy," and "we love [the president]." The activist stated that "95 percent of the time" these are fake accounts that were opened in the last couple of weeks, have no friends, and have posted nothing. Their comments overwhelm the post, drowning out his original message and weaponizing his own Facebook page against him.

> A Tunisian activist interviewed stated that they have to constantly delete and block accounts because they are targeted by a barrage of negative comments from fake accounts.

Another interview subject noted that many of his friends in Tunisia have had their accounts shut down "[without] any explanations." Indeed, in 2020, over 60 Tunisian Facebook profiles were shut down, including ones affiliated with high profile activists, with Facebook blaming a technical error.[8] The interviewee believes that this is due to Meta's cooperation with the Tunisian government. The interviewee states that "a lot of [our] friends, their accounts have been closed" because "if the ministry or the government flags some accounts to Meta, Meta will close them." Others suggested that they were subjected to mass reporting campaigns, likely directed by the government, that were used to take down posts. These same accounts would also then boost pro-government messaging.

Some activists also reported engaging in self-censorship out of fear of potential consequences for what they may post online. "We try to have the team avoid writing anything directly about the president or the authorities in general, whether it's a minister, mayor, or governor."

HARASSMENT AND INAUTHENTIC BEHAVIOR

Inauthentic behavior is used not just for censorship but also for harassment across the MENA region. These tactics include the use of fake accounts and bots to spread propaganda, harass activists, and report their accounts. One interviewee, who is based outside of Tunisia, described being targeted by "tens of thousands of fake accounts" based in Egypt and Saudi Arabia after the 2021 coup in Tunisia. They noted that in addition to overwhelming posts, these accounts spread pro-government messages and insult activists, creating a hostile online environment. Some interviewees noted that these accounts seem to be especially active around flashpoints such as elections.

> Tactics include the use of fake accounts and bots to spread propaganda, harass activists, and report their accounts.

Another interviewee stated that they encountered what they described as "online armies" of fake accounts that flood their posts with government narratives and attempt to discredit

8. Simon Cordall, "Facebook Deactivates Accounts of Tunisian Political Bloggers and Activists," *The Guardian*, June 4, 2020, https://www.theguardian.com/global-development/2020/jun/04/facebook-deactivates-accounts-of-tunisian-political-bloggers-and-activists

them.[9] The interviewee states that "they're kind of like online armies . . . like all of them would come at once and they'll start retweeting and liking each other. And like, even if you're ignoring them, you're not even engaging in their conversation. They're kind of responding to each other, just adding to each other until they stop." In some cases, the harassing accounts are not necessarily hostile but may be posing as friendly accounts trying to gain a user's trust. One of our interviewees described to us how her mother was targeted by accounts posing as people offering to help her father, who is detained by the UAE. The accounts contacted her mother through direct messages and tried to get information out of her, requesting her ID and status in the United States.

Some interview subjects expressed frustration with Meta's seeming inability or unwillingness to deal with inauthentic behavior. One Tunisian activist interviewed mentioned that it seemed "useless" to report fake accounts to Meta because "there's nobody to talk to at Facebook." They told us that "I reported them but then you never hear back anything." Another interviewee stated that they "don't understand" why Meta cannot identify bots if even they were able to tell that an account was fake. They believe that "Meta has the responsibility to put an end to these fake accounts and they're very easy to recognize." They argue that "if I can recognize them, I'm sure Meta can recognize them. It's not hard."

ABUSE OF LEGAL FRAMEWORKS

Authoritarian governments across the MENA region have implemented laws and regulations that restrict online freedoms and enable digital repression. This legislation often contains vaguely worded provisions that give authorities broad powers to censor online content, surveil individuals, and arbitrarily detain activists for their online activities. Regimes in the region are increasingly granting themselves broad authority to monitor online activities, often without judicial oversight or notification to the surveilled individuals. These sweeping powers enable authorities to collect vast amounts of data on citizens' digital lives, from social media posts to private communications. These laws are leveraged even against those not in the country. One activist, who is no longer based in Tunisia, shared with us the legal text of a case against him in Tunisian court which was brought against him after he had already left the country.

