ARTICLE 19

Queer resistance to digital oppression

Queer communities in MENA fighting for better tech futures

July 2024

Executive summary

In collaboration with the DeCenter

In this three-part report series, ARTICLE 19, in collaboration with The De|Center and local experts, reveals how authorities in eight Middle East and North African (MENA) countries are weaponising technology against the LGBTQ community, and how tech companies can keep these – and other – marginalised communities safe from harm.

ARTICLE 19 has spearheaded work on this issue since 2016, in partnership with local, regional, and international experts. Our new research builds on our previous work in four key ways:

- **Over 5,000 individuals from 8 countries participated, making this the largest research project ever conducted with LGBTQ communities in MENA.** Between 2019 and January 2024, we conducted 15 focus groups, 93 in-depth interviews, and surveyed over 5,000 individuals in 8 MENA countries: Algeria, Egypt, Iran, Jordan, Lebanon, Morocco, Tunisia, and Sudan. In total, our research included 5,205 participants.

- **It investigates a broader scope of tech-enabled harms, from the perspective of LGBTQ people themselves.** Our previous work focused first on LGBTQ dating apps and next on how authorities collect digital evidence to prosecute LGBTQ people. But since we started this work, the toolbox of tech used against the community has expanded. Our new research therefore dives deeper and further into the harms facilitated by a broader scope of platforms, from chat-based messaging apps to social media, and centres the lived experience of the LGBTQ community themselves – including the changes they want tech companies to make.

- **It exposes the dangers faced by not only the LGBTQ community, but also the wider MENA population, at a time of significant regional turbulence.** The research period was marked by Covid-19, Tunisia's descent into autocracy, uprisings in Iran, and catastrophic wars in Sudan and on Gaza. Our research shows the added impacts and abuses faced by the community, particularly

the most marginalised (half of our survey respondents were highly marginalised[1]), in a period that has been one of the region's most painful.

> *'The Rapid Support Forces are prevalent on dating apps during this period, which wasn't the case before the war. This stopped [us] from using these platforms due to fear.'*
>
> – Research participant, Sudan

- **It reveals that, while the LGBTQ community faces particularly high risks from tech-facilitated state policing, these methods are also being used against other marginalised communities – as well as against the wider population.** The research also demonstrates that if we protect the most criminalised and marginalised communities, we will protect everyone. This is because we have seen methods initially deployed against the most marginalised are later used against other populations.

[1] 'Highly marginalised', in the context of the LGBTQ population in MENA, includes individuals who are Indigenous, disabled, refugees, migrants, sex workers, trans, and/or live in rural areas.

Key findings

1. **LGBTQ people in MENA, especially the most marginalised, are at significant risk of arrest and police violence.**

    - **25%** of survey respondents and **65%** of interviewees reported experiencing physical abuse and violent harassment at the hands of the police – including **7** cases of rape by state-affiliated persons.

    - **45%** of our survey respondents and interviewees had been arrested for their sexual orientation and/or gender identity – and over **1 in 5** had been arrested multiple times.

    - **13%** of our interviewees reported arrests linked to protests and 'morality' policing, showing that queer people are being criminalised and targeted for their identity during national uprisings, protests, and even war.

    - **100%** of sex worker, trans, and refugee participants reported police abuse. These groups also reported the highest arrest rates of all our respondents.

'I spent two days [in there] where I was tortured, and they hit me. They hit my family too. For a week they didn't let me sleep at all ... They even sexually harassed me and raped me using objects.'

– Research participant, Tunisia

---

2. **The police are using not only queer dating apps, but also social media and messaging apps, to entrap and arrest LGBTQ people – and they have started using the apps for sexual and financial extortion.**

    - **23%** of survey and interview respondents reported experiencing police entrapment[2] via apps. Survey respondents also reported this in Lebanon, where the phenomenon had not been documented before.

    - Respondents reported that the apps most commonly used for entrapment are the dating apps **Grindr, Hornet, Sugar, Tinder,** and **WhosHere,** as well as **WhatsApp**, **Facebook Messenger, Facebook,** and **Instagram.**

    - In a new and concerning trend (reported **53** times in our surveys and interviews), police used entrapment-style luring not to arrest people but to extort them out of money or sexual favours.

> *'A policeman trapped me through [Facebook] Messenger … I was arrested for 10 days, and I was humiliated. [They] broke my teeth also.'*
>
> – Research participant, Egypt

3. **Police are searching people's devices to 'verify' their queerness – and biometrics are increasing the risk of physical violence.**

    - **50%** of interviewees had experienced police searching their devices, including to 'verify' their queerness.

    - Of those who had interacted with the police, the police searched or attempted to forcibly access the devices of **nearly all** interviewees.

