Supporting Lesbian Gay Bisexual Transgender and Intersex human rights defenders in the digital age

Dan O Clunaigh

Introduction

The widespread diffusion of Information and Communications Technologies (ICTs) has empowered activists and minority communities to spread information, campaign, build communities and challenge injustice in new and powerful ways. The LGBTI activist community has been no exception to this, as the increased potential for communication beyond established social channels, less confined by social norms and geographic isolation has facilitated LGBTI people's expression and development of identity and ability to join forces to challenge the dangers and injustices faced by the community.

However, the spread of ICTs have also created new opportunities for antagonists to subject human rights defenders' to entrapment, control, intimidation and harassment. This has led to the need for an awareness-raising and capacity-building effort in order to strengthen Human Rights Defenders' (HRDs) capacities to react against emerging threats to their wellbeing from the digital space. Over the past decade, Tactical Technology Collective (Tactical Tech) has been at the forefront of this movement. Working with actors in the field of Human Rights, including Front Line Defenders, Tactical Tech's effort has spawned the development of a range of toolkits and guides, awareness-raising and training initiatives in order to build capacities among HRDs in terms of their wellbeing, the security of their communities and the safeguarding of their information and privacy.

Over the past year, Tactical Tech has begun a process of further deepening our efforts to raise awareness and inspire behaviour change among HRDs through further integrating digital security practices into the contexts of specific communities at risk. This article details the development and content of the first such materials to be developed with this in mind – a digital

security guide for the Arabic-speaking LGBTI community – the first version of which was launched in September of 2013.

Digital (in)security, activism and the LGBTI community

The ascent and spread of the internet and ICTs over the last two decades has had a profound impact on the promotion and defence of human rights on a global scale. As perhaps most profoundly evidenced by the rapidly changing political landscape in the Middle East and North Africa since 2011, along with many other countries, HRDs – journalists, lawyers, whistleblowers, students, the unemployed, political dissidents, and a wide variety of other social and political groups – have taken to ICTs as a potent tool in campaigning, researching, spreading information, organising and communicating.

In parallel, the diffusion of ICTs through global society has had a profound impact not only on LGBTI activism, but in many cases the establishment or development of LGBTI communities themselves, particularly in closed, repressive and heteronormative societies. Indeed, the world over, the internet often provides the first exploratory path or even "refuge" for young LGBTI individuals exploring or affirming their identity; this is perhaps due to the sense of "safety" and relative anonymity provided by the experience of browsing the internet for information, exploring online communities, chat rooms, dating sites, and so on, where people often feel that simply employing a pseudonym precludes them from being identified.

However, in spite of the progress achieved by progressive elements of civil society thanks in part to these tools, the continued repression faced by HRDs in the sites of some of the most turbulent uprisings of the last couple of years – Bahrain, Egypt, Syria, and Tunisia, to name just a few – is sad testament to the fact that along with new opportunities for organising, communicating and fighting for recognition, ICTs also provide new opportunities for the surveillance, entrapment, control and persecution of HRDs.

It is becoming ever clearer that social networking, media and communication tools, perhaps most notably Facebook, Twitter, and Skype among others, are now routinely being utilised as particularly rich "honey pots" for the surveillance and information-gathering on progressive elements of civil society. The surveillance of HRDs' activities or compromising of their accounts, achieved through a broad range of methods including phishing attacks, installation of trojan spyware such as FinSpy software, legal demands

for information from site hosts or internet service providers, or the widespread collection of account metadata, can and have been used against HRDs in order to expose their networks, access their information and identities, discover their location and plans, and subject them to juridical harassment.

Similarly, notwithstanding the vital outlet it provides for LGBTI individuals in repressive societies to reach out to one another, connect, establish relationships, friendship and community, the information vulnerabilities in the architecture and use of ICTs have unfortunately become a tool in the repository of antagonists to the LGBTI community – whether agents of the state, religious or political groups, or homophobic elements within local communities, clans and families.

