Digital Security of LGBTQI Aid Workers: Awareness and Response

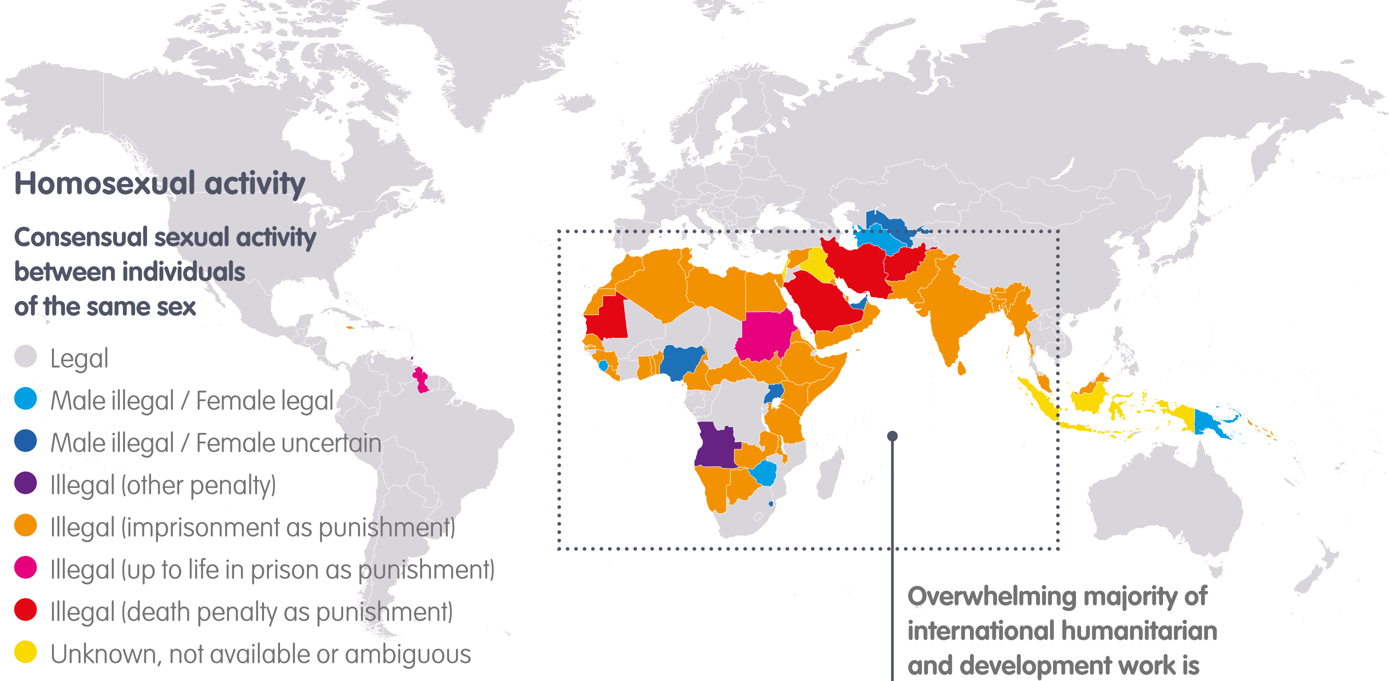
Mala Kumar

Mala Kumar is a technology for international development (ICT4D) professional and UX/UI designer who has worked for several agencies of the United Nations and for international NGOs throughout sub-Saharan Africa, New York and London since 2009.

She is the author of the novel The Paths of Marriage*, which has been sold worldwide. Her Op/Eds and interviews on ICT4D, LGBTQI rights, technology and diversity have appeared on* The Guardian UK, The Advocate, CNN India *and* USA Today.

Introduction

As the world becomes increasingly connected and more of our lives are recorded, accessed and processed digitally, the nature of threats and personal risks changes. Digital security threats[1] on their own can have a range of consequences to a person's life – from identity theft and fraud to destroying a credit history or ruining a reputation. For lesbian, gay, bisexual, transgender, queer and intersex (LGBTQI) aid workers working in areas of the world that are hostile and sometimes violent to people who identify or are perceived as LGBTQI, these digital threats can translate into real incidents in the physical space, such as harassment and imprisonment. Digital threats can also take a toll on mental health and destroy livelihoods.



Criminalization of homosexuality/homosexual acts as of 28 December 2016

Homosexual activity
Consensual sexual activity between individuals of the same sex
● Legal
● Male illegal / Female legal
● Male illegal / Female uncertain
● Illegal (other penalty)
● Illegal (imprisonment as punishment)
● Illegal (up to life in prison as punishment)
● Illegal (death penalty as punishment)
● Unknown, not available or ambiguous

Overwhelming majority of international humanitarian and development work is in these regions.

Source: Equaldex

[1] In this article, the term 'digital security threat' will refer to any potential or realised risk, threat or harm that is conducted, facilitated or enabled through a digital (i.e. online or virtual) environment.

Though the stakes are high, there is scarce research into the particular digital threats that affect LGBTQI aid workers. As such, this article provides an overview of the digital security threats and risks that LGBTQI aid workers face, offering simple strategies that NGOs and aid workers (LGBTQI staff and their colleagues) can take to identify, mitigate and respond to these risks to the greatest extent possible.With proper coordination among LGBTQI aid workers, their employing organisations and, where possible, greater civil society, all aid workers, regardless of their sexual orientation or gender, can realise their professional potential without undue physical, emotional, mental or personal harm. This allows individuals to thrive and organisations to meet their duty of care responsibilities towards staff.

The concepts of LGBTQI and SOGIE

The concepts of sexual orientation, gender identity and gender expression (SOGIE) can be interpreted in many ways. Often, the definition and understanding of the concepts vary by country or region, and ethnic, cultural or religious norms. Indeed, by the very nature of working in international humanitarian and development contexts, defining what 'SOGIE' means can be one of the hardest aspects in preventing and responding to both the digital and physical threats that NGO staff of a minority SOGIE may face.

