LGBTQ ONLINE

Summary Report

ARTICLE 19

Apps, arrests and abuse in Egypt, Lebanon and Iran

February 2018

Apps, arrests and abuse in Egypt, Lebanon and Iran

An investigation into use of social and dating apps by the LGBTQ community in Egypt, Lebanon, and Iran. This study focuses on security, risk-management, and user perceptions of how the structure and features of apps and social media platforms interact with their own risk-levels.

TABLE OF CONTENTS

INTRODUCTION: APPS, ARREST AND ABUSE IN EGYPT, LEBANON AND IRAN

For more information on our methodology please contact **Afsaneh Rigot** at: **afsaneh@article19.org**. We have not made this public due to the potential risks involved to participants.

There has been widespread repression and marginalisation of Lesbian, Gay, Bisexual and Queer (LGBTQ) groups and individuals globally, limiting safe opportunities for connecting, socialising, organising, and meeting in public spaces. The targeting of LGBTQ groups in the Middle East and North Africa (MENA) region reached a climax in September 2017 when more than 70 people were arrested due to perceptions of their gender and sexual identities in Egypt after the rainbow flag was flown during a concert. At least 16 were convicted with sentences ranging from 6 months to 6 years in prison. Many of these arrests happened via entrapment through LGBTQ dating apps.

Fear and real risk forces the LGBTQ communities to communicate online, where they have created vibrant and resilient hubs of connection, but the apps and platforms being used can also put users at risk.

In 2014, stories surfaced about apps being used entrap gay and transgender users in Egypt through the apps' geolocation features. Yet, limited investigation was done into the full methods used and the extent LGBTQ groups were targeted.

It has since emerged that these apps are routinely used both by authorities and non-state actors to target members of the LGBTQ community.

> "WE ARE A LOT **MORE CAUTIOUS** TO THE HUGE RESTRICTIONS IN THE LAW. BUT IN GENERAL **IT DOESN'T STOP ME**, I CONTINUE TO MEET QUEER PEOPLE ON THESE ONLINE NETWORKS."
>
> *Anonymous app user*

But what exactly is happening? Who has been targeted and how? What are the consequences for those targeted? Has enough been done to secure the safety of apps users in the region since?

This summary report looks to answer these questions. The full report from July 2017 has not been made public to date for the safety and security of those involved.

Our research

ARTICLE 19 has been working on the digital safety and security of online LGBTQ communities in Egypt, Lebanon, and Iran, using a multi-stakeholder approach.

This short summary report presents data gathered about users in Egypt, Lebanon and Iran. These are three very different Middle Eastern contexts where the LGBTQ community are heavily reliant on technologies such as dating apps to communicate, assemble, date, “hook up”, and fall in love.

These are also countries in which communication and dating tools have been used by state authorities and homophobic non-state actors to target members of the LGBTQ community.

KEY FINDINGS

> "LGBTQ users will continue to use apps even where their safety is at risk."

Apps and platforms are used despite risks

The testimonies of users and the results of our research make it clear that these LGBTQ-focused dating apps have become important tools to connect individuals and communities that are frequently targeted for their identities. Despite this real and present danger, users see benefits that outweigh the risks. The drive for sex, love, intimacy, and association is stronger than the fear of the risks.

Risks are significant, complex, and little-understood

A combination of factors can increase risk, ranging from identity and location, to online behaviour. Despite previous assumptions, geolocation or the lack of encryption are not the dominate risk to users (although they do play an important role for users and their sense of security). In addition, the interaction between dating apps and social media further complicates risk and its mitigation.

Apps and tech companies have a responsibility towards their users

LGBTQ-focused apps, such as Grindr, Hornet, PlanetRomeo, Growlr, and Her, as well as group chat functions[1] in messenger apps, are important tools to connect individuals and communities that are otherwise frequently targeted for their identities. Due to these platforms' unique ability to connect, empower, and provide an avenue for expression, as well as to build personal relationships, our research has shown that LGBTQ users will continue to use them even where where it directly risks their safety or privacy. Crucially, the responsibility then falls on service providers to protect the users of their products by implementing prevention and mitigation strategies when desiging their products and practicing due diligence as set out in international standards, such as the UN Guiding Principles on Business and Human Rights (UNGPs), as well as making proactive efforts to support users in staying safe. This should be done through the application of human rights and security principles to their operations. This is especially the case when these apps are functioning in countries with higher risks to LGBTQ users. It is essential that apps acknowledge and assess the risks faced by their users and