The spread of social networking sites has brought a number of benefits to LGBTI individuals in terms of access to alternative information, speed of communication and community building. However, due in part to the architecture of such services, which tend to guide users towards oversharing and making public of information by default, has also led to the exposure of LGBTI individuals to homophobic elements of the state and society. In May of 2013, two men in Algeria were reportedly jailed on accusations of "breaching public morality" and "incitement to debauchery" because they allegedly announced their marriage on facebook and addressed one another there as "husband" and "wife," which was seen by people from the community who reported them to the police, who in turn acted upon the report.[1]

A further means by which LGBTI individuals have been exploited through ICTs is through their use of LGBTI dating sites. In relatively liberal and deeply heteronormative countries and regions alike, LGBTI people take to these sites as a place where they can express their sexual or gender identity in a supposedly secure environment, and seek personal connections. In contexts where people cannot safely engage in this activity in their public lives, such sites are quite naturally understood as something of a refuge, both in terms of the external search for friendship, sexual encounters, romance and so forth, as well as no doubt a comforting antidote to discourses which encourage people to think that LGBTI individuals – much less an LGBTI "community" – exists in the first place.

Sadly, homophobic agents of the state, religious groups and communities have taken to these sites in order to exploit, entrap and attack the vulnerable. The practice of setting up fake profiles on such sites and using them to lure

vulnerable individuals into meetings where they can be then subjected to physical attacks, blackmail, arrest, detention, torture, sexual assault and rape is extremely widespread and utilised by a wide range of actors, most notably the Egyptian police, who in the years following the Queen Boat incident in 2001, began a campaign of entrapment, arrest and torture of LGBTI individuals through dating sites. While this widespread practice poses a threat to all users of LGBTI dating sites, individuals engaged in activism are naturally at higher risk, particularly if they maintain a public profile as an element of their activism.

As with social networking sites more generally, this is in part due to a lack of knowledge and thus ability to think critically about the architecture of such sites on a technical level. However, a significant vulnerability to such attack lies in behavioural aspects of using such sites, such as having a publicly accessible profile with an identifiable face picture, registering under a real name, agreeing to meet hastily or in an unsafe environment such as a private home without having first verified the *bona fides* of their potential new contact. At times, digital security doesn't relate to technology but rather the decisions we, as users, make about our interaction with it.

Aside from surveillance and entrapment, ICTs have also been used as a direct means of attacking and stigmatising LGBTI individuals, which could be seen as an extension of the issue of technically mandated violence against women. A very public example is demonstrated by the vandalisation of the website of the Tunisian LGBTI magazine *GayDay* in 2012, when a group of malicious hackers defaced the website with homophobic slurs, and also gained access to the magazine's Twitter profile as well as the email accounts of contributors (Amaya-Akermanns, 2012).

Security in context

It is in this context that, in early 2012, Tactical Tech was contacted with a view to creating specific digital security materials aimed at the LGBTI community – in the first instance, focusing on the Arabic-speaking region. Over the past decade, Tactical Tech and our partner organisations including Front Line Defenders, have developed a wide range of awareness-raising and capacity-building materials, along with direct trainings and curricula, aimed at the human rights community worldwide. In 2012, over 6 000 activists, HRDs, journalists and communities at risk were exposed to our awareness-raising

and direct training interventions worldwide, and our online digital security learning resource, *Security in a Box: Tools and tactics for your digital security,* now averages around 250 000 unique hits per month.

The request to create materials for a specific community coincided with a process of reflection, re-evaluation and refinement of our approach to digital security awareness raising and capacity building: in particular, we have noted problems with the adoption of a tool- or technology-focused approach to digital security which tends to encourage HRDs to fight technology with technology, and reify a false distinction between digital security and "security" more generally, as well as its other elements, including personal, organisational and psycho-social security.

This is leading us to shift towards what, for now, we're calling "security in context": that is to say, placing information and digital security within the context of HRDs' broader context, in terms not only of their missions, work, and personal lives, but also within the broader context of security planning – personal, organisational, psychological, and so on - as an aspect of the work of HRDs.