In North America, Europe, and Oceania (i.e. primarily Australia and New Zealand), a common way to define SOGIE is by the categorisation 'lesbian, gay, bisexual, transgender, queer and intersex', or 'LGBTQI' for short. The first three letters – LGB – relate to sexual and affectional (or romantic) orientation. As is commonly known, 'lesbian' refers to women who are primarily attracted to other women and 'gay' refers to men who are primarily attracted to other men. The term 'bisexual' refers to a person whose sexual and affectional orientation is toward people of the same and other genders, or towards people regardless of their gender. A heterosexual person does not identify as lesbian, gay or bisexual; they are sexually orientated to only the *opposite* sex.

People who feel their birth sex and gender identity are consistent are referred to as 'cisgender', whereas someone whose gender identity and/or gender expression differs from their assigned sex at birth is *transgender*. This manifests in a wide range of identities and experiences – not all trans people undergo surgery or physical transition and some trans people question the gender binary altogether, identifying as neither entirely male nor female.

The 'I' in the LGBTQI acronym refers to 'intersex', meaning a person whose reproductive or sexual anatomy includes characteristics that are not consistent with the typical definition of either 'male' or 'female'. Finally, 'queer' is an all-encompassing term that refers to anyone who does not identify as entirely heterosexual and cisgender. It should be noted that the word 'queer' was and can still be used as a homophobic slur; however, in recent decades the term has been reclaimed by the LGBTQI community in many countries.

The concepts of sexual orientation and gender identity and gender expression as defined by the LGBTQI acronym do not necessarily translate globally, particularly in many Asian, African and Middle Eastern countries. Similarly, ethnic minority populations residing in North America, Europe and Oceania may not find the LGBTQI definition accurate. Many organisations thus opt to define physical sexual acts rather than a person's identity. For example, in public health, target populations in HIV/AIDS programmatic work are often defined as 'men who have sex with men' rather than 'gay men'. The former is the physical act of two men having sex, whereas the latter is an identity. Depending on the organisation and context, security experts may thus find it more appropriate to refer to LGBTQI staff as 'men who have sex with men', 'women who have sex with women', and so on.

Entire theories and discourses are devoted to SOGIE, and there are of course infinite nuances to these situations. For the purposes of this article, the LGBTQI acronym will be used interchangeably with those of a minority SOGIE; it will refer to those who identify as non-heterosexual and/or non-cisgender. Throughout this article, several intersections will be discussed within these acronyms, as they are principle motivating factors for discrimination, bias, violence and hostility against people who are, and/or people perceived to be, LGBTQI.

Intersectional considerations of being LGBTQI

As with many security issues, complicating factors in the security of LGBTQI persons are intersectional characteristics, such as a person's sex, ethnic origin, nationality, race and disability. Young women, for example, are the most likely to be harassed online, as discussed further below. Intersectional characteristics thus elevate the risks to LGBTQI staff's digital security in several ways, especially:

- Increasing the likelihood of an act of aggression taking place;
- Changing the nature of the threat;
- Changing the best response to the threat.

Certain intersectional characteristics of a person can change the leverage they have in society, which can also change the most appropriate response to digital threat. National origin and citizenship are two particularly complicating intersectional factors for organisations that have global, multi-national offices. Because digital threats can escalate quickly, decisions may have to be made before the full bearing of a person's national origin or citizenship can be understood and taken into account.

Responding to a digital threat on behalf of an LGBTQI aid worker therefore requires a balance to ensure the best outcome for the victim, as consequences can be a life or death matter. Though some aid workers may feel they have the leverage to stand their ground, seek punitive recourse or address the challenge head on, others may face a harsher reality that requires them to resolve issues discreetly. Any reaction to a digital threat must thus take into account intersectional challenges and the opinion of the aid worker affected whenever possible.

Figure 2 below provides a more complete list of intersectional characteristics.

Figure 2: Some factors in assessing personal risk in being an LGBTQI aid worker

• Duty station • Contract modality and level • Evacuation protocol (country, duration, etc.) • Mission (travel) obligations • Post (job) relationship with national government(s), partner organisations, etc. • Organisation's special legal provisions	**Organisation**
• Race • Religion • Nationality • Gender/Sex • LGBTQI expression • Physical or mental disability • Partner	**Person**
• National laws • Country culture towards LGBTQI people, your personal demographic • Where in the country you are based • Bi-lateral agreements with your country of citizenship	**Country**

Digital security risks particular to LGBTQI aid workers

Digital security threats for LGBTQI aid workers can come from a number of sources, hereafter referred to as aggressors. Gauging both the source of the threat and the appropriate response largely depends on whether the possible aggressor is within an LGBTQI aid worker's professional, personal or greater societal sphere. See Figure 3 for possible aggressors (overleaf).

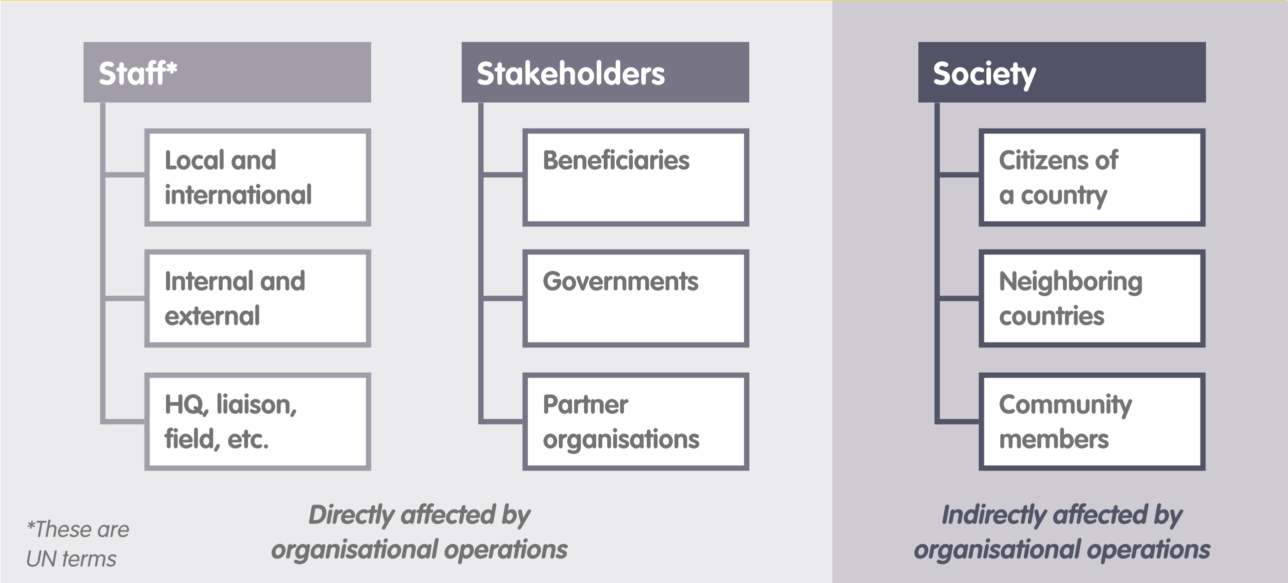
The bridge from digital to physical security