[1] This would mean group chats as seen in WhatsApp and Telegram, with group admins, where information on events/meetings is often shared.

commit to work with the relevant stakeholders to mitigate those risks. This project also evidenced the necessity for companies and developers to consider human rights implications in the design and operation of their products. This can be seen from the requests from users, following the range of threats faced when these considerations are not taken into account.

> "Companies and developers must consider human rights implications in the design and operation of their products."

Findings indicate that market forces favour the most popular apps over the safest ones. However, we found this "network effect" in the three countries to be be affected by the perceived safety and/or risks of using an app. If a popular app is targeted, no longer seen as secure, research shows that users generally default to another popular app.

Customised measures need to protect against threats

Some respondents indicated that they take creative measures to protect themselves from both perceived and real risks. These measures can be very successful and could be drawn on by apps and technologies for their relevant country. These kinds of practical steps can support users to remain safe. However due to a lack of available information, some other measures taken by respondents have not reduced risk but been dangerous and left many with no security precautions. For example, some users mentioned using Virtual Private Networks (VPNs) to obscure their location, but were unaware of the risks insecure VPNs could cause. Others mentioned their method of only sharing pictures of either their body or face to protect themselves, both of which can be used by authorities in cases against them. Sharing these experiences with apps and tool providers is imperative in supporting communities.

> "LGBTQ users want more information from the apps they use, particularly legal advice."

Information and support from apps is welcome

Respondents felt that security advice received from apps themselves so far had been good advice. Many wanted more, particularly legal information and advice. While largely a positive move, it is not sufficient to address all the risks and threats. The security protocols of these platforms should be reviewed by trusted security experts and local groups. They must be updated regularly. Further measures must also be taken in light of idiosyncratic risks faced by users. Apps should not feel that solely sending security messages in countries seen as dangerous to LGBTQ users is sufficient due diligence on their behalf. This isn't enough to protect their users – more proactive measures are necessary.

A large proportion of security information circulated to date has been aimed at male gay and bisexual app users. There is still great demand for information relevant to other sectors of the LGBTQ community.

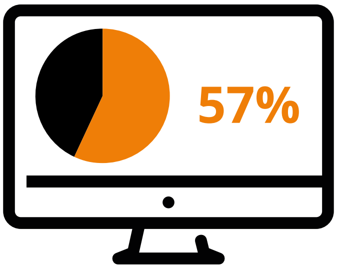
THE CONTEXT

Egypt

Egypt does not have clear laws in its penal code on the term “sodomy” or “homosexuality”. However, Egypt’s legal provisions, particularly Article 9(c) of the “anti-debauchery law”, Article 178 of the Penal Code, and Articles 98(f) and 256 of Law 58/1937 enable discrimination against LGBTQ individuals and groups, punishing “debauchery” in various forms as well as the publication of materials and information relating to non-heterosexual relations. The Egyptian Penal Code criminalises homosexuality under the vague and broad term “habitual debauchery” in Article 9(c) of Law 10/1961 for combating adultery and debauchery. The status of same-sex relations between women is legally unclear.

Despite the Egyptian Constitution containing safeguards against discrimination, state and court backed harassment in Egypt continues at concerning levels, including “morality-policing”, heavy monitoring by Egyptian police, and waves of arrests, often based on online behaviour. In 2014 there were reports of arrests being made using the geolocation feature of Grindr and other apps.

Since 2015, observers have recorded an increase in authorities’ monitoring of LGBTQ apps and community websites. According to project partners in the Egyptian Initiative for Personal Rights (EIPR), these efforts are now being more openly discussed and published in police reports. Most notorious was the arrest of 11 individuals in September 2015 in Giza’s Agouza neighbourhood for “practicing, inciting and publicising immoral practices”. The individuals were sentenced to between three and 12 years’ imprisonment.



According to Solidarity with Egypt LGBTQ, 57% of charges against LGBTQ individuals featured the use of websites and social media to entrap or incriminate them.

