GUIDEBOOK

on

Data Protection & Privacy in Kenya

from a Gender Perspective

KICTANet Policy Brief
December 2022

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

DIGITAL TRANSFORMATION CENTER KENYA

Co-funded by EU

KICTANet
The Power of Communities
www.kictanet.or.ke

Imprint

Published by:
Kenya ICT Action Network (KICTANet)
Email: info@kictanet.or.ke
Web: www.kictanet.or.ke
Twitter: @kictanet

Programme:
KICTANet Women Strengthening in ICTs

Project title:
Strengthening Women's Safety Online in Kenya

Supported by:
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Authors:
Mercy Mutindi & Paul Kithinji

Editor:
Victor Kapiyo

Editorial Team:
Grace Githaiga, Liz Orembo and Angela Minayo

Design & Layout:
Stanley K. Murage (stanmuus@gmail.com, Cell:+254 720316292)

Photo (Title):
young-african-american-woman-is-happy-with-laptop-computer.jpg - source, https://www.freepik.com/

Location:
Nairobi 2022

Year of publication:
December, 2022

Table of Contents

Glossary of Terms

Anonymization - the removal of personal identifiers from personal data so that the identity of the data subject is hidden.

Data Breach - a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an unauthorised person.

Data Controller - a natural or legal person, public authority, agency or other body which alone or jointly with others determines the purpose and means of processing of personal data; [i]

Data Processor - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller; [ii]

Data Subject - an identified or identifiable natural person who is the subject of personal data identified, directly or indirectly, via identifiers such as a name, an Identity card number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural or social identity. [iii]

Processing of personal data - any activity undertaken on personal data, such as the collection, storage, use, transfer and disclosure of personal data. All activities involving personal data, from the planning of processing to the erasure of personal data, constitute the processing of personal data. [iv]

Respondent - a party against whom a petition is filed, especially a data processor or controller who processes personal data. In this case, the anyone who while processing Zara's data breaches her rights or principles of the DPA 2019

(*)- Where you see * In the text, it means names and facts are fictitious and created to reflect realistic scenarios for purposes of illustration and teaching. The story, names, characters, and incidents portrayed in this work are fictitious. No identification with actual persons (juridical, living or deceased), places, buildings, and products is intended or should be inferred.

Abbreviations

COVID	-	Coronavirus Disease
DPA	-	Data Protection Act 2019
FAQ	-	Frequently Asked Question
GPS	-	Global Positioning System
iOS	-	iPhone Operating System
IT	-	Information Technology
IAPP	-	The International Association of Privacy Professionals
ISP	-	Internet Service Provider
ODPC	-	Office of the Data Protection Commissioner
OECD	-	Organisation for Economic Co-operation and Development
UDHR	-	Universal Declaration of Human Rights
URL	-	Uniform Resource Locator
ICCPR	-	International Covenant on Civil and Political Rights
OECD	-	Organization for Economic Co-operation and Development

Executive Summary

In 2019, Kenya enacted the Data Protection Act 2019 (DPA), to operationalize the right to privacy in Kenya.

Since then, Kenya has established the Office of the Data Protection Commissioner whose mandate is to enforce data protection rights and principles as envisioned in the DPA.

Despite this, there exists a gap in awareness and understanding of existing safeguards for data subjects and more so women under the law and privacy features on social media platforms.

This guidebook aims to raise awareness on data protection and privacy in Kenya from a gender perspective. It is divided into ten chapters: The first chapter gives an overview of the right to privacy and data protection and its relation to gender.

Chapter two provides a hypothetical case study from which we can highlight and data protection rights and principles violations that may be encountered by women in their day to day lives.

Chapter three lays out the legal and policy framework in Kenya post the Constitution 2010, with emphasis on the objective of legal statute, regulations, policy and guidance notes from the ODPC.

Chapter four and five go into detail on the principles and rights governing data processing in Kenya as provided for by the DPA. They seek to inform the reader on the principles and rights and why they matter.

Subsequently, Chapter six speaks to data and data processing exempted from the application of the DPA.

This chapter provides for adequate examples where such specific cases may arise and their justifications accordingly.