For LGBTQI aid workers, the bridge between digital security and physical security is of particular concern. Although most harassment and threats initiated online do not translate into physically harming a person, there are cases, however, where digital threats do lead to physical harm. This can occur in the following ways:

- An assailant physically targets a victim they had harassed online.
- Online abuse prompts a third party to physically target a victim.
- Continual and/or extreme online harassment leads to a victim experiencing mental distress, which can result in self-inflicted physical harm.
- Arrest if authorities deem the local laws to have been breached.
- The perception of the individual or organisation locally may impact the ability to implement programmes.
- The perception of the individual could result in job loss or job demotion.

Digital risks present within an LGBTQI aid worker's professional circle, such as those presented by colleagues in the same organisation or colleagues working on the same programmes or projects, can have the most immediate consequences, as physical access to the person and knowledge of the internal digital systems of an organisation are greatest. In any given organisational digital ecosystem, there are common tools: email, chat/messaging services, mobile/tablet devices, desktop/laptop PCs, video conferencing facilities and virtual protocol networks (VPNs). In relation to the first two scenarios above, these tools can be (mis-)used to track a person's movements, retrieve information about a (same-sex) partner or spouse, access financial records or housing information, and more. Similarly, details of an LGBTQI aid worker's life can be published online to give malicious third parties easier access to the victim.

Figure 3: Possible aggressors



In some cases, nearly every aspect of an aid worker's life in a country can be accessed by an NGO digital ecosystem. If this information is weaponised, an LGBTQI aid worker and their employer may find themselves in a number of precarious situations.

Commonly cited concerns include losing one's job, being transferred or demoted, being isolated or phased out from work, and being verbally or physically harassed. Though few international organisations based in North America, Europe or Oceania allow for open discrimination against LGBTQI staff, *proving* discrimination, bias or mistreatment on the basis of being LGBTQI is difficult and the onus falls largely on the victim. Organisations may also experience consequences, internally and externally, that may affect their programmes, operations or even their reputation, if one of their LGBTQI staff members is targeted by malicious actors.

Though national estimates vary and singular causes are hard to pinpoint, livestreaming suicide on social media is becoming a global phenomenon.[2] ThinkProgress, a progressive American think-tank, reported that children who are harassed online are 'three times more likely to contemplate suicide' and 'LGBT youth are particularly at risk for being targeted with this type of harassment.'[3] Similar studies elsewhere have not been conducted yet, but mental illnesses, such as post-traumatic stress disorder (PTSD), are increasingly being associated with humanitarian situations. Though there is a lack of research on the subject, a natural extension is that online harassment in the field because of one's SOGIE is likely to have an increased effect on an aid worker's propensity to self-harm.

Common examples of digital security risks and threats

The term 'digital footprint' refers to a person's digital mark on the world – from social media profiles, to articles and media about a person, to digitally stored financial records, electronic medical records, government records, and so on. Digital records can both reveal a person to be LGBTQI and are easily disseminated. In interviews conducted with LGBTQI UN staff for a forthcoming paper to be published by Fordham Law, participants cited threats arising out of digital records as particularly stressful and hard to control. Because digital threats are easily delivered, access to the victim is quicker and easier than face-to-face contact. In essence, the entire cycle of a digital threat – from identification of the victim, the discovery of the vulnerability, contact with the victim, the threat being administered, to the resolution – can be conducted digitally, making it hard to detect unless one is directly involved.

As with physical risks to security, digital risks can have consequences for the LGBTQI victim and the organisation alike. Consequences may include a compromised relationship with the government, partner organisations or beneficiaries. In some extreme cases, the status of an NGO's eligibility to work

[2] Boursquot, S. (2017). Facebook Live Suicides: Deaths on Social Media are a Growing Crisis. *International Business Times*. Available from: http://www.ibtimes.com/facebook-live-suicides-deaths-social-media-are-growing-crisis-2481865. [Accessed 10 July 2017].

[3] Culp-Ressler, T. (2014). The Real Life Consequences of Online Harassment. *ThinkProgress*. Available from: https://thinkprogress.org/the-real-life-consequences-of-online-harassment-5c8e9547a93e. [Accessed 9 July 2017].

in a certain part of the country or the country overall may come into question. Thus, while some incidents may be resolved through official police or government forces, the organisation may wish to take particular note of possible risks and threats, and prepare a response in advance.

Online harassment

Certain groups of people are more at risk for digital security threats than others, especially when it comes to online harassment. According to the Pew Research Center, young women are disproportionately more likely than any other group to experience sexual harassment and stalking online.[4] Psychological effects are more pronounced when the severity of the harassment increases. By virtue of being female and young, certain aid workers are already more likely to face online harassment due to their inherent characteristics, which is further complicated if the aid worker is also LGBTQI. Generic threats can escalate to specific threats of: revealing against someone's will that they are LGBTQI, sexual violence to 'correct' a person's orientation[5], or a larger group of people targeting someone due to their SOGIE. Particularly for those aid workers who must engage on social media for their job (a large portion of whom are young women), engaging with website comment sections or other online platforms can result in continued exposure to online harassment and take a toll on their mental health.