Regimes in the region are increasingly granting themselves broad authority to monitor online activities, often without judicial oversight or notification to the surveilled individuals.

Laws such as Tunisia's Decree Law No. 54, Egypt's cybercrime law, and Saudi Arabia's anti-cybercrime and counterterrorism laws criminalize the publication of "false news," insulting government officials, or posting anything that may be seen as harmful to the "national interests."[10] As such, in many cases, people have been jailed for their social media posts. One interviewee estimated that just in Tunisia "at least 100 to 200 people are in jail for, you know, insulting the president or something like that on their Facebook account."

9. Leena Khalil, "Inside the Middle East's Epic Online Propaganda War," Wired Middle East, September 29, 2024, https://wired.me/technology/privacy/inside-the-middle-easts-epic-online-propaganda-war/; Marina Ayeb and Tiziano Bonini, "'It Was Very Hard for Me to Keep Doing That Job': Understanding Troll Farm's Working in the Arab World," *Social Media + Society* 10, no. 1 (2024), https://doi.org/10.1177/20563051231224713; Katie Benner, Mark Mazzetti, Ben Hubbard, and Mike Isaac, "Saudis' Image Makers: A Troll Army and a Twitter Insider," *New York Times*, October 20, 2018, https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html

10. Human Rights Watch, "Tunisia: Cybercrime Decree Used Against Critics," Human Rights Watch, December 19, 2023, https://www.hrw.org/news/2023/12/19/tunisia-cybercrime-decree-used-against-critics; Wafa Ben-Hassine, "Egyptian Parliament Approves Cybercrime Law Legalizing Blocking of Websites and Full Surveillance of Egyptians," Access Now, January 13, 2023, https://www.accessnow.org/egyptian-parliament-approves-cybercrime-law-legalizing-blocking-of-websites-and-full-surveillance-of-egyptians/; Dina Sadek, Layla Mashkoor, Iain Robertson, and Andy Carvin, "Intentionally Vague: How Saudi Arabia and Egypt Abuse Legal Systems to Suppress Online Speech," Atlantic Council, June 12, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/intentionally-vague-how-saudi-arabia-and-egypt-abuse-legal-systems-to-suppress-online-speech/

One common thread across these laws is the use of vague language that gives authorities broad discretion to determine what constitutes a violation. Terms like "false information," "rumors," "insulting a government official," "national security," and "public order" are not clearly defined, leaving them open to abuse and subjective interpretation. This lack of clarity creates a chilling effect on freedom of expression, as individuals self-censor to avoid potential prosecution for online activities that could be deemed criminal. Additionally, laws may be purposefully overly broad, such as Egypt's media regulation law which defines media outlets broadly to include blogs and personal social media accounts with at least 5,000 followers, subjecting individuals to account removal, fines, and imprisonment.

Authoritarian governments exploit these vague and overly broad provisions to silence dissenting voices, target political opponents, and control the flow of information online. They often justify these restrictions under the guise of combating terrorism, protecting national security, or maintaining public order. However, in practice, these laws are frequently used to suppress legitimate criticism, peaceful dissent, and the free exchange of ideas.

Authoritarian governments exploit these vague and overly broad provisions to silence dissenting voices, target political opponents, and control the flow of information online.

The same legal frameworks that are used to target activists domestically can also be used to carry out transnational repression, targeting activists and dissidents living abroad. For instance, an interviewee mentioned receiving phone calls from the Emirati government threatening prosecution and imprisonment if they return to the country due to their online activism.

In addition to specific laws, authoritarian regimes in the MENA region utilize existing legal frameworks, such as defamation laws and anti-terrorism legislation, to criminalize online activities. They also employ a combination of legal and technological tactics to control the online sphere, using surveillance technologies, troll armies, and sophisticated spyware to monitor, harass, and silence critics.

