Section 2: General safety considerations in choosing technology for storytelling and sharing your stories

Unpacks the general safety and security considerations in digital storytelling.

Introduction

The general arc of digital storytelling is to gather photos and videos, record the narration, edit the visual and audio elements together, and then share the completes digital stories with other people. In thinking about safety and digital storytelling, storytellers are encouraged to:

Thinking about safety before beginning

When it comes to safety, there are two main considerations a storyteller should think about before production begins:

Imagining the impact of the story. The storyteller has to try to foresee how the story will affect whoever sees it. In this way, they can anticipate negative responses to their story, as well as make plans to avoid potential threats from those who are negatively affected by their story.

The Impact Field Guide has a guide to exploring a story environment for documentary films. In it, themes are categorised into four types:

FRESH: an unknown issue to your target audience and little or weak opposition.
FAMILIAR: a known issue that still has little or weak opposition.
HIDDEN: an unknown issue (to your target audience) but with strong and organised oppositional forces may require your film to prove the case - to INVESTIGATE.
ENTRENCHED: a known issue (and so possible fatigue from target audience) with strong opposition to your story and campaign - often need to offer no more new facts or assertions

It is a good idea to have storytellers think about where their stories fall into these five types, and then start thinking about what does that mean in terms of their and their story´s safety.

Some questions for storytellers to ask themselves:

- What are the positive consequences of my story? What are the negative consequences?
- Will my story hurt someone or a group of people? In what way?
- How will I feel about telling my story? Will it affect me and in what way?
- Do I have someone to speak to if telling my story makes me re-live difficult events?
- Will my story put the people in it at risk? How so?
- What can the people who are negatively impacted by story do to express their opinions? Good to think about this from what they can do to the storyteller, the people in the story, and the story itself.

Sharing of the story: Location and people. Next, based on the previous considerations, the storyteller then can think about who they want to share their story to, and how.

Generally, there are two ways that a digital story is distributed and shared. The most usual way to share digital stories is by uploading them on a commercial platform (Facebook, Twitter, YouTube). Another way to distribute digital stories is through external storage devices (DVDs, USB sticks, external hard drives).

Safety considerations in uploading digital stories on commercial platforms

 The two main safety issues in sharing digital stories on commercial platforms are: the lack of control over the content and its ownership; and the lack of control over how the audience will react.

This is further explored in Section 3: Safety and Online Videos

Safety considerations in sharing via physical devices

One of the biggest issues in sharing stories via physical devices is the potential for the device to be corrupted with either malware or just reach the limit of its capacity to function. It is important therefore to have multiple copies of the content being shared, and a main back-up of the final digital story.

Safety considerations in screening your digital story

Face-to-Face Screening

If the storyteller decides to hold a face-to-face screening of their digital story, the first area of decision-making is about how private or public they want the screening to be. In order to make that decision, storytellers need to think about the following:

- What is the goal of screening this digital story? Is it to raise awareness of an issue? Is it to share personal experiences?
- Is the story going to be offensive to the viewers? Does it cover issues that people will reject because it challenges what they know or believe in?
- Will the story trigger memories in the viewers that might be difficult for them? Do you have support for these viewers from a self-care and psycho-social perspective?
- If the story will then challenge its viewers, has the storyteller taken sufficient steps to protect the people in their story to make them less identifiable and therefore, safe from repercussions?
- What can the storyteller do to prepare for possible negative, adverse reaction from the audience?

If the storyteller feels that their stories are more controversial, will put people at risk, and / or put they themselves at risk, then they can consider doing a private screening among trusted communities instead of a public one, and to be doubly sure, have a pre-registration list vetted by people whom you trust.

The next level to think about in doing face-to-to-face screenings (both private ones and public ones) is who does the storyteller want to share their stories with. In making decisions about this, the storyteller needs to reflect on a few questions:

- Who is this story for?
- Who is this story not for?
- How can I prepare the viewers of my story in managing how they will react to it?
- What can I do to prepare if sharing my story with someone offends or hurts them? What can I do to manage my own expectations about sharing my story?
- If the audience negatively reacts to my story, how can I prepare for that?
- If the audience shows minimal reactions to my story (no one loves it or think it's a well-told story), how will I react? Will that hurt me?
- Do I need to be there as the storyteller? What risks does my presence bring me?

Learning objectives

This section aims to unpack the general safety and security considerations in digital storytelling, and to highlight strategies, tactics and decision-making points in the use of technology in the digital storytelling process.

This session will tackle the safety of the storyteller as well those in their stories, and the safety of the stories they are telling in terms of their potential impact on audiences, interested parties and authorities.

By the end of this section, the storyteller will:

- Understand why it is important to imagine the possible impact of their stories before they start making their stories
- Gain an understanding of the different safety considerations in making and sharing digital stories
- Learn about some basics of digital security as it applies to digital storytelling

It is recommended that you read the previous section on Digital Identifiability to understand the larger issues around safety and storytelling.