Sexually explicit media leaked

Depending on the national laws that govern privacy, hacking, and sharing, a digital privacy breach in one country may not be considered such in another. In recent years, several countries in North America and Europe have taken steps to introduce 'anti-revenge porn' laws, which make it illegal to post nude photos or recorded sexual acts of a person even if the act was consensual at the time of the recording. Though the jurisprudence required to have the media removed from online can be lengthy, the introduction of the bill itself has reduced the number of cases and has changed the discourse around ownership of sexually explicit property. However, these laws are not present in many countries that have a heavy aid worker presence. Without protection policies for LGBTQI people in a given country, there can be dire consequences for those who are implicated in sexually explicit content leaked online. Furthermore, depending on the context, an LGBTQI aid worker may be subject to criminal charges and increased harassment.

Being 'outed' online

Being outed (exposed as LGBTQI against one's will) online is a commonly encountered digital risk. When digital footprints overlap, for instance on project chatrooms, on LinkedIn or other social media, the lines between personal and professional boundaries become blurred, making the balance between withholding personal information and expressing oneself online challenging. Aid workers in information communications technology for international development (ICT4D), for example, are the most likely to engage with beneficiaries, stakeholders and government counterparts in a digital capacity. LGBTQI aid workers must therefore take special precautions to control privacy settings of every post, share, like, etc. that may reveal someone is LGBTQI in order to avoid unwanted information leaks. Depending on the complexity and transparency of the platform, managing the professional/personal line can be both time-consuming and painstaking.

An additional complication to the issue of social media management is legacy information. Aid workers who were early adopters of social media now have more than a decade of their lives stored online. Ten years in the context of LGBTQI rights can make a massive difference, and not always for the better. In India, for example, Section 377 of the national penal code was reversed in 2013, which *recriminalized* same-sex sexual acts. Nearly 1,500 arrests were made in 2015 under the law[6], many of which were facilitated by social media posts and other digital records the victims had posted of themselves while homosexual acts were still legal. Going back to all digital platforms that have been previously used and retroactively changing settings can be difficult due to new application versions, different privacy laws in different countries, interoperability among devices, and restoring access to platforms that are no longer used. Furthermore, as social media is, by definition, interconnected to other people, potentially sensitive information may not have been posted by the LGBTQI aid worker themselves; it might have been posted by a (well-meaning) friend, family member or colleague. Management of legacy information therefore includes not only the LGBTQI aid worker's activity online, but those in their greater online network.

Government surveillance

Surveillance laws and activity highly depend on the national government. In countries in which the government closely monitors digital activity within

[4] Duggan, M. (2014). Online Harassment, Summary of Findings. *Pew Research Center*. Available from: http://www.pewinternet.org/2014/10/22/online-harassment. [Accessed 15 July 2017].

[5] Carter, C. (2013). The Brutality of 'Corrective Rape'. *New York Times*. Available from: http://www.nytimes.com/interactive/2013/07/26/opinion/26corrective-rape.html. [Accessed 4 Aug. 2017].

[6] Duffy, N. (2016). India arrested hundreds last year under colonial-era anti-gay law. *Pink News*. Available from: http://www.pinknews.co.uk/2016/09/29/india-arrested-hundreds-last-year-under-colonial-era-anti-gay-law. [Accessed 2 Aug. 2017].

its borders, LGBTQI aid workers may be subject to deportation or other criminal charges for breaking government norms in expressing their SOGIE. This could include using dating apps that allow for same-sex matching, advocating for LGBTQI rights in online forums, posting pictures of oneself that are interpreted as immoral or impure, or surfing for gay or other 'non-normative' pornography. Especially for those NGOs that work closely with a national government, government surveillance of LGBTQI activity could compromise organisational relationships or collaborations. While every person is endowed with inalienable human rights, it is important for both LGBTQI aid workers and their employing organisations to understand the practical outcomes if cultural norms or local laws are broken.

Viral media

Like traditional media outlets, digital media outlets largely function on an ad revenue model. The more shares and views a piece of media receives, the higher it appears in Google and other algorithmic search engines, and the more the outlet can charge advertisers to appear on the article or video webpage. More shares equal higher profits.

Many digital media outlets do not have an ethical code that governs accidental or intentional outings of LGBTQI people. Indeed, major outlets such as *Gawker*[7] and *The Daily Beast*[8] have been implicated in such controversies in the past few years. In some contexts, a news outlet's desire to find viral content may result in backlash from greater society or the national government on an LGBTQI aid worker. According to a report by the Internet Governance Forum on 'Digital Threats and Opportunities for LGBTQI Activists in Jordan', one such incident was a blog posting the profile pictures of members on the gay dating apps, Grindr and Scruff.[9] The blog post was shared more than six times as often as the average news piece in Jordan. In national polls, up to 97 per cent of Jordanians say they are against homosexuality, making a public outing dangerous. Though it was unclear if the Jordanian government took action against the outed men as a result of the publication, other incidents have been reported in Chechnya and throughout East Africa and South Asia, whereby the outed person was subject to state-sanctioned violence or faced deportation.[10] For many LGBTQI aid workers, a viral media outing can compromise the worker and the organisation's relationship with the national government and local community.

Blackmail

Digital security threats to LGBTQI aid workers can come from their personal sphere, including family, friends and romantic or sexual partners. With the ever-increasing popularity and accessibility of online dating websites and apps, LGBTQI aid workers often have the same or similar means to find romantic and sexual partners as their non-LGBTQI colleagues in areas typically hostile to LGBTQI people.