According to the EIPR, one of the accused was initially targeted via a dating app (Grindr). Authorities reportedly entrapped this individual using a fake profile on social media and/or a dating app, posing as a user interested in a relationship. Via the private messaging feature, they gained the address of this individual and were granted permission by the public prosecutor to raid the apartment. This led to his arrest, along with eight individuals relating to the case, before a raid took place on a second address.

“THE [POLICE] ARE NOW MORE **TECHNOLOGICALLY ADVANCED**.”

Dalia Abdel Hameed,
Head of the Gender Programme at
Egyptian Initiative for Personal Rights (EIPR)

In September 2017, this intensified after one of the worst crackdowns on LGBTQ people in the region. After a concert in Cairo where the rainbow flag was waved, more than 70 people were arrested based on their perceived sexual orientation, many of who were targeted and arrested through dating apps.

A detailed report of the police actions and work on these apps has been published by EIPR. In their press release about the report, EIPR noted:

> *The cases analysed by the report demonstrate that the Interior Ministry’s General Directorate for the Protection of Morals employs primarily three worrying strategies or practices. The first and most prevalent is entrapping individuals using fake accounts on dating sites and apps for gay or transgender people, especially transwomen. Second, the Interior Ministry deporting of foreign gay nationals, or foreigners thought to be gay, even when charges of habitual practice of debauchery are not upheld against them. Third, the creation of major sex scandals that receive exceptional media coverage.*

The report also notes that the average number of those arrested and referred to trial in these cases has increased five-fold since the last quarter of 2013, in comparison with previous years. In the three and a half year period ending in March 2017, a total of 232 people had been arrested, or about 66 each year, compared to an average of 14 people a year in the period from 2000 to 2013.

Iran

Iran is the only country of the three that directly criminalises same-sex relations according to its Islamic jurisprudence, and its newly-revised Penal Code, including Articles 233 and 234. Authorities have gone as far as to deny the existence of homosexuality in the country, with transgender individuals acknowledged only as having "Gender Identity Disorder (GID)" requiring medical and psychiatric treatment (which can be facilitated by the state). The medicalisation of non-normative sexual and gender identities is an official stance of the Iranian government.

> "Authorities in Iran have gone as far as to deny the existence of homosexuality."

The punishments for same-sex relations are harsh. Lustful touching or passionate kissing is described by the Islamic Penal Code as same-sex sexual behaviour and is punishable by 31 to 74 lashes (Article 237 of the Penal Code), including the death penalty for some convictions of "sodomy"; trans individuals can even be subjected to forced medical treatments for transition. LGBTQ individuals are harassed, threatened, and arrested in Iran on a daily basis, often after being surveilled on the apps and social platforms hey use.

Research findings and local experts' testimonials indicate that there are unofficial and random monitoring of apps used by LGBTQ persons. The use of the data gathered has ranged from threats of arrest to use of the information incriminating them under Iran's anti-LGBTQ laws when interrogating users for political or other activities seen as punishable by the state. Chat groups on Telegram have also been monitored with LGBTQ groups having their admins arrested.

Lebanon

Lebanon's laws do not outlaw homosexuality per se and there have been a number of positive rulings by select judges. However provisions including Articles 209, 533, and 534 of the Lebanese Penal Code have been interpreted by authorities in a way that has allowed the authorities to police sexuality. The main article used, Article 534, prohibits "acts against nature". The vague nature of these laws have allowed for raids and repeated reports of cases where the police randomly stop and check people on the streets based on their perceived sexuality. Testimonials of local groups indicate that at army checkpoints national security is used as an excuse to search individuals' and mobile devices. This has meant the discovery of LGBTQ apps on mobiles which have led to arrests and intimidation. This practice is unduly exercised on LGBTQ Syrian refugees.