Chapter seven then provides for legal remedies for data protection breaches by controllers and processors. Here we list the possible outcomes resulting from enforcement measures undertaken.

Chapter eight provides for quasi-judicial redress and reporting mechanisms on social media platforms.

These platforms include; Facebook, Instagram, WhatsApp and Twitter. Finally, Chapter and nine and ten provides for privacy tips geared to protection your personal data online.

However, it is important to note that the guidebook offers additional reading material that proves beneficial to the reader seeking to learn more of data protection from a gender perspective.

How to Use this Guidebook

This guidebook was written to provide a practical understanding of life situations where privacy issues exist as well as how Kenya's Data Protection Act, 2019 may apply in real life.

We use a case study of Zara, a representation of a typical modern woman to explain the principles of data protection, the rights under the privacy law as well as the practical ways to file complaints, report breaches as well as take proactive action to protect ourselves online.

We recommend that you read through the glossary before proceeding to the rest of the chapters to help you gain understanding of key terms. As you read through the chapters, use this guidebook to reflect on your own privacy journey and audit your privacy practices as an individual in real life as well as across the various social media platforms including WhatsApp, Instagram, Twitter and Facebook.

Read, reflect and attempt the exercises provided in different chapters to assess your understanding of how to protect your privacy and exercise your rights. You may also use the guidebook to facilitate discussions about everyday privacy concerns and available social media privacy controls.

We hope that the actions you take from reading through will help provide better privacy protections for your life and our nation.

1. Introduction:

What is Privacy and how does it relate with Data Protection?

a) Privacy

Privacy is a fundamental right, essential to protect and support our right to human dignity, autonomy and personal identity.

The concept of privacy regulates access to our bodies, households and property, as well as to our communications and information about us.

It enables us to create boundaries to protect ourselves from unwanted interference to our lives, identity and communication.

Globally, the UDHR 1948, Article 12 proclaims *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." This is reiterated by Article 17 of the ICCPR 1966. Article 31 of the Constitution of Kenya, 2010 provides for the right to privacy.* [v]

b) Data Protection

Data Protection is one of the elements of the right to privacy which focuses on protecting a subset of information known as personal data.

Personal data refers to any information relating to an identified or identifiable natural person known as a 'data subject'. [vi]

We can now uniquely identify individuals amidst sets of mass data and make decisions about people based on streams of data they do not know exist. [vii]

It is also possible for individuals, companies and governments to monitor all our communications, commercial transactions, locations and sites visited and more recently our religious and philosophical opinions.[viii] These instances of interference often lead to profiling, discrimination

and other forms of harm.
According to the data protection laws, processing personal data means any function or set of functions, either automated or manual in nature, which are performed on personal data or on sets of personal data.

These processes include collecting, recording, organizing or structuring personal data; storing, altering, retrieving, using or disclosing personal data by whatever means as well as combining personal data sets, applying restrictions, erasing or destroying personal data.

In essence processing of personal data refers to the entire range of activities undertaken throughout the life cycle of personal data from the point of collection to the point of its destruction. [ix]

The way we process personal data determines whether we enhance or infringe a person's right to privacy. The wise men say, "information is power." By processing personal information in line with data protection principles, we can protect ourselves and society against arbitrary and unlawful use of data.

Privacy is essential to who we are as human beings. As of August 2022, the world population stood at an estimated 7.96 million people, [x] of which 50.42% are male and 49.58% of those are female. [xi]

The United Nations Human Rights Council and the General Assembly have noted that "violations and abuses of the right to privacy in the digital age may affect all individuals, with aggravated effects on women and children as members of marginalized groups. This reality requires State action to develop and maintain gendered preventive measures and remedies for violations and abuses of the right to privacy." [xii]

Locally, as of January 2021, there were 21.75 million internet users in Kenya and the Internet penetration stood at 40%. [xiii] Of the 21.7 million, 11 million were social media users. [xiv] As of August 2022, Kenya's population is estimated at about 56.19 million [xv] with 49.69% being male and 50.31% female. [xvi]

According to the Organisation for Economic Co-operation and Development (OECD), women typically participate more than men in social networks (Facebook, Twitter etc.) and trends over time show that more women are now buying goods and services online and doing more e-banking than before. [xvii]

This guide looks at data protection and the right to privacy in Kenya from a gender perspective with some focus on effects as experienced by the female gender including on popular social media platforms.