In a forthcoming paper to be published by Fordham Law on LGBTQI United Nations staff rights, a commonly cited threat that arises from a staff member being outed as LGBTQI was blackmail. As many aid staff are from abroad, they are oftentimes relatively more affluent than the local community, or perceived to be so, elevating the risk of being threatened for monetary gain. Blackmail can imply many forms of pay out; if an LGBTQI NGO aid worker is not relatively affluent or not perceived to be so, the demand in exchange for keeping an LGBTQI identity secret can shift from monetary to sexual favours or demands to commit criminal acts. Not only does this present a serious threat to the affected aid worker, but blackmail-related crime would also negatively impact the reputation of the aid worker's employing organisation.

The entire cycle of blackmail can take place in the digital space, making it difficult to identify and address the warning signs and appropriate responses to the threat. In cases throughout sub-Saharan Africa, Asia and the Middle East, former male sexual partners of male international aid workers are commonly cited as the source on the basis of which the police arrest or demand bribes from the implicated aid worker.

Mitigating and responding to digital security risks

There are some basic precautions that LGBTQI aid workers and NGO security professionals can take to mitigate digital security risks affecting LGBTQI aid staff. Organisations must also consider ways in which to respond to these digital security threats to protect their staff and programmes. It is important that all aid staff are made aware of the risks faced by LGBTQI colleagues and their role in safeguarding these colleagues' security.

[7] See Bolton, D. (2015). Tommy Craggs and Max Read resign from Gawker Media following controversy over article 'outing' David Geithner. *Independent*. Available from: https://www.independent.co.uk/news/media/tommy-craggs-and-max-read-resign-from-gawker-media-following-controversy-over-article-outing-david-10402799.html. [Accessed 16 Nov. 2017].

[8] See Demianyk, G. (2016). The Daily Beast Apologises After Being Accused Of Outing Gay Olympians With 'Unethical' Grindr 'Stunt'. *Huffington Post*. Available from: http://www.huffingtonpost.co.uk/entry/daily-beast-grindr-olympic-village-gay-athletes_uk_57accb04e4b01ec53b3ee717. [Accessed 16 Nov. 2017].

[9] Abdel-Hadi, K. (2017). Digital Threats and Opportunities for LGBT Activists in Jordan. *Medium*. Available from: https://medium.com/my-kali-magazine/report-digital-threats-and-opportunities-for-lgbt-activists-in-jordan-ef60672dcac1. [Accessed 9 July 2017].

[10] Gesson, M. (2017). The Gay Men Who Fled Chechnya's Purge. *The New Yorker*. Available from: http://www.newyorker.com/magazine/2017/07/03/the-gay-men-who-fled-chechnyas-purge. [Accessed 1 Aug. 2017].

NGO security professionals

Although digital security is not typically assigned to NGO security professionals, in smaller organisations, digital security might be an extension to the job, as many do not have the resources to employ full technical security personnel. Conversely, large organisations often have their primary IT staff located in headquarters, and these IT teams may be disconnected from the digital security realities of staff working in the field. Therefore, NGO security professionals should consider the following practical steps that they and appropriate colleagues can take to ensure the safety of LGBTQI aid workers (and all staff).

Organisational security

The most immediate step is to check that the organisational digital ecosystem is secure and roles are clear. As with physical security, a threat analysis should be conducted. Who or what are the most likely aggressors? Are they internal to the organisation or external? Are the organisation's Internet connections secure? Is software installed to prevent viruses and to block hackers? Furthermore, what information about aid workers must be collected? Is it stored in a secure fashion? Who has access to that information, when and for what purpose? Can that information be illegally or immorally shared, stored or otherwise abused? Understanding how organisational digital technology and data is supposed to be used clarifies how it should not be used, and what can be done to prevent misuse or breaches.

(Better) Training

Despite the seemingly ubiquitous nature of digital technology, the adoption and comprehension rates of global aid staff varies widely. With this in mind, creating mandatory trainings and seminars on how to use organisational and personal technology, including social media, can be invaluable. Most training that is conducted on digital technology is tedious and tends to focus on minute tasks. Adding a training module that stresses the security risks one faces can better engage staff; for example, by comparing dummy social media profiles with weak/strong privacy settings. As the link between digital security and personal well-being is not always evident, this training would be especially valuable for new aid workers or aid workers who have not worked in hostile environments before. Though care should be taken to not out any one person or persons, using inclusive language and alerting staff that certain groups may be at higher risk to digital security threats is essential. Staff should be sensitised to the concept of informed consent, so that any person who is tagged, named or photographed for a social media post, article, website or blog knows in advance and can react if needed.

Creating safe spaces

One of the simplest solutions for creating a more digitally secure environment for LGBTQI aid staff is simply creating safe spaces and open dialogues. Rarely are security and technology trainings inclusive of LGBTQI people in their language. As mentioned in a previous section, the entire cycle of risk and threats to LGBTQI aid workers can occur digitally. If an aid worker does not feel comfortable or is not sure if they can approach security personnel with their problems, the issue can easily go undetected. Eventually, this can pose a larger problem to an organisation.

Whenever possible, gender neutral words, such as 'partner' or 'spouse' instead of 'wife' or 'husband' should be used. Inclusive language should also avoid implying that non-LGBTQI are 'normal' and that LGBTQI people are 'abnormal' or should be otherwise stigmatised. Depending on the openness of the organisation's policies, security staff may also want to work with the organisation's marketing and communications staff to include pictures of LGBTQI staff, families, stakeholders or beneficiaries on the organisation's website or other promotional materials. Even if these images can only appear on websites or promotional materials distributed in certain countries that are relatively open to LGBTQI people, the message of inclusion can be powerful.