> “THE INCIDENTS OFTEN OCCUR IN PARKS AND CAFES, BUT THERE ARE ALSO INCREASING CASES IN WHICH **SECURITY FORCES RAIDED HOMES AND MONITORED INTERNET SITES** FOR THE PURPOSE OF DETAINING PEOPLE THEY SUSPECTED OF ENGAGING IN NON-CONFORMING SEXUAL CONDUCT OR GENDER EXPRESSION.”
>
> *Human Rights Watch, 2010*

Police and the army in Lebanon selectively raid both public and private spaces known to be frequented or occupied by people of diverse sexual orientation or gender expression. The arrest of 45 people during the raid of Turkish hammams in 2014, in the Hamra-Concord section of Beirut, was the most notorious. Although raids of this kind are not as common, searches at check-points based on perceived sexual orientation and gender identity are becoming more frequent.

As well as the targeting, searching, and humiliation of LGBTQ individuals at police and army checkpoints, anal “examinations” (deemed to “confirm” the homosexuality of detained individuals) are also routinely carried out, especially by the military or police, to gather evidence of “homosexual acts”.

HUMAN RIGHTS AND TECH

Under the UN Guiding Principles on Business and Human Rights (UNGPs), a framework for understanding and respecting human rights is established: businesses have a responsibility to conduct due process and impact assessments, as well as incorporate transparency and safeguards into their design. The guidelines also set out responsibilities to track performance relating to human rights, and make remedies available when human rights are violated or negatively impacted.

> "
> **App providers have a responsibility to protect the users by implementing prevention and mitigation strategies, and support users in staying safe.**
> "

> ""IT'S THEIR BUSINESS, **WHY SHOULD THEY CARE ABOUT US?"**
>
> *Anonymous app user*

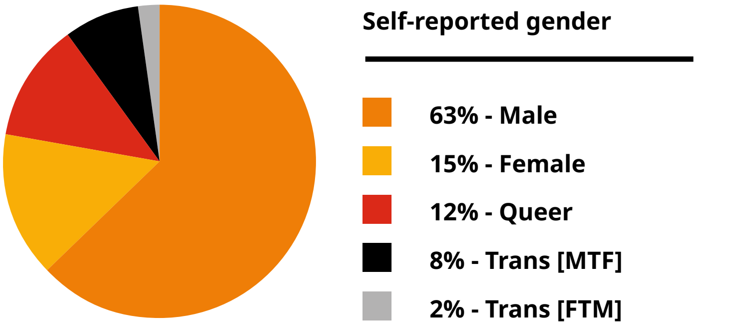
Dating apps and online social platforms have a unique ability to connect, empower, and provide an avenue for expression and personal relationships. It is the responsibility of providers to protect the users of their products by implementing prevention and mitigation strategies, as well as making proactive efforts to support users in staying safe.

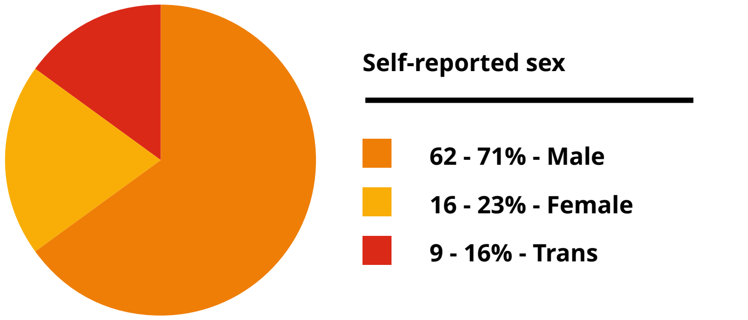
Human rights and security principles must be applied to design and operations. This is especially the case when apps are functioning in countries iith higher risks for LGBTQ users.

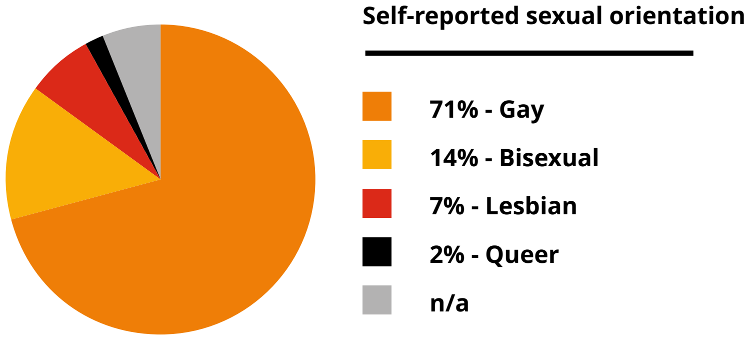
WHO WE SPOKE TO

With 429 usable responses, our demographics were varied. In all three countries over 30% of the respondents were aged 25-34. 63% identified their gender as male, whilst only 15% as female, 12% as queer, 8% as trans [MTF] and 2% as trans [FTM]. Sex followed a similar pattern in each country where between 62-71% identified as male, 16-23% as female and 9-16% as trans.