This process – while it's just starting – will take shape in the development of materials which will give specific communities at risk context-relevant entry points to *Security in a Box* as well as other awareness-raising and capacity-building materials, and help us identify areas where the technical guide could be expanded. These guides should represent the answers to a number questions HRDs may ask themselves upon discovering *Security in a Box*, such as *"how would I take all the material from Security in a Box and use it in a practical sense? What is my practical motivation for doing this? What are the most important elements in this for me? How does it relate to my work? How does it relate to my security in general?"*

This initial request gave us our first opportunity to test this approach. So, in February 2012, a team of trainers from Tactical Tech organised a training for 10 LGBTI human rights defenders from the Arabic-speaking region in Istanbul, Turkey, designed both as a "regular" training as well as a springboard for sourcing material that the first guide might include. In the 15 months that have followed, Tactical Tech worked with Fadi Saleh, a participant in the training and LGBTI activist from Syria, to research and write the first version of what is now called "*Security in Context: Tools and tips for the Arabic-speaking LGBT community*" (Tactical Technology Collective, 2013).

This version of the guide – which, we hope, will be expanded upon and further refined with time and feedback from the community – includes a context-setting visualisation which explores the legal situation for the LGBTI community in each country, as well as highlighting individual demonstrative cases of digital attacks, such as those mentioned above. Regarding the latter, a challenge was posed by the simple lack of data available in some countries, where LGBTI-related information is, due to the severity of the social context, kept quiet.

Of course, one of the key principles of "security in context" is that HRDs need to carry out a "risk analysis" in order to determine which digital security practices are necessary in their situation: some digital and information security practices may be of vital importance in one situation, and entirely counterproductive or even insecure in another. Therefore, we included a short guide to risk analysis which gives readers the basic tools and concepts necessary to think critically about digital security risk in their context.

Participants at the training in Istanbul also – maybe unsurprisingly – requested a guide to how to use dating sites safely, which looks both at technical and behavioural considerations to take into account. This includes advice ranging from simple things, like having a first meeting in a safe, public location or verifying someone's *bona fides* through shared contacts within the community, to slightly more complex, but still quite user-friendly options like connecting to the sites anonymously through the Tor network. Participants also requested a chapter on how to remove hidden information, known as metadata, from files – particularly photographs, which can often include sensitive information such as GPS locations inside them. This chapter is accompanied by a hands-on, step-by-step guide for an image metadata removal software.

As an alternative to using commercial, heavily surveilled social networking sites for organising and collaborating, we also wrote a hands-on guide for the use of RiseUp.net's "Crabgrass" online collaboration platform which – while not necessarily perfect in every situation – offers activists an opportunity to remove their sensitive work-related collaborations from the servers of the likes of Facebook and Google.

As mentioned above, we hope that this initial set will be expanded upon in the future, in accordance with the community's needs. Moreover, in the coming months and years we hope to make a number of similar *Security in*

Context materials for other communities at risk: among those currently being sketched is a guide which will look at digital security in the context of women HRDs (WHRDs), which may explore the role played by ICTs in facilitating acts of violence against women; and the specific dangers faced by WHRDs in the context of their work and their implications for their use of ICTs in that context.

Input and feedback from the human rights community is essential in order for us to continue empowering HRDs to be defend themselves and challenge injustice in the face of ever-evolving threats.

Endnotes

1. See http://www.elkhabar.com/ar/nas/334385.html (Arabic, accessed on 24 July 2013).

References

Amaya-Akermann, A. 2012. "Tunisia's GayDay Magazine Hacked." *Leo's Passagen*. Available at <http://passagenlevant.blogspot.de/2012/03/tunisias-gayday-magazine-hacked.html>.

Tactical Technology Collective. 2013. *Security in Context: Tools and Tactics for the Arabic-speaking LGBT Community*. Available at <https://securityinabox.org/sbox/pdfs/SecurityinContext_en.pdf>.