While the terms and language for the LGBTQI community can be complex, NGO security personnel may find it well worth their time to survey the local context and figure out the best way to address and speak about the LGBTQI community. This can be done through connecting with local LGBTQI human rights centres or organisations, reaching out to partners who have previously worked on LGBTQI rights in the area, or reaching out to staff who have indicated they are willing to help. Clarifying that NGO security personnel are not only there to serve heterosexual and cisgender people will encourage LGBTQI aid staff to seek help if needed. A slight change in language, phrasing, tone and body language can make a large difference in encouraging LGBTQI aid workers to seek assistance.[11]

Safe spaces can be created online or offline, in open or (semi-)closed environments. When observing the correct security protocols, internal chat services, support via email or teleconferencing can be an effective way to engage LGBTQI aid staff, especially those serving in remote locations. These digital spaces can be held regularly and as an open forum for

[11] See Stonewall for help and advice: https://www.stonewall.org.uk/help-advice. [Accessed 13 Sept. 2017].

anyone who wishes to participate. They can also be set up in closed environments and/or one-on-one, though it is important that NGO security staff clearly and widely articulate that it is an organisational norm to seek help on a variety of issues. If seeking assistance becomes synonymous with being LGBTQI, those who are most in need of support will be deterred from reaching out. Any support session should be held by a person sensitive to LGBTQI issues who can then relay digital security issues to the appropriate party without compromising stated or understood anonymity. Even if the best support person is not located in the same country, creating avenues to receive counsel can be critical to starting much-needed dialogue.

Be clear and transparent

NGO security professionals should make it clear what organisational policies can realistically do to help LGBTQI aid workers. Considerations can vary from the contract modality of an aid worker, to the national laws of a country, to the financial resources of an organisation. If it is known that a national government will conduct surveillance on NGO staff, being transparent *to all staff* about that reality is paramount. Complex social norms and societal standards mean it is impossible to know every member of staff that may identify as LGBTQI simply based on appearances or mannerisms. Informing all staff of the possible digital threats LGBTQI staff face, and what an organisation has in place to prevent, mitigate or respond to these digital risks will help LGBTQI aid staff make the best decisions for themselves.

Responding to digital security threats

Responding to any digital security threat or transgression can take a wide range of actions. Similar to physical security responses, one of the first steps is to isolate the threat. If the victim of the attack does not know the aggressor, work with the IT department of your organisation to pinpoint who did what. Identify all possible breached platforms or devices and reset associated passwords; if necessary, change usernames and other associated credentials. If possible, contain any unwanted pictures, texts, digital communications or other personal information from being shared by contacting the customer service desks of social media or telecom providers that are being used to share the information. Be sure to use a secure connection when doing so. Alert banks and other financial institutions if monetary demands are made or are likely to be made. Aim to manage and limit the impact on the organisation itself in order to avoid placing other LGBTQI staff at risk or undermining the organisation's reputation with local authorities and partners.

Depending on the victim's preferred course of action, their citizenship, contract modality and other particulars, alert the appropriate embassy or embassies of possible criminal activity. Similarly, depending on the local law, contact the appropriate police authority if advisable. Finally, alert other staff members that they should report directly to the organisation's security personnel if further threats or transgressions are made. If the situation is particularly dire, consider starting the evacuation or relocation procedure for the victim, their family and other affected persons. Throughout the entire response, take extra caution to only share the information needed to contain the threat. Do not unnecessarily disclose that the victim is LGBTQI, as this may deter help and further complicate the victim's situation.

LGBTQI aid staff

Check the settings on digital platforms and search for your own name

Especially while in a context that is hostile to LGBTQI people, ensure that social media posts are only viewable to trusted people, 'trusted' being defined as those who are both supportive of LGBTQI people and who will not accidentally or purposely reveal someone else's SOGIE. To check legacy information, search for one's own name in both Google and non-algorithmic/non-ad driven based search engines, such as DuckDuckGo.com. It is also possible to set up a Google Alert (https://www.google.co.uk/alerts) to regularly check this. Also, to see if one's email address and passwords have been subject to breach it is possible to use https://haveibeenpwned.com. If access to a platform with potentially sensitive information cannot be gained, write to the customer service of the platform using a secure connection and ask the information to be taken down. When safe to do so, repeat this process whilst in-country, as search results may change depending on where the search is conducted. Finally, test multiple share settings. Facebook's 'View As' feature is a useful way to quickly see what the public, a specific person or someone in a given network, can see on one's own personal profile. Similarly, test the viewability of potentially sensitive comments on websites, other social media profiles and apps. While the process can be cumbersome and frustrating, combing through one's own digital footprint is still one of the most effective ways of preventing unwanted information from being exposed.

Using best digital security practices

Making safe digital practices a habit is an effective way of avoiding preventable information leaks. Every device that has access to email, chat, or social media accounts should be password or pincode protected. Poor password management in itself can be a security risk. While creating a long and unique password or pincode for every account is not always possible, at the very least, personal and work accounts should not have any overlapping passwords or pincodes. Though higher-end smartphones have multiple unlocking technologies, such as fingerprint and retina recognition, as relatively nascent technologies, there are more unknown security gaps. As such, having at least one layer of security in the form of a standard pincode or password that must be typed in is preferable.[12] It is recommended to turn on encryption as a standard practice. Also, consider the use of tools for chat that allow an extra level of digital security, such as Signal App that have disappearing messages.

As discussed in a previous section, online dating websites and apps have given LGBTQI aid workers the same or similar means as their non-LGBTQI colleagues to find romantic and sexual partners in areas typically hostile to LGBTQI people. While this article does not intend to deter LGBTQI people from exercising their right to associate, it should be stressed that the utmost caution should be taken whilst using these websites and apps. Before first meeting someone from a dating website or app, always voice verify with a phone call (or Skype, WhatsApp, FaceTime, etc.) to ensure the person is real. When meeting for the first time, pick a location that is public and with an easy escape route. Even if the nature of the meeting is not disclosed, take caution to tell a colleague, friend or security official in your organisation who is currently in the country when and where you are meeting someone. Establish a check-in procedure with this person, such as phoning or sending a message on a designated platform (WhatsApp, Facebook messenger, etc.) at a designated time.[13] Consider, also, that different applications have different security implementations.[14]