Sexual orientation followed this pattern too, with the top three sexual identities being 71% gay, 14% bisexual, 7% lesbian and 2% as queer.


Self-reported gender


Self-reported sex


Self-reported sexual orientation

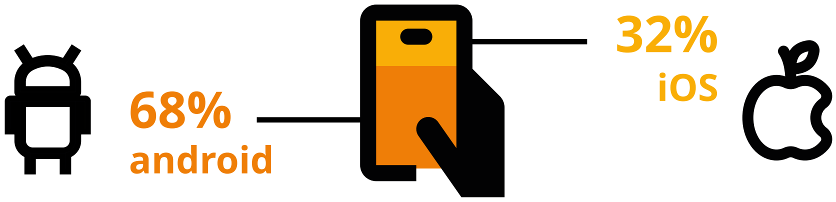
We saw a clear disproportionality in the demographic of respondents regarding sex and sexual orientations, with more than 60% in each country identifying as male and 73% as gay.

The large majority (60%) of respondents were professionals, with 22% students or unemployed, 16% business owners, and 2% identifying themselves as sex workers.

With regards to type of devices used, 68% of respondents use Android; 32% use iOS.

We also collaborated with local partners to gain context-specific insight to the above and help develop the multi-stakeholder approach.

Devices used



Refugees are particularly at risk

The migrant and refugee respondents have been in their resident country for less than 11 years. The counties of origin mentioned predominately included: Syria, Palestine/Occupied Territories, Jordan, Sudan, Saudi Arabia, and Iraq.

Local partners confirmed that these individuals have particularly low levels of access to legal help and information about their rights, as well as a higher rate of arrest and intimidation. This is particularly the case for Syrian individuals.

An overwhelming number of LGBTQ refugees and migrants live below the poverty line, and many resort to transactional same-sex sexual activity, for which dating apps are a major tool. This may go some way to explaining the proportionally high number of migrant and refugee responses.

WHICH APPS AND SOCIAL PLATFORMS ARE USED?

The variety of apps used by the respondents is large. There are however more popular apps, namely Grindr, Hornet, PlanetRomeo, and Growlr, which are also the apps most used to observe and entrap users.

Most respondents are using dating apps to seek sex, romance, and love, but there are a minority who have the aim of community-building and advocacy through the networks.

> "I PERFORM **HIV AWARENESS** ON DATING APPS AND ALSO CAN SPREAD INFO AND ORGANISE COMMUNITY EVENTS"
>
> *Anonymous app user*

Some simply see the apps as a place to express themselves.

> "I TRY TO KEEP IT LOW-PROFILE AND **I RARELY MEET**. I MORE USE THE APPS AS EXPRESSION PLATFORMS."
>
> *Anonymous app user*

Dating apps

Iranian respondents were typically less reliant on LGBTQ tailored apps than those from Egypt and Lebanon. This is potentially because the communication environment in Iran is simply more restrictive, with more blocking of certain apps and higher levels of fear and intimidation. Other factors may include the popularity of the messaging app Telegram which maintains around 40 million monthly users, despite the high levels of attention authorities place on monitoring them[2].

The "network effect" is a huge factor in determining respondents' choice of app – the biggest motivation for use was the fact that all their contacts were already using the app. This is especially problematic given that the better-known and more-used an app is, the more attention it is likely to attract from authorities and individuals looking to threaten, harass, and target LGBTQ users.

> "SOME APPS ARE MORE POPULAR AND WE USE THEM MORE BUT YOU SHOULD KNOW THAT **THEY ARE THE RISKIEST APPS** AND ENTRAPMENTS HAPPEN MAINLY THROUGH IT"
>
> *Anonymous app user*

However, responses from users show that this is influenced by the perceived safety and/or risks of using an app in the three countries. If a popular app is targeted, not seen as secure, and more users are put at risk, many users will default to another "popular" app. So although popularity is the defining factor in app usage, risk will affect the use of popular apps. This is an important observation to be noted by tech companies and developers.

