By Dia Kayyali

If you are documenting human rights abuses, technology can put powerful people's wrongdoings in the spotlight, or it can put you in jail. Whether you're facing down police to protect the environment, documenting systemic state violence, or communicating with activists in conflict areas, it's very important to think about issues of security–and not only for yourself. Everyone you communicate with or document could be at risk if you do not protect your video, photographs, and communications. Better security is just the right thing to do.

Digital security can seem overwhelming at first. Many people believe that they need special technical expertise to understand and mitigate threats to their security. That's an understandable misconception.

In fact, improving your digital security means figuring out what your own risks are and making a decision about what tools and techniques you're willing to learn to use to protect yourself and those around you.

Security trainers call this process risk assessment or threat modeling. It sounds complicated, but there are many organizations that have created resources online to help you with assessing and addressing your digital security needs. This blog post lists some of these guides and what they can teach you.

Assessing Your Risk

Your first step in better security is threat modeling or risk assessment. This requires asking yourself the following five questions. Consider taking out pen and paper and brainstorming, and consider discussing these questions along with the people you work closely with, since security is a collective effort:

- What do I need to protect?
- Who do I need to protect it from?
- How much do they want that information, and how easy is it for them to get it?
- What happens if they do get it?
- What am I willing to do to stop that from happening?

What do you need to protect?

Let's look at these questions in more detail using one specific example. Perhaps you filmed a police officer beating a protester on your phone in a place where the police aren't afraid to retaliate against perceived threats. If you're documenting human rights abuses, you need to protect the material you create.

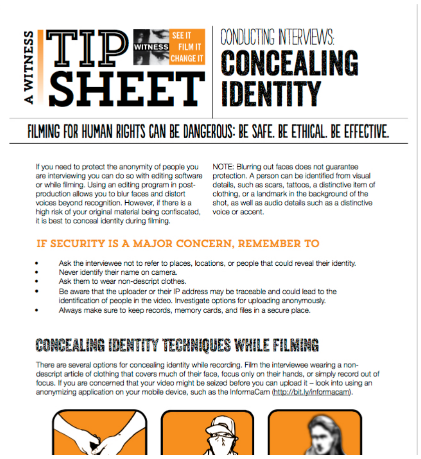
You need to protect the data you gathered from falling into the wrong hands. You may need to protect the identity of the protester as well. And you may need to hide the fact that you filmed it in the first place, for your own safety. Of course, you would need to protect all of this from the police. But perhaps you also need to hide it from, for example, your place of employment because you could get fired for your activism. Remember, this is only one example of something that needs to be protected, and you have to think very carefully about your own situation.

Once you have figured out what you need to protect and from who, next you think about what the actual risk is. Perhaps in your case, you know that the police in your area regularly take away people's cell phones, and they are very angry about being filmed. You don't know what technology they have, but you suspect they can figure out your location from your cell phone.

Then, you have to think about the consequences if your security is compromised, and what you're willing to do to avoid them. For example, perhaps the consequence of the police getting your film is only that you can't make it public. But if they're angry about being filmed, perhaps the consequence is that you end up getting harassed and threatened by police. Perhaps the protester, who was badly beaten, is getting charged with assaulting a police officer and the charges don't get dropped because you lost your video. In some places, your life or the life of your subjects could even be at risk.

Lastly, using this information you decide what tools you are willing to adopt and practices you are willing to change to avoid this consequence. Weigh the difficulty of adopting tools against the consequences if you don't. For example, turning encryption on on your phone is an easy step that could make it much more difficult for police to get your data. And perhaps you are very concerned about the person you filmed and don't want their identity public–the risk of reprisal they face could be very great. In that case, you could consider downloading and using tools such as ObscuraCam or the YouTube Blur Tool to remove identifying parts of the video. It's a little bit more work than just turning on encryption, but it could save someone's life.

Learning how to protect yourself and others



A WITNESS TIP SHEET

WITNESS SEE IT FILM IT CHANGE IT

CONDUCTING INTERVIEWS: CONCEALING IDENTITY

FILMING FOR HUMAN RIGHTS CAN BE DANGEROUS: BE SAFE. BE ETHICAL. BE EFFECTIVE.