Mental health awareness

With digital technology constantly evolving, its effect on mental health is also ever-changing. As mentioned previously, the direct link between the two appears to be strengthening as society places increased value on a person's digital presence. Every year, Facebook has seen a rising number of suicides livestreamed and posted online.[15] Mental health among aid workers in general has become a topic of increased discussion, particularly on news outlets such as *The Guardian*.[16] While the sub-group of LGBTQI aid workers has not received as much attention, undoubtedly there is a link between mental health and being LGBTQI in the field.[17]

Understanding the mental health effects of field postings is important for international LGBTQI aid workers and their use of digital technology. In periods of sadness, depression and vulnerability, posting online and sharing information digitally is a natural outlet. While LGBTQI aid workers should be free to use digital means of expression, being aware of an altered state of mind and always using secure methods of communication is critical. Some digital platforms offer self-checks in (anticipated) periods of vulnerability. Gmail, for instance, offers an 'Undo Send' feature that gives a sender up to 30 seconds to 'unsend' an email. Apps such as DrunkLock track alcohol consumption of a user and can automatically cut access to social media platforms on mobile devices once a user has hit a threshold.[18]

Finding safe spaces

An unfortunate reality that many LGBTQI aid workers face is not having the proper organisational support that heterosexual, cisgender colleagues may receive. Mobile devices and personal computers often carry intimate details of a person's life. Thus, allowing someone else to view a device and, therefore, intimate personal details, to resolve a security breach can be a risk itself. Several technology-oriented organisations, such as Out in Tech[19] and Lesbians Who Tech[20], can link LGBTQI aid workers to pro-bono services, including technology counselling. Though these should not be considered as an alternative to proper organisational mechanisms, they can be a great starting point for inquiries that cannot be solved by searching online.

[12] See Security First online digital security training resources on the Advocacy Assembly website: https://advocacyassembly.org/en/courses/?filter=Digital%20Security. [Accessed 16 Nov. 2017].

[13] Technical advice available from: https://securityinabox.org/en/lgbti-mena/lgbt-dating/. [Accessed 16 Nov. 2017].

[14] See Greenberg, A. (2016). Gay Dating Apps Promise Privacy, But Leak Your Exact Location. *Wired*. Available from: https://www.wired.com/2016/05/grindr-promises-privacy-still-leaks-exact-location/. [Accessed 16 Nov. 2017].

[15] Boursquot, S. (2017). Facebook Live Suicides: Deaths on Social Media are a Growing Crisis. *International Business Times*. Available from: http://www.ibtimes.com/facebook-live-suicides-deaths-social-media-are-growing-crisis-2481865. [Accessed 10 July 2017].

[16] Various authors. (2016). Aid worker wellbeing (series). *The Guardian*. Available from: https://www.theguardian.com/global-development-professionals-network/series/aid-worker-wellbeing. [Accessed 22 Aug. 2017].

[17] Moreno, R. (2015). I'm an aid worker…and I'm gay. *The Guardian*. Available from: https://www.theguardian.com/global-development-professionals-network/2015/mar/12/im-an-aid-worker-and-im-gay-lgbt-ngos. [Accessed 22 Aug. 2017].

[18] Karch, M. (2017). Avoid Drunk Emails and Drunk Social Media. *Lifewire*. Available from: https://www.lifewire.com/avoid-drunk-emails-social-media-1616668. [Accessed 9 July 2017].

[19] See https://outintech.com/. [Accessed 13 Sept. 2017].

[20] See https://lesbianswhotech.org/. [Accessed 13 Sept. 2017].

Safe spaces through Facebook groups and online forums, such as GAYd worker[21], are targeted to LGBTQI aid workers. Especially for those LGBTQI aid workers working from remote and/or very conservative contexts, finding support online can offer much needed reprieve and support for ensuring strong mental health.

Conclusion

Changes in digital technology move at an exponential pace. While the evolution of LGBTQI rights has dramatically improved in some countries in recent years, these improvements are far from uniform globally. The digital footprint of an LGBTQI aid worker can be both the best tool to keep one safe, as well as easily weaponised to cause harm.

NGO security professionals and LGBTQI aid staff alike must constantly be aware of possible aggressors, digital risks and digital threats. This article offers a basic breakdown of each of these, though the list discussed here is not intended to be comprehensive. As countries in which aid workers are based embrace new digital technologies, such as drones, the Internet of Things[22], and increasingly sophisticated audio and graphical manipulation tools, the risks and threats will necessarily change. At the core, NGO workers, both LGBTQI and their colleagues, should use inclusive language, employ standard best digital security practices at personal and organisational levels, be aware of the role of mental health, and be open and transparent about the limitations of an organisation's advocacy. While it is impossible to completely avoid risk, by following these practices individuals and employing organisations will greatly reduce their digital security concerns and ensure LGBTQI aid workers are able to contribute fully, safely and securely.

[21] See https://gaydworker.wordpress.com. [Accessed 22 Aug. 2017].

[22] See https://en.wikipedia.org/wiki/Internet_of_things. [Accessed 13 Sept. 2017].

Bibliography

Abdel-Hadi, K. (2017). Digital Threats and Opportunities for LGBT Activists in Jordan. *Medium*. Available from: https://medium.com/my-kali-magazine/report-digital-threats-and-opportunities-for-lgbt-activists-in-jordan-ef60672dcac1. [Accessed 9 July 2017].

Bolton, D. (2015). Tommy Craggs and Max Read resign from Gawker Media following controversy over article 'outing' David Geithner. *Independent*. Available from: https://www.independent.co.uk/news/media/tommy-craggs-and-max-read-resign-from-gawker-media-following-controversy-over-article-outing-david-10402799.html. [Accessed 16 Nov. 2017].

Boursquot, S. (2017). Facebook Live Suicides: Deaths on Social Media are a Growing Crisis. *International Business Times*. Available from: http://www.ibtimes.com/facebook-live-suicides-deaths-social-media-are-growing-crisis-2481865. [Accessed 10 July 2017].

Carter, C. (2013). The Brutality of 'Corrective Rape'. *New York Times*. Available from: http://www.nytimes.com/interactive/2013/07/26/opinion/26corrective-rape.html. [Accessed 4 Aug. 2017].

