# GLOBAL INFORMATION SOCIETY WATCH 2013

Women's rights, gender and ICTs

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

# Global Information Society Watch

## 2013

APC Hivos

**Steering committee**
Anriette Esterhuysen (APC)
Loe Schout (Hivos)

**Coordinating committee**
Janine Moolman (APC)
Monique Doppert (Hivos)
Valeria Betancourt (APC)
Mallory Knodel (APC)

**Project coordinator**
Valeria Betancourt

**Editor**
Alan Finlay

**Assistant editor**
Lori Nordstrom

**Publication production**
Mallory Knodel

**Proofreading**
Valerie Dee
Lori Nordstrom

**Graphic design**
Monocromo
info@monocromo.com.uy
Phone: +598 2400 1685

**Cover illustration**
Matías Bervejillo

**Financial support provided by**
Humanist Institute for Cooperation with Developing Countries (Hivos)
Ministry of Foreign Affairs of the Netherlands Funding Leadership and Opportunities for Women (FLOW)


*Global Information Society Watch*
Published by APC and Hivos
2013



ISSN: 2225-4625
ISBN: 978-92-95102-06-4
APC-201310-CIPP-R-EN-DIGITAL-197

# Digital security online

**Mary Lawlor**
Front Line Defenders
www.frontlinedefenders.org

## Taking back control...

For human rights defender Satang Nabaneh, social media and new technology have been a fast, effective way for her to reach out to other young women in The Gambia. It is what makes her different from the older generation of women's rights defenders in the small West African nation.

"Facebook is there, Twitter is there," she says, "all of those communication tools, and this is what young people are interested in, so I can actually relate to them and talk to them and they can see what I want them to, what I am working on."

Digital technology – from computers and tablets to mobile phones – is increasingly being recognised across the world as an important tool for the empowerment of women and women human rights defenders, lifelines through which they can share experiences, access information and mobilise for their rights.

This is one of the reasons why the United Nations is pressing countries to address the current digital security gap between men and women users of devices, because technology enables women to create a space where they can operate.

For many women rights defenders – just like their male counterparts – the reliance on digital technology has a darker side. It raises the spectre of being tracked and defamed, monitored and hacked. If women rights defenders are to make the most of the opportunities these new tools offer, they have to make sure they are also ready to counter these threats with a comprehensive digital security plan.

## The dangers of revealing too much

For small, cash-strapped organisations a couple of decades back, it was often a challenge to get word out. The internet seemed to change all that: a web page for a few dollars for your contact details, a Facebook page and a Twitter account to keep supporters up to date with what you are doing.

But spreading all these details around has its own dangers that human rights defenders have been forced to think about. Women human rights defenders are finding that once their personal details are in the public sphere, it is impossible to control who sees them.

Roma rights defender Agnes Daroczi was shocked to find her personal details, including her address, plastered all over the internet on neo-Nazi websites, alongside racist incitement to violence against her. She is planning to build a larger fence around her home to protect herself from physical attack, but are there online security measures she could also be adopting?

In Ukraine, lesbian, gay, bisexual and transgender (LGBT) rights defender Olena Shevchenko has decided that it is time for her and her colleagues at Insight Public Organisation to restrict information about the organisation in the public domain, following a flood of threatening letters from right-wing and religious activists, emboldened by anti-LGBT political rhetoric.

They had moved from their old premises, but found the same pattern of threats following them. After three moves in the last year and the installation of CCTV and security equipment in their new offices, the staff finally decided that they would have to limit the information they put on the internet. They now keep their office location secret and rely on word-of-mouth, a simple way to limit risk.

## Sheltering from state surveillance

If an organisation is at risk from attacks by other groups in society, there are simple steps that can be taken to protect workers, as shown by Insight Public Organisation. But in some parts of the world, human rights defenders are less threatened by ideological gangs, and more by the very institution that is supposed to protect them: the government.

Governments have been quick to latch onto the internet, computers and mobile phones, as great tools for hunting their citizens. By hacking emails, eavesdropping on phone calls, or tracking people through GPS, it is easier than ever before for governments to know where you are, who you are with, and what you are saying.

Confronted with mighty state apparatus, it is tempting for human rights defenders to cross their fingers, put their heads down, and press on with their work. But you do not have to rely on luck to ensure safety.