Social platforms

Respondents favour WhatsApp, Facebook, Instagram, Snapchat, and Telegram. Though the motivations for these choices remains unclear, security is not a priority for most, cited by only 15%.

Respondents regard social media as easier, as well as safer, to use, and local partners reported that lesbians and bisexual women feel more comfortable using apps which are not dating-specific, but generally connective.

[2] See ARTICLE 19's December ***Tightening the Net*** briefing on the recent persecutions of Telegram channel administrators.

Combined usage and cross-referencing

As well as apps often functioning through connection to a Facebook account, the actual use of dating apps and social platforms is connected, with contact occurring initially through the dating app, and then moving to a messaging platform like Facebook or WhatsApp.

This can mean a transfer or even a doubling of risk. A number of respondents said that authorities had combined their use of apps with their use of a Facebook account in order to target them, and that the evidence from the two sources was cross-referenced in both arrest and blackmail situations.

As well as being tools for LGBTQ individuals, social platforms are also routinely used to “out” people, share information, or humiliate those who have been discovered by infiltrators of groups and applications.

When asked if users will continue to use apps despite the risks, 60% of users responded that they will/do continue to do so.

> “The drive for sex, love, intimacy, and association is stronger than the fear or risk.”

60%
of users will continue to use apps despite the risks

Regardless of the apps, platforms, and security measures chosen, respondents spoke of the isolation from the community which would come with disconnection or stopping use altogether. The risks of online communication are still lower than meeting people in public, allowing many people to be connected in digital spaces.

Those who choose not to continue using apps tend to do so due to fears for their **physical safety (53%), digital safety (20%), or privacy (24%)**.

For men, the fear of physical harm included harassment and arrest by the police, whereas for women it included threats from men using fake accounts to pose as women, arrest and blackmail.

We believe that this is an important and unsurprising finding. This is an essential service that is – and will continue to be – used by a community faces higher levels of risk to their physical safety. It shows the responsibility of the service providers to protect users and take positive steps to mitigate the security risks that they face. By providing an essential service that is used by marginalised groups, despite risks, a business has accepted a responsibility for the safety of their users.

HOW ARE USERS PROTECTING THEMSELVES?

Though some precautions are taken, only 15% said that they choose an app on the basis of finding it safe and secure, and there is a high level of misunderstanding of digital security principles among respondents. This summary report does not reveal all the methods the respondents mentioned they are using to protect themselves online.

> "only 15% of respondents choose an app on the basis of finding it safe and secure."

Security knowledge

The level of security information varies enormously from country to country, with 74% of respondents from Egypt and 84% from Lebanon having had access to security training or information in some form, but only 22% of respondents from Iran.

Generally, knowledge and information was weak among respondents in all countries, both in terms of security and their situation as LGBTQ individuals in their countries more widely.

It is however a positive note that 97% of respondents said they updated their mobile systems regularly, 52% of these say their phone automatically updates its software.

Stopping usage

Despite a majority continuing to use online platforms, some respondents had stopped their use of some apps, the main five of which were Badoo, Tinder, Manjam, Scruff, and GayRomeo. However, this stop in usage can in some cases be explained by government filtering.

Despite controversy, there has not been a reduction in the large numbers of users of Telegram in Iran, though partners have suggested this is due to a lack of information and news circulation regarding security issues.[3]

[3] ARTICLE 19's observations about Telegram security protocols can be seen in September ***TTN*** report, p.12. Also see ARTICLE 19's December ***Tightening the Net*** briefings on the recent persecutions of Telegram channel administrators, including arrests of administrators for sharing "immoral homosexual content".

INFILTRATION, SURVEILLANCE AND DETENTION

Fake accounts and infiltration

Fake accounts are being used by state and non-state actors to lure individuals into face-to-face meetings, entrap them, and subject them to arrest or cruel and degrading treatment, or blackmail them for money or sexual services.

