THE JOURNALIST SURVIVAL GUIDE

ANANIMATEDVIDEOGUIDE

Lesson 2

How to protect your sources' identities?

Samir Kassir eyes

The decision to protect a source›s identity is one of the most serious decisions a journalist can make. In many cases they put their career, the well being of their family and even their lives in your hands. Before you make this decision, you must be as clear as possible with your source about what you can and cannot do to protect them.
Above all do not make promises you cannot keep.

[Establishing the terms]
Before conducting the interview, establish the rules under which the information you get will be reported.
Can you use their first name?
Can you identify their place of work or position within an organization?
Can you quote them directly?
As a journalist it is important that you reveal as much information about your source as possible to establish their, and your, credibility to your audience.
When negotiating these terms, try not to make too many suggestions, let the source think and decide for him or herself how much to give away about who they are.
Avoid saying you WILL keep their identity secret, because there may be circumstances where you are compelled to reveal it.
Instead say you will do EVERYTHING IN YOUR POWER to keep their identity secret, and then be specific about how you intend to do that.
As always, take careful notes during these discussions, and secure those notes. Use a single notebook for all of your reporting on the confidential source. Do NOT use that notebook for his or her contact information. If possible, commit their name to memory, and identify them in your notes by a number or a symbol.
Do not discuss the identity of your source or the information you have obtained with friends or family.

[First Contact]
The absolute best way to get information that cannot be traced is to have an in person conversation in a private place. Emails, texts and phone calls can be traced.
Bring a small compact camera capable of shooting video with you to the meeting, even if you intend to do a full interview later. It›s always possible that the source will only agree to speak with you once. Do not use a smart phone camera or anything that is online.
In many cases an in person interview is impossible and you will need to communicate electronically. You should familiarize yourself with the technology that exists to conceal your own identity.
Secure internet services such as TOR will mask your computer›s ip address.
Secure chatrooms and email services offer a degree of security. One popular method of chat encryption that can take advantage of Facebook's widespread use is Off-The-Record messaging through the Pidgin chat client for the PC. [http://pidgin.im/]

Similar services are available for MAC users with the Adium chat client with OTR, and a step-by-step guide forinstallation is offered byencrypteverything.ca.
There is an encrypted email service for Google's Gmail through a Google Chrome browser extension called SafeGmail.
But nothing is foolproof, and you should operate on the assumption that your online communications can be monitored, logged, and recorded. Wi-fi networks are notoriously insecure. And the very presence of safe mail or proxy internet software on your computer may be seen as suspicious.

[Filming Anonymous Sources]
If your source agrees to an on camera interview, there are several production techniques you can use to protect their identity.
One of the most commonly used techniques is blurring the face in edit after the interview is completed. Be careful if you do this, because your raw video files will of course reveal the person›s face.
Shooting ‹in shadow› is also not particularly secure. Facial recognition software can easily identify people by their profiles, or even the shape of their ears, and even if the face looks completely blacked out on your camera monitor there is a good chance the dark areas contain much more information than you think.
Another technique is using face scarves or masks to hide everything but the eyes, but eyes are unique to individuals, and your interview subject can easily be identified by their irises alone.
You may be able to cover your interview with shots of the subject that do not include the face. Be aware that clothing, hands, even gestures, can give away their identity as well.
One effective solution, if you have a camera operator, is to shoot back at yourself with the back of the subject›s head in the foreground. If they have a scarf or a hood then you can protect their identity and still maintain a visually interesting shot. Be aware of any reflections that might show their face.

[Securing Your Media]
You should always use a camera that has removable media and record onto that rather than the camera›s built in memory. Most modern cameras use SD cards. These are very useful for securing your media. Bring at least two with you to the interview.
As soon as your interview is shot, you should immediately remove the SD card and secure it. Replace the card with a fresh one, and once you are clear of your source shoot some new material- for example a street scene, or a marketplace. This way if you are stopped and your camera is confiscated, you will have a plausible explanation for what you were doing because the new media will be time and date stamped. If the SD card in the camera is blank, whoever confiscated it will be more suspicious.

[Editing Video Footage]
Video journalists who routinely deal with confidential sources will often keep two computers, one for general use and another that is never plugged into the internet. If you have two computers, use the offline one to import and edit your media. If you don›t have two computers, avoid being online while you›re working with the material.
Once your edit is complete, you may export the finished project, delete your source files and any proxy files created during the edit. The original SD card should be the only archive you need. If you need to transfer or upload your finished report via the internet, copy it onto a thumb drive and plug it into your online computer.
Depending on your circumstances, you may come up with systems of your own to protect the identity of confidential sources. The important things to remember are to be careful about what you promise, stick to those promises, and continuously educate yourself about all the technological changes that can both make your work more dangerous, and safer.

Produced by:
The SKeyes Center for Media and Cultural Freedom at the Samir Kassir Foundation

The content of the video was prepared with the pro bono assistance of:
The ICT team at the National Democratic Institute

Executive producer: **Maroun Sfeir**
Storyboard creation and animation: **kook creative studio**

Video Consultant: **Andrew Codd**
Translation: **Nour El-Assaad**
Voice over - Arabic: **Rima Khaddaj**
Voice over - English: **Andrew Codd**
Sound recording: **Creative Impact**
Music: **"Mining by Moonlight" by Kevin MacLeod**

This project has been made possible thanks to the support of the **National Endowment for Democracy**.