What data is best kept private and why?

Hi, My name is Catherine Gicheru.

I am an ICFJ Knight Fellow and the Director of the African Women Journalism Project, an initiative that works to support, train and mentor women journalists in Africa in covering underreported communities and issues.

Last week Arzu Geybulla took you through what online harassment looks like, how to look after your emotional wellbeing and shared resources for psychosocial support.

This week, I will be telling you about online privacy...what is it and why it's important.

You will learn what information you should or shouldn't share online and how the information you share online can make you vulnerable to online attacks and targeted by bad actors.

We shall also share some practical tips on what you can do to protect your privacy online.

This week in addition to the videos there will be additional reading materials. I encourage you all to participate in the discussions that we shall be having throughout the week.

Thank you for joining me and I look forward to working with you to better understand Online Privacy.

I would like to start this second module by quickly talking about how the internet works so that you can better understand what data you share knowingly or unknowingly, and why some information should be kept private.

There's a lot of technical explanations of how the internet works, but the simplest explanation is this, the Internet is a vast, sprawling collection of networks that connect to each other.

In fact, the word "Internet" comes from this concept: interconnected networks.

Computers, phones and other devices connect to the internet via wires, cables, radio waves and other types of networking infrastructure (like cellphone towers).

So where does data come in? All information sent over the internet from one device to another is sent as data. When data gets sent over the internet it is first broken into smaller segments called “Packets”.

Each packet contains both data and information about that data. This will include where the data is coming from, what type of data, what time it was sent and where the data is going.

One other term that is important when looking at how the internet works is protocols.

One of the fundamental problems that had to be solved when the basic concepts for the internet were being developed was how to connect 2 devices, which might use different hardware and run different software.

A good example of this is when someone posts a blog on their laptop but another person wants to view it on their phone.

Or you are working with an Apple laptop which runs on one software and you are emailing someone on a Windows machine which runs on another.

This problem was solved with standardizing protocols. There are protocols for sending packets to devices on the same network for sending packets from network to network (IP - Internet Protocol) as well as others including HTTP (HyperText Transfer Protocol) for formatting data for websites and applications as well as encryption protocols.

The data packets used by apps, websites and businesses can be used to collect a large amount of information about you, what device you use, your location, what your interests are, personal health information as well as your financial information.

I have shared a video that will better explain to you how the internet works in the additional course materials.
Now that we know how the internet works the question we must then ask ourselves is, who has access to our data and what does this mean for our privacy? What is Online Privacy?

Online privacy also referred to as internet privacy or digital privacy refers to how much of your personal, financial and browsing information remains private when you are online.

When it comes to online privacy, there are two types of information that you should be concerned about.
Personal Information. This is information that can confirm your identity, can be used to locate you and contact you. Some examples of personal information include your IP address, your physical address or phone number, your email addresses.

Sensitive information. This would include very private data like medical records but may also be information you may not be ready to share publicly such as your sexual orientation, political views and your home life.

Online harassers are interested in your personal data.

They can use this information in well-organised harassment campaigns targeting you and your family.

They may also use the information to impersonate you online or to try and access your finances.

Online abusers may be working in groups to look for your personal data and share it online.

It might seem impossible to control what information is available about you on the Internet especially if you need to have an online presence as a journalist.

But you can take practical steps to protect your data from individuals, governments and corporations. But first, you must understand what data is important to protect and why.

The most important data to protect online is Personal Data.

This is information that can be used to confirm your identity, locate you, or contact you.

It is the type of information that companies often ask you to verify in order to give you access to your accounts.

In the wrong hands, this information can be used to impersonate, threaten, and harass you and your family or even your sources.

Your online security is linked directly to your physical security.

So whatever tool or platform you are using, be it a mobile phone, the internet from a computer or social media, always check your privacy settings and the security of your equipment.

Some personal identifiable information can also be found in public databases such as voters' registers.

Other information about you can be found on your social media accounts, the accounts of your family and friends and even your news sources.

This information when grouped together can create a robust profile of who you are, where you are, what you are doing, the circles you move in, your habit, your likes, dislikes and much more.

We all use search engines every day. They are usually our first port of call when researching information for a story.

Many of the popular search engines deploy user tracking techniques which collect a lot of information about what you are looking for, the sites you visit, your location when making the search, the device you are using, your location when you were making the search as well as what devices you are on.

You have to be especially vigilant of your search engines that control access to most of your information.

Additionally, if the search engine provider also makes the browser (Google Chrome, Firefox, Internet Explorer, etc.), they have your browsing history regardless of whether you searched for the site.

Search engines can and do collect your

1. Search history
2. Cookies
3. IP address
4. click-through- history

The collection of this data is controversial because search engines often claim to collect a user's data in order to tailor better results to a specific user, they can, however, and often do compromise its users' privacy by selling their data to advertisers for profit.

Collectively this information can be used for "profiling" you.
Let's look closely at one of the bits of information that search engines collect, Cookies.

Cookies are code that tell a website the information on your browsing history. They are for the most part harmless but and can help the user remember

- logins
- identification
- preference settings
- ad settings
- language settings

Most websites because of various attempts to start protecting user privacy will ask you to accept or decline their use of cookies.

Cookies become a concern when 3rd party AD serving is involved. This is when a search engine allows advertisers access to their usage data to target users with products and services.

When you visit a site, your browser has assembled information from various sources that dictates the ads you see. You have, essentially, become a profile/persona, even if it's only seen by bots.

Sites and search engines use first-party cookies to track users who visit their pages, then use third-party cookies to follow you around the web once you leave their page.

This has been questioned by privacy advocacy groups, as companies like Google amass vast amounts of consumer data to deliver personalised ads based on browser history.

Search engines aren't the only place that we are vulnerable online as journalists. The apps we use in our everyday life to connect, travel, pay for things and share content also pose a threat to our online privacy.

A significant amount of personal information online is put there by journalists themselves or by their family and friends.

Journalists are often unaware of how much information is easily available about them and how this data can be used to harass and target them.

And when it comes to social media, the majority of these platforms are “free” since you pay nothing to use them. However, they aren’t really free because just like with websites, these platforms collect a lot of data based on what you share, what is shared about you, the things you like, the links you click on while on the platforms and even your IP address.

Journalists use social media channels to source stories, vet story ideas, sharing information and conduct research for stories about corrupt individuals and organisations.
These channels are susceptible to data breaches and manipulation. Bad actors can access private data from social media platforms and elsewhere and use it to manipulate opinions for the benefit of a few such as the Cambridge Analytica breach of the Facebook data.`

Do not use the personal information that you used to set up your social media profile to formulate a password. These details put you at risk of hacking due to the predictability of your passwords especially when your personal information is easy to find online.

And when interacting online, make sure you do not share this information with just anyone whether it is in a chat, a photo or a video.

Some apps will also track your browsing habits even if you do not allow your browser or websites to store cookies.

User Privacy agreements that you agree to when you sign up to most platforms give them permission to track and save information on your activity even when you aren’t on the platform.

Do you have a Facebook, Twitter or Instagram account? What info do you share there? Do you share pictures of your family? Do you add locations to your pictures or posts? Are your accounts private or public?

What data and permissions have you accepted by clicking ‘agree’ on the user agreements for the platforms you are on.

Asking yourself questions like these is the first step to securing your online privacy. Stay vigilant about what details you are being asked to share and why they are needed.

On your privacy settings, keep personal identification details to yourself and secure how your other information appears publicly.

Remember, you can decide what personal information you want to reveal, when, why and to whom. You can control what you share.

In the next lesson, we will be looking at how to better protect yourself online.