In Europe's last dictatorship, Belarus, Tatsiana Reviaka knows the government watches her. With her colleagues at the Human Rights Centre Viasna in Minsk, she has been helping political prisoners and their families in Belarus for the last 15 years, since one of the first brutal crackdowns by the Alexander Lukashenko government back in the spring of 1996.

She is on the government's radar, recalling an incident last year when a KGB officer phoned her and told her to come to the agency's office. She asked for an official letter, setting out why they wanted to question her. He said it was on its way. He knew exactly where she was.

Because Reviaka has realised this, she makes sure to take certain measures to try to limit what the government can hear. She is careful about what she says over the phone, saving sensitive conversations for face-to-face meetings. She will leave her phone at home if she is going to a secret meeting. These measures are important not only for her own safety, but also for the safety of those she is trying to help.

As the recent scandal over the US National Security Agency's vast spying programme has shown, it would be wrong to assume that this is just a problem in authoritarian regimes. In 2011, indigenous rights defender Cindy Blackstock from Canada got hold of records showing that the Canadian government had been systematically monitoring her professional life, and her personal online activity, to try to get information to use against her in a court case she had filed.

## With great data comes great responsibility

For many human rights organisations, a vital part of their work is documenting abuses to make sure that when the time arises to hold people accountable for terrible crimes, there is the evidence to back up accusations.

In Mali, Fatimata Toure and her organisation GREFFA have played a key role in documenting the use of rape as a weapon of war in the northern region of Gao, where young men trained in the Libya conflict have been responsible for hundreds of sexual attacks against girls and women. Women have been raped, forced into marriage – at times to several men – flogged in public and beaten.

GREFFA's report is the only documentation of sexual violence and rape by armed groups in Mali and, on the basis of their work, the government of Mali has started a case against these rebel groups at the International Criminal Court.

Because their documentation is so important for the court case, GREFFA employees are vulnerable to attacks from groups implicated in the report. The rebels know who they are and have threatened workers at the organisation, making their work more difficult and dangerous. Their office has been ransacked and human rights defenders working there have received serious death threats.

For organisations like GREFFA, it is vital to know how to keep all the data they have collected safe, to protect not only their employees but all those who have been brave enough to step forward and share their harrowing stories.

This includes not only making sure that an office is secure so that hardware cannot be easily stolen, but also making sure that computers are secure as well, so that nobody can access the data. But how do you do this?

This can include something as simple as setting a password for the computer, not your mother's maiden name, or your place of birth, but a hard-to-crack combination of upper case, lower case and digits. The next step is to use a unique password for each account, so that if one is compromised then someone will not be able to maliciously gain access to all of your digital assets. Even if the files on your computer are safe, your electronic communications across the internet can still be intercepted. To protect information you send over the internet, it can be encrypted to hide its contents from anyone trying to monitor it. However, in some countries, even to use encryption software is a crime.

While there are many options for encryption and other security measures, it is important to pay attention to which software you use. It might seem like a good idea to turn to programmes made by Microsoft or Apple, but do not be fooled by the price tag. Open source software – which is software not provided by a big-name company, but instead honed by hordes of enthusiastic, freelance developers – is far more secure. Because the code is available to all, and not a trade secret of a giant company, any weaknesses in the encryption can be spotted and exposed by the global community of digital security experts. There has been recent concern that weaknesses have been purposefully built into some proprietary software at the demands of security agencies, so that they would have a "back door" into what were otherwise considered to be secure systems. Open source software is a more reliable way of ensuring that encryption works as it is supposed to.

## Conclusion

As Daroczi, Shevchenko, Reviaka, Blackstock and Toure all know, it is impossible to talk today about personal security without talking about digital security, which is why there was a whole day dedicated to digital security training at this year's Front Line Defenders Dublin Platform, one of the largest gatherings of human rights defenders in the world, held on 9-11 October.

The training provided by Front Line Defenders is based on our manual *Security in-a-box*,[1] and covers everything from secure passwords to protecting your email to mobile and social media security.

Digital security can be intimidating, and is often seen as the reserve of male computer boffins and techie types. But around the world, women rights defenders are becoming more confident about securing their networks and communications, safe in the knowledge that by using technology to press for their rights, they are not losing control, but taking it back. ■

1 Available online at: securityinabox.org