If you need to protect the anonymity of people you are interviewing you can do so with editing software or while filming. Using an editing program in post-production allows you to blur faces and distort voices beyond recognition. However, if there is a high risk of your original material being confiscated, it is best to conceal identity during filming.

NOTE: Blurring out faces does not guarantee protection. A person can be identified from visual details, such as scars, tattoos, a distinctive item of clothing, or a landmark in the background of the shot, as well as audio details such as a distinctive voice or accent.

IF SECURITY IS A MAJOR CONCERN, REMEMBER TO

- Ask the interviewee not to refer to places, locations, or people that could reveal their identity.
- Never identify their name on camera.
- Ask them to wear non-descript clothes.
- Be aware that the uploader or their IP address may be traceable and could lead to the identification of people in the video. Investigate options for uploading anonymously.
- Always make sure to keep records, memory cards, and files in a secure place.

CONCEALING IDENTITY TECHNIQUES WHILE FILMING

There are several options for concealing identity while recording. Film the interviewee wearing a non-descript article of clothing that covers much of their face, focus only on their hands, or simply record out of focus. If you are concerned that your video might be seized before you can upload it – look into using an anonymizing application on your mobile device, such as the InformaCam (http://bit.ly/informacam).

Concealing Identity in Interviews

The WITNESS Library offers a wide variety of resources in over 15 languages, many of which include information about protecting yourself and those you film.

Two of the most comprehensive online guides are the Electronic Frontier Foundation's "Surveillance Self-Defense" (SSD) and Tactical Tech and Frontline Defender's "Security-in-a-Box." Both sites indicate when they were last updated, which is important since digital security resources can get outdated quickly.

SSD is available in English, French, Spanish, Russian, Turkish, Vietnamese, Portuguese, Thai, Arabic, Amharic, and Urdu. SSD has guides for specific situations (e.g. "things to consider when crossing the US border"), detailed tutorials on how to use specific tools, and lists of suggested tools for specific people, such as journalists or LGBTQ youth.

Security-in-a-Box is available in fifteen languages, and also has a comprehensive list of tools and tactics, as well as a section that focuses on specific communities, such as the LGBTI community in Middle East and North Africa.

Other helpful resources include:

- Tactical Tech's "Zen and the art of making tech work for you" guide, which is focused on "women and trans activists, human rights defenders and technologists," and has some unique resources, such as "creating and managing identities online." It's not yet complete, but still very helpful. Available in English and Spanish.

- The Rapid Response Network's Digital First Aid Kit, which "aims to provide preliminary support for people facing the most common types of digital threats." The kit is especially helpful when you have already been compromised, since it has information such as what to do if your devices have been seized.

- The Crash Override Network provides cybersecurity resources for people who are targeted for online abuse, including a Doxing Prevention Guide (doxing is the practice of making information like your phone number, legal name, and home address public). Their guides have some US specific information, but they have a lot of information useful for anyone.

- Hollaback! has Social Media Guides for Twitter, Facebook, Tumblr, Youtube, and Reddit to enable you to better navigate using these platforms safely.

- The Free Software Foundation's "Email Self-defense" guide, available in fifteen languages, is a great resource if you have decided you need to start protecting your email with "PGP" (Pretty good privacy).

Being empowered with this knowledge is a service to anyone you organize with or care about – and to the fight for human rights.

> ***Dia Kayyali** is an independent consultant and writer focusing on censorship and surveillance. They fight for freedom of expression online, especially on social media platforms, advocate for anonymity and privacy with governmental bodies and companies, help activists and other vulnerable communities identify and defend against security threats, and fight against the rapid spread of street level surveillance technology. They have coordinated a variety of US campaigns to limit surveillance at the national and local level, most recently as an Activist at the Electronic Frontier Foundation. They served as a 2016 fellow at Coding Rights, a Brazilian digital rights organization, where they researched surveillance technology at the Olympics.*

Feature Image: Flickr – Jun, CC BY-SA 2.0

Archived in Video for Change and tagged digital security, safety, Technology.

Share this article: Facebook Twitter