Many respondents reported this happening to themselves or to friends or family, especially in Egypt. Few outlined the sentences they received and the cruel and degrading treatment they were subjected too. They also mentioned the content of their chats on apps being used as evidence on each occasion. This is a well-documented operation by Egyptian police that the users are recounting. But, this is also a tactic that is sporadically used in Iran and Lebanon, yet gets little mention.

In other reports of fake accounts with non-state actors, cruel and degrading treatment or blackmail for money or sexual services was reported. This was especially the case for women and trans individuals.

> “I WAS **RAPED** TWO TIMES ON FAKE DATES.”
>
> *Anonymous app user*

Blackmail seems more prevalent through dating-specific apps in Egypt and Lebanon, while in Iran these cases occur via messaging apps such as Telegram (although there were a few reports of these occurrences on the Hornet app and the Manjam dating website).

The infiltration of group chats on mainstream social platforms and messaging apps endanger the entire chat group, and can allow access to extensive lists of contacts. This increases risk within the community, and creates risk of contact with both partners and family members.

Apps as evidence

Accounts of cases describe the presence of the app itself as a danger for users – i.e. the recognisable logo of the app followed by the contents of the app. The existence of an app logo itself on their mobiles has been held as sufficient grounds for arrest or prosecution after users have been stopped and searched, or their houses raided.

> “THE SOLE ISSUE OF HAVING THE APP PUTS YOU IN A **VULNERABLE** SITUATION.”
>
> *Anonymous app user*

> **“Possession of photos, videos or other media in phone galleries which are deemed to be pornographic has lead to arrests in Iran, Egypt and Lebanon.”**

The presence of the app logo on their picture has also led to users being targeted, arrested, harassed, and blackmailed, providing grounds for prosecution on basis of their activities on the app. This issue has been mentioned predominately by users whose picture with the app logo was screenshotted without their knowledge, and used against them for harassment and/or blackmail especially when stopped at army check-points in Lebanon.

One case describes a situation of exploitation and blackmail that lasted over five years, through initially being identified on Facebook, Grindr and Hornet.

The checking of phones for LGBTQ-focused dating apps at certain police and military checkpoints in Lebanon has been prevalent, with local NGOs like Helem documenting cases and hoping to support LGBTQ persons from their community protect themselves from the problem.

In addition to being discovered with certain apps, possession of photos, videos or other media in phone galleries deemed to be pornographic has lead to arrests in Iran, Egypt and Lebanon.

Two respondents mentioned being arrested and detained in Egypt for a number of months for possessing such content, without having engaged in any physical sexual activity. In another case, the respondent was arrested not due to material on his phone, but due to pictures of him at a “gay party” saved and shared in groups – after which he fled the country.

> "I HAVE HEARD OF MANY CASES WHERE SOMEONE WOULD GET CRIMINALISED WITH THE [LEBANESE] PENAL CODE 534 **JUST FOR THE PRESENCE OF MOBILE DATING APPS OR PICTURES OR MOVIES** DOWNLOADED FROM MOBILE DATING APPS ON THEIR MOBILE PHONES."
>
> *Anonymous app user, Lebanon*

"Great risks are run through the use of apps – risks which users acknowledge.

Respondents do, however, have a strong sense of what should be done to make their interactions online within their community safer."

Taking a screenshot of the profiles of users is also widespread. These screenshots are used for blackmail, or as a basis for violence, coercion, or arrest.

Location services

Two cases mention the targeting and harassment without users knowing how they were located – leading them to guess that it was due to geolocation features of the app. However, statements suggest there is only circumstantial evidence for this, with no exact cases provided.

WHAT USERS WANT

Authenticated anonymity?

Respondents were keen to maintain their own anonymity, while desiring that other users are verified and authenticated, to avoid the risk of speaking with fake profiles or infiltrators.

This forms a paradox at the centre of the research: the nexus between authentication systems, and desirable anonymity.

Secure sign-up

84% of respondents feel unsafe with an app which links other social media apps

86% feel anxiety about sharing their real name

74% feel unsafe sharing their phone number

72% feel unsafe sharing their geolocation

> “SOCIAL MEDIA **SHOULD BE SEPARATE FROM DATING AND DATING APPS**! THEY ARE TWO DIFFERENT THINGS. WHY SHOULD WE CONNECT EVERYTHING TO EVERYTHING?!.”
>
> *Anonymous app user*

The anxiety around sharing personal details and connection to other forms of communication demonstrates a lack of trust in the apps and social platforms.