META'S POLICIES AND RESPONSIVENESS

Compounding concerns regarding regimes' abuse of Meta platforms, activists and civil society organizations consistently report challenges related to Meta's responsiveness and communication channels for addressing digital repression and online harassment on the platform as well as concerns related to Meta's policies and procedures more broadly.

Uneven moderation is a recurring concern, with activists perceiving a bias against Arabic-language content and Palestinian voices, compared to content in Hebrew.[11] One interviewee suggested that Meta disproportionately removes Palestinian content due to what he described as "overcompliance" with Arabic-language moderation policies and a lower threshold of trust for Arabic, and specifically Palestinian, content. This is the result of not just algorithmic bias, but human decision-making. The interviewee explained that "platforms might want to address the issue for example of terrorist content . . . and they don't know how to approach this issue and the path they choose is that they would remove any content that is 20 or 25 percent according to the threshold" whereas normally the threshold would be much higher. This results in the frequent takedowns and restrictions of accounts belonging to individuals and news organizations, even when reporting news in a professional manner. The same interviewee told us that "in 50 percent of the cases that we follow up with companies the cases are overturned and

11. Marwa Fatafta, "It's Not A Glitch: How Meta Systematically Censors Palestinian Voices," Access Now, February 19, 2024, https://www.accessnow.org/publication/how-meta-censors-palestinian-voices/

restrictions are removed which obviously is more proof that there is a problem with the automated method that Meta implements." He noted that the same issue appears not to exist when it comes to Hebrew-language content on the same topics, providing more evidence that there is a bias against Arabic speakers.

Several interviewees also complained about the reach of political content or content deemed sensitive or graphic being limited without explicit notification or explanation, known as "shadow banning." One digital security expert suggested that Meta justifies this practice as a means of "keeping the community a safe space" by promoting content that generates high levels of engagement and demoting content that users tend to skip over. However, this practice raises concerns about the arbitrary suppression of content deemed critical of governments or related to human rights violations. This again seems to be especially prevalent with regards to content related to Palestine.[12]

Several interviewees also complained about the reach of political content or content deemed sensitive or graphic being limited without explicit notification or explanation, known as "shadow banning."

Limited reporting mechanisms and slow response times create a further trust gap between Meta and activists. Interviewees frequently highlighted the lack of readily accessible channels for individuals and organizations to report violations and receive timely support. One interviewee emphasized the difficulties associated with reporting fake accounts, noting that Meta's response often involves taking down individual accounts, while the perpetrators simply create new ones.

Additionally, individuals seeking to protect their accounts or those of their loved ones often have to rely on third-party organizations that advocate for digital rights like Access Now and SMEX due to the lack of direct reporting channels to Meta. This process can be time-consuming and requires individuals to have prior knowledge of and relationships with these organizations, potentially creating barriers for those who lack such connections. These groups often connect activists with vital services such as account shut downs but those who are not already in communication with the groups or have a large enough public profile to be easily vouched for are at a disadvantage.

One Egyptian activist and digital security researcher noted that there is fundamental tension at the heart of Meta's platform designs. As a for profit business, Meta "was not made for activists" and "security and privacy was never part of the design." As such, their incentives to cater to their main user base may inadvertently create security vulnerabilities for their more vulnerable users. This is particularly evident in how Meta handles platform updates, where new features that might create security vulnerabilities are often turned on by default rather than allowing users to opt-in, potentially exposing activists to new attack vectors before they can assess and mitigate the risks. He continued to note that compared to its peer tech companies, Meta consistently fails to invest in securing its platform, at least compared to its investments in other areas.

CONCERNS ABOUT DATA SHARING AND DATA PRIVACY

Activists also expressed concern regarding Meta's data sharing practices with governments, raising concerns about what they perceived to be a lack of transparency and the potential misuse of user information.