Safety in content gathering and production

Collection of images and videos

A typical digital story contains images and audio narration, edited together to tell a personal story. Sometimes, the storyteller will have the means to take photos, record videos and audio. Sometimes, the storyteller will have to choose to use existing photos, video and footage, and audio found online.

Protecting digital stories by using free to use content

Copyright – the right to use images, audio and other creative content made by others – is an important safety consideration in selecting which images, audio or video to use for a digital story. This is especially true if the storyteller wants to make their digital stories publicly available, and if the stories will cover topics and themes that people on the internet would object to. Copyright violations are often used as an excuse to take down content on the internet. All commercial platforms have guidelines and policies against the use of copyrighted material.

There are some strategies and tactics to make sure that storytellers are using material for their stories that do not violate copyright laws.

For images that are free to use and adapt:

Do an advanced Google Image Search

safety-content-gathering-1.jpg
Image you could not type unknown

Then select the option to only search for ¨free to use and modify commercially¨.

safety-content-gathering-2.jpg
Image you could not type unknown

You can also use the following repositories of content that have Creative Commons licenses. Creative Commons licences recognize the ownership of the content creator and is an alternative to the current accepted practices of Intellectual Property Rights, where ownership tends to lie largely with large companies. It allows the original content creator to decide who can use the content, and how it can be used (non-commercial or commercial) or modified. The most unique features of Creative Commons licences is how it ensures attribution to the original content creator and that the same practice of copyright terms and conditions must be honoured and extended to others by those who use and/or modify the original content. To learn more about Creative Commons, see https://creativecommons.org/about/.

> **Creative Commons licences** recognize the ownership of the content creator and is an alternative to the current accepted practices of Intellectual Property Rights, where ownership tends to lie largely with large companies. It allows the original content creator to decide who can use the content, and how it can be used (non-commercial or commercial) or modified. The most unique features of Creative Commons licences is how it ensures attribution to the original content creator and that the same practice of copyright terms and conditions must be honoured and extended to others by those who use and/or modify the original content.

- Creative Commons Search: https://search.creativecommons.org/
- Wikimedia Commons: https://commons.wikimedia.org/wiki/Main_Page
- Internet Archive: https://archive.org/
- The Public Domain Project https://www.pond5.com/free. Here you can download historical content that are free.
- Pexels Creative Commons section: https://www.pexels.com/creative-commons-images/
- Flickr´s Creative Commons section: https://www.flickr.com/creativecommons/

Free audio sites:

- https://musopen.org/
- http://ccmixter.org/
- https://freemusicarchive.org/

While these sites generally have content that is free to use, edit and adapt, e. Each material to be used has to be checked for the specifics of their copyright permissions. Some of the materials are free to use and edit / adapt but requires crediting the original creator of the content. Some do not.

It is also recommended that storyteller adds credits at the end of their story to attribute the content that they used in telling their stories.

Protecting storage devices

It is important to protect the storage devices the storyteller will be using throughout the process. Devices should be password protected, in order to secure the files within it.

Password protect computers with a more than twelve character password.

For mobile phones, there are different ways to lock the screen.

- **PIN**: four to six number combination
- **Pattern Lock**: Create a pattern with dots on your screen
- **Password**: any combination of numbers, letters and special characters
- **Biometric locks**: fingerprint, face recognition or retinal scanning to unlock your phone

Out of the options, having a secure password (more than twelve alphanumeric characters) is the safest.

- Computers and mobiles phones can also be encrypted. This provides a much more secure way to protect devices.
- According to Apple, all their computers and iPhones are encrypted by default.
- Windows machines have Bit Defender that is available on Windows 8 to later versions.
- For Android, the user has to encrypt their phones by going through the Settings.

As a digital storytelling trainer, it is good to encourage the storytellers you will be working with to do this before the training.

Backing-up content

It is a good idea to create copies of collected and created content and materials for stories in a separate device from the main working device at different points in the storymaking process. This protects the storyteller from any unforeseen and unpreventable issues like device failure or loss of files.

For example, having a USB drive where the storyteller can create a back-up of the directories of their story content. Or having an external hard disk. Depending on the sensitivity of the story as well as the internet access available to the storyteller, they can also consider backing up to cloud storage services like Google Drive and iCloud.

It is important for storytellers to determine when they are backing up their materials. Depending on the time that a storyteller is collecting content for their digital story and producing it, it is usually recommended to back up material when the collection or creation phase is over – before they work on editing or manipulating their content. Then once an edit of a material is done, there should be a back up of that. Then a back up of the final story. Do be mindful that sometimes you may realise that you do not have the content you need to create the final digital story, but do not forget to back up after all additional material is collected or created.