Geolocation removal

There is a great deal of anxiety around location services relating to dating apps, and whether they can be or even are already used to entrap individuals from the LGBTQ communities of these countries. Information on this issue is, however, limited.

> "What respondents expressed, perhaps most of all, was a desire for information.
>
> They want to be empowered in their decisions, particularly when they are engaging in risky behaviour, to allow them to take measures and calculate their own risks using up to date, reliable information."

Though some felt that the location services provided useful information on the individual they were chatting to, they expressed interest only in knowing approximate location, with 89% saying they only needed to see a neighbourhood or city.

Emergency reporting systems

Users would like to have options for communication with companies for more than just technical issues, i.e. a way to contact the app in case of security and safety issues, or emergencies relating to the app.

> "THE HELP OPTIONS ARE ONLY FOR TECHNICAL PROBLEMS, NOT **HUMAN PROBLEMS**."
>
> *Anonymous app user*

The help options on most apps currently only offer solutions or contacts relating to technical difficulties. The lack of information regarding safety, security, and emergencies is seen to exacerbate the risks faced.

WHAT THEY WANT TO KNOW

"The respondents are keen to have advice about what laws apply to them and how it can be used against them."

Legal advice

The respondents are keen to have advice about what laws apply to them and how they can be used against them. Reports suggest that although users are aware there are laws in their country that can be used to prosecute them based on their sexual and gender identity, the exact nature of these laws are not clearly understood. This is especially the case for lesbian and bisexual women and trans individuals.

> "WE KNOW NOTHING! I NEED TO KNOW **WHAT COULD HAPPEN TO ME IF I GOT CAUGHT**."
>
> *Anonymous app user*

Emergency protocols for arrest

The respondents also wanted to know practical advice about what they can do if they are arrested and who they can reach. This is fundamental advice that needs to be regularly updated and maintained through contacts with local groups if provided.

Warnings and updates for LGBTQ people in country

The respondents stated that they are receiving advice from certain apps which they have found helpful. They are keen to get more up-to-date advice about what is happening in their country – including positive changes.

Sexual health advice

The respondents expressed much interest in getting more up-to-date advice on sexual health relevant in their country. This includes where they can turn to for medical support.

LOOKING TO THE FUTURE

What developers and tech companies must do

There is a clear international consensus that companies should, at a minimum, respect all human rights.

The UNGPs set out the human rights responsibilities of all business enterprises, and the UN Special Rapporteur on Freedom of Expression clarified that for ICT companies, a proper process of due diligence requires taking into account the human rights impacts of "design and engineering choices."

Due to these platforms' unique ability to connect, empower, provide avenues for expression, and build personal relationships, our research shows that LGBTQ users will continue to use them, even where usage entails serious risks to personal safety or privacy.

In order to meet the responsibility of respecting the human rights of users, app companies must implement effective prevention and mitigation strategies against established threats—as set out in the UNGPs—including proactive efforts to support users in staying safe. This requires the application of human rights principles throughout their operations.

Transparency in the implementation of the standards is also key: to publish efforts to address human rights impacts, especially to relevant stakeholders.

Apps should consider the design and operation of features within specific national contexts and with consideration to specific groups and demographics of users, particularly when their function relates to distinct at-risk groups.

Research – next steps

Going forward, more research will be needed: focussed on the most at-risk groups, the most under-researched and uninformed groups, and working to resolve the paradox of anonymity and verification.

This research is only the first step in finding methods to protect users of these technologies, aiming to increase the digital safety and security of

LGBTQ communities in the MENA region. We have aimed to find out what the risks are, and ask the users themselves which existing and missing features cause them concern.

We will continue to work directly with LGBTQ dating apps, international and local organisations, technology experts and advisors, and corporate social responsibility advisors to address the holes in the apps, develop methodologies to reduce the exposure of users, and raise awareness on digital and physical security and technologies among the larger communities of at-risk users in these countries.