Culp-Ressler, T. (2014). The Real Life Consequences of Online Harassment. *ThinkProgress*. Available from: https://thinkprogress.org/the-real-life-consequences-of-online-harassment-5c8e9547a93e. [Accessed 9 July 2017].

Demianyk, G. (2016). The Daily Beast Apologises After Being Accused of Outing Gay Olympians With 'Unethical' Grindr 'Stunt'. *Huffington Post*. Available from: http://www.huffingtonpost.co.uk/entry/daily-beast-grindr-olympic-village-gay-athletes_uk_57accb04e4b01ec53b3ee717. [Accessed 16 Nov. 2017].

Duffy, N. (2016). India arrested hundreds last year under colonial-era anti-gay law. *Pink News*. Available from: http://www.pinknews.co.uk/2016/09/29/india-arrested-hundreds-last-year-under-colonial-era-anti-gay-law. [Accessed 2 Aug. 2017].

Duggan, M. (2014). Online Harassment, Summary of Findings. *Pew Research Center*. Available from: http://www.pewinternet.org/2014/10/22/online-harassment. [Accessed 15 July 2017].

Equaldex homepage image. (2017). http://www.equaldex.com/. [Accessed 8 Dec. 2017].

GAYd Worker. (2016). https://gaydworker.wordpress.com. [Accessed 22 Aug. 2017].

Gesson, M. (2017). The Gay Men Who Fled Chechnya's Purge. *The New Yorker*. Available from: http://www.newyorker.com/magazine/2017/07/03/the-gay-men-who-fled-chechnyas-purge. [Accessed 1 Aug. 2017].

Greenberg, A. (2016). Gay Dating Apps Promise Privacy, But Leak Your Exact Location. *Wired*. Available from: https://www.wired.com/2016/05/grindr-promises-privacy-still-leaks-exact-location/. [Accessed 16 Nov. 2017].

Karch, M. (2017). Avoid Drunk Emails and Drunk Social Media. *Lifewire*. Available from: https://www.lifewire.com/avoid-drunk-emails-social-media-1616668. [Accessed 9 July 2017].

Moreno, R. (2015). I'm an aid worker…and I'm gay. *The Guardian*. Available from: https://www.theguardian.com/global-development-professionals-network/2015/mar/12/im-an-aid-worker-and-im-gay-lgbt-ngos. [Accessed 22 Aug. 2017].

Security-in-a-Box. (2017). Protect Yourself And Your Data When Using LGBT Dating Sites. *Security-in-a-Box*. Available from: https://securityinabox.org/en/lgbti-mena/lgbt-dating/. [Accessed 16 Nov. 2017].

Various authors. (2016). Aid worker wellbeing (series). *The Guardian*. Available from: https://www.theguardian.com/global-development-professionals-network/series/aid-worker-wellbeing. [Accessed 22 Aug. 2017].

Acknowledgements

The author would like to thank fellow ICT4D professional, Linda Raftree, for her facilitation with EISF and for her support on the issue of LGBTQI rights and security over the years.

The author would also like to thank Gabrielle Demblon for her insights on LGBTQI/SOGIE identity, as well as her editorial contributions to this article.

Finally, the author would like to thank the EISF staff, especially Adelicia Fairbanks and Lisa Reilly, for creating this opportunity.

EISF would also like to thank Rory Byrne (Security First) for his kind support in contributing to this article.

European Interagency Security Forum (EISF)

EISF is an independent network of Security Focal Points, who currently represent over 90 Europe-based humanitarian NGOs operating internationally. EISF is committed to improving the security of relief operations and staff. It aims to increase safe access by humanitarian agencies to people affected by emergencies. Key to its work is the development of research and tools which promote awareness, preparedness and good practice.

EISF was created to establish a more prominent role for security risk management in international humanitarian operations. It facilitates exchange between member organisations and other bodies such as the UN, institutional donors, academic and research institutions, the private sector, and a broad range of international NGOs. EISF's vision is to become a global reference point for applied practice and collective knowledge, and key to its work is the development of practical research for security risk management in the humanitarian sector.

EISF is an independent entity currently funded by the US Office of Foreign Disaster Assistance (OFDA), the Swiss Federal Department of Foreign Affairs (FDFA), the Department for International Development (DFID) and member contributions.

www.eisf.eu

About the Communications Technology and Security Risk Management Hub

The Communications Technology and Security Risk Management Hub is a project by EISF that was launched in October 2014. The project aims to begin a conversation towards a better understanding of the specific nature of the security threats created by the digital revolution, and the implications for the security risk management of humanitarian staff and programmes.

The first publication of this project (October 2014) brought together 17 authors who analysed in 11 articles how communications technology is changing the operational environment, the ways in which communications technology is creating new opportunities for humanitarian agencies to respond to emergencies, and the impact that new programmes have on how we manage security.

The hub aims to provide an outlet for researchers and practitioners to make original and policy-relevant research available to the humanitarian community. Each article is reviewed by experts. If you would like to contribute please contact the editor of the series at eisf-research@eisf.eu.

http://commstech-hub.eisf.eu

Disclaimer

EISF is a member-led grouping and has no separate legal status under the laws of England and Wales or any other jurisdiction, and references to 'EISF' in this disclaimer shall mean the member agencies, observers and secretariat of EISF.

The content of this document is not intended to amount to advice on which you should rely. You must obtain professional or specialist advice before taking, or refraining from, any action on the basis of the content of this document.

While EISF endeavours to ensure that the information in this document is correct, EISF does not warrant its accuracy and completeness. The information in this document is provided 'as is', without any conditions, warranties or other terms of any kind, and reliance upon any material or other information contained in this document shall be entirely at your own risk. Accordingly, to the maximum extent permitted by applicable law, EISF excludes all representations, warranties, conditions and other terms which, but for this legal notice, might have effect in relation to the information in this document. EISF shall not be liable for any kind of loss or damage whatsoever to you or a third party arising from reliance on the information contained in this document.