One interviewee questioned both whether and why Meta would provide user data to governments, especially when those governments have a history of targeting activists. Other activists

12. Human Rights Watch, "Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook," December 21, 2023, https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and

were already convinced that Meta cooperates directly with the state. One activist told us that he thinks that the only reason his account has not been closed down yet is because he is in the United States, and that if he was in Tunisia his account would have been shut down at the request of the Tunisian government. He told us that this had already happened to several of his colleagues and when this happens "they don't receive any explanation. Their account is just shut down." He continued to say, "I understand Facebook is a for profit company, but if they're going to align themselves with dictators, that's very bad for them and very bad for us. And very bad for humanity."

Another activist told us that he does not have any direct evidence that Meta shares information with the Egyptian government but that he "expects or believes that there is cooperation between the state, or the agencies associated with information technology or information technology crimes, and platforms such as Meta." He referenced the fact that there were activist-led Facebook pages that had secret administrators whose identities were leaked, putting them at serious risk.

One digital security expert told us that "the main thing is that Meta is not fully transparent about government requests for access for information. Usually they say that if government requests are done for a certain account they would inform the user, and that they have a transparent process that would clarify that they might be handing over a user's data. However, they have not been transparent about the number of such requests, how much they've said yes, how much they've said no."

Even end-to-end encryption is not a complete safeguard, as governments can exploit metadata from platforms like WhatsApp to identify and target activists, even if the content of their messages remains private.

Even end-to-end encryption is not a complete safeguard, as governments can exploit metadata from platforms like WhatsApp to identify and target activists, even if the content of their messages remains private. This information can be used to build what one activist referred to as "social graphs" that reveal an individual's connections and associations. The case of the Lavender AI system, which used WhatsApp metadata to target individuals in Gaza, illustrates the risks associated with the collection and potential misuse of this information.[13]

RECOMMENDATIONS

- *Improve Transparency and Accountability:* Meta should be more transparent about its moderation policies, data sharing practices, and responses to government requests. Regular transparency reports should be published, detailing the number of accounts restricted or removed, the reasons behind these actions, and the number of government requests for data received and fulfilled. Meta should also establish a clear and accessible mechanism for individuals and organizations to appeal content moderation decisions and report violations.

- *Invest in More Effective Moderation Tools:* Meta should invest in more sophisticated and nuanced moderation tools, particularly for languages and regions where activists face significant threats. This includes developing more accurate classifiers for hate speech and incitement to violence and addressing concerns about uneven moderation across different languages. Meta should also consider implementing mechanisms to proactively identify and disrupt coordinated harassment campaigns, such as those involving bot networks or fake accounts.

- *Prioritize User Privacy and Security:* Meta should prioritize user privacy and security by implementing robust encryption protocols across all of its platforms, including end-to-end encryption of both messages and

13. Yuval Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza," +972 Magazine, April 3, 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/

metadata. Meta should also clearly communicate its policies regarding data sharing with governments and provide users with greater control over their personal information. This could also include turning off new features that might create security vulnerabilities by default, or enabling users to choose whether these features are automatically turned on.

- *Improve Responsiveness and Support for Activists:* Meta should improve its responsiveness to reports of harassment and threats against activists and provide clear channels for individuals and organizations to seek support in emergency situations. This includes establishing direct communication channels with human rights organizations and developing expedited processes for handling urgent requests, such as requests to disable accounts after an arrest.

By implementing these recommendations, Meta can take concrete steps to mitigate the risks of transnational repression on its platforms and better protect the rights of activists and dissidents in the MENA region and beyond.

The Authors

YOUSUF ABDELFATAH is the Unjust Detention Hub casework officer at MEDC.

SARA MOHAMED is the Unjust Detention Hub manager at MEDC.

Acknowledgment

The authors wish to thank Meta for its support for the research of this publication. The findings and conclusions expressed are solely those of the authors and do not represent the views of Meta or its subsidiaries.