[2] Police officers using fake profiles and feigning romantic or sexual interest to elicit a sexually explicit or otherwise queer-leaning conversation, providing all the evidence needed for the charge. They then arrange to meet and arrest the unsuspecting individual.

- In a concerning new trend, our findings show that biometrics increased not only privacy risks but also the chances of experiencing physical violence at the hands of the police. Police had violently forced **8%** of our interviewees – that is, **every single one** who had been in custody and had biometrics enabled on their device – to open their device via biometrics through physical violence.

'At the precinct I was handcuffed, he kicked me to the floor and asked me to open it … he came close to me with the phone in his hand and forced me to place my fingerprint and open it. … They accessed Messenger and took it as an excuse to throw accusations at me.'

– Research participant, Lebanon

---

4. **Security features introduced in recent years as a result of our work are extremely popular – and are often the deciding factor when considering whether to use an app/platform.**

    - **59%** of survey respondents said the availability of harm-reduction features determine whether they use an app/platform.
    - **Nearly half** (**49%)** of our survey respondents said these are the safety features they use the most – and, for some, they were the difference between being imprisoned and being released.
    - **45%** of all participants had used app cloaking to hide an app, and **26%** had used timed messages.

'[When I was arrested] I used the feature to change the icons of the dating application and change its name, so they could not find it, and I claimed that I forgot the password for social networking applications.'

– Research participant, Egypt

Reports structure

Our research is split across three reports:

- **Part I sets out the regional context.** Laws that directly or indirectly criminalise queerness (many of them remnants of colonialism) have enabled the targeting of the LGBTQ community with practical impunity. With the rise of the internet in general and social media in particular, many queer people sought refuge online, yet state authorities were hot on their heels. Nevertheless, as we show, the LGBTQ community has used digital tools to resist oppression, create community, have sex, and fall in love.

- **Part II presents and analyses the findings from our focus groups, interviews, and surveys.** Our findings provide harrowing evidence of tech-enabled police and state violence against the LGBTQ community, reconfirm the findings of our previous reports at a larger scale and in more countries, and show an overwhelming overlap of issues faced.

- **Part III offers detailed recommendations to tech companies.** These recommendations are based on what our participants want and need to reduce the risks they face. We developed them in partnership with technical experts.

What should tech companies do?

Our research shows that LGBTQ people in MENA are taking high-risk measures to avoid giving the police and prosecutors access to their devices. These measures might seem drastic, but the individuals affected are only too aware of the alternative: risking further personal incrimination and exposing their friends, loved ones, and community to harm.

Yet the onus for protection against state violence and human rights abuses should not solely fall on the individual. Tech companies have human rights responsibilities to their users – and they urgently need to do more to meet them.

Report III sets out concrete and granular recommendations that apps and platforms must follow to protect their users in the MENA region.

With technical input from our experts,[3] we lay out precisely how tech companies can protect users' privacy and reduce their risk of harm – from code bases to user-experience design – including:

- **16** recommendations for privacy changes to existing infrastructure; and
- **15** recommendations for new features and changes to reduce harm in cases of arrests and device searches.

By implementing our recommendations, tech companies can make their LGBTQ users in MENA safer – and these changes, in turn, will keep *all* their users safer.

This is the Design From the Margins methodology on which our research is based. To make tech more equitable and safer, it must centre the needs of the most marginalised and criminalised users, from ideation to production. When they are designed for, we are *all* designed for.

[3] The main team has been The De|Center and Afsaneh Rigot (the principal researcher and author of the reports), the team of experts at the Guardian Project (which offers open-source software, as used by Grindr, to protect users from harm), and Norman Shamas (an expert in privacy and harm reduction).

Our method works

Our 2018 investigation into how authorities in Egypt, Iran, and Lebanon use dating apps to entrap and prosecute LGBTQ people led to **Grindr** rolling out new safety features worldwide, such as stealthy app cloaking, PINs, timed messages, and more. Other dating apps followed.

Our 2022 research, which revealed how law enforcement in Egypt, Lebanon, and Tunisia heavily relies on WhatsApp evidence to criminalise LGBTQ people, led to **WhatsApp** and **Signal** introducing similar safety features, such as updated timed messages and locked chats (WhatsApp) and app icon changes (Signal), for people in similar situations globally.

Our new research shows how the changes that some tech companies have made, based on our earlier work, have already helped to make LGBTQ people in MENA safer.

These changes have blocked the authorities from accessing incriminating data or apps, leading to individuals being released on lower or no charges.

Our method works.

Now is the time to extend the safety net.

> *'This [research] made me feel really good that someone cares enough about making these apps, which are providing services in the third world, more secure. I hope that we will see some changes soon and we will not be disappointed.'*
>
> – Research participant, Iran