The guide is useful for all genders as most of the laws and tips explored are written in gender-neutral perspective and the outlined platform controls can be used by either gender as well.

> ***"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."***

2. Zara's Story- Part of Our Story

The Data Protection Act (DPA) is the main law that governs the processing of personal data in Kenya.

All data controllers and processors (in both the private and public sector) are required to ensure that personal data is processed as required under the DPA.

To help us better understand the relevance of the Data Protection Act, we will use a case study of Zara* a Customer Service Manager working at Manufacturer One* in the industrial area, Kenya.

Zara has worked with her current employer for 9 years. She has been hoping to get a promotion and pay rise without any success over the last 6 years.

Despite this challenge, she is grateful to have had her job during the pandemic and post-pandemic. Though not happy with her current pay, Zara really appreciates her employer's efforts in caring for employees at Manufacture One, as seen through the keen interest her line managers have shown over the past 9 years.

They consistently check in on her professionally and personally. They are always keen to hear about her vacation experiences, her health and any symptoms of illness or diagnoses.

Additionally, they support her through family issues and her expression and exercise of religious beliefs. This is mostly done via Welcome Back Talks after any absences from work and informal talks with supervisors.

While grateful for her current job, Zara worries about financial stagnation in her career. Zara finally feels the economy is stable enough to job hunt and is open to new opportunities even

while she tries to set herself up for a promotion at Manufacture One. She recently saw an online advertisement for a Customer Service Director at a company called Airline One* and has been fantasizing about all the staff discounts she could get if she landed the job. She applied for the job in January and was shortlisted for interviews.

In February, Alfred*, a Human Resources assistant at Airline One called from the office landline to give Zara the good news and somewhat fell in love with Zara, her beautiful voice and warm persona on the phone.

After informing Zara on the date, time and location of her interview, Alfred took Zara's number from her CV and saved it on his personal mobile phone, he also went online and searched for Zara's social media accounts and sent her friend requests on Facebook, added her as a friend on Instagram and started following her on Twitter.

Alfred spoke to the receptionist at Airline One to inform him once Zara arrives for her interview since he wanted to meet her in person. On the day of Zara's interview, Alfred personally welcomed her, introduced himself, took a selfie with her then ushered her to her interview room.

After her interview Alfred messaged Zara on WhatsApp to inform her that she would have a telephone interview with him the next day.

Alfred called Zara from the office line (where all calls are recorded) and before talking about work asked her intruding and rather personal questions about herself namely; where she lives, her marital status, if she is dating, questions about men in her photos on Instagram, if she has kids due to the children he saw on one of her recent Facebook posts, what she thinks of pregnancy, how many children she wants to have, whether she knows how to cook, if she washes her own clothes, what she thinks about living in the village and living with her husband's relatives plus a bunch of other personal questions.

Zara was shocked and could not understand why any of this information was relevant and felt like Alfred was interviewing her for the position of a "village wife" without her consent or interest. Alfred eventually gave her feedback that she is qualified but above company budget and would therefore not be getting the job.

While grateful for the feedback, Zara was disgusted by Alfred's invasion of her privacy and immediately blocked him on WhatsApp hoping to never hear from him or Airline One again.

In May, Manufacture One identified a security breach at their main office, which resulted in employee personal data becoming available to the whole company for several hours.

Zara discovered that over the 9 years she had worked at Manufacture One, her line managers had been keeping comprehensive notes of all their welcome back and informal conversations on a database accessible to 50 members of the senior management team and that this database was used to monitor employees and determine career progression.

Manufacture One reported this breach to the Regulator via *https://www.odpc.go.ke/report-a-data-breach/* and for the first time in her life, Zara heard about the Office of the Data Protection Commissioner when they came to interview her and her colleagues.

The investigation involved an analysis of 60 Gigabytes of data, witness interviews, and a review of Manufacture One's policies.

She did not really understand the importance of this exercise until her employer was fined 2% of the annual turnover of the preceding year. As a result of this turn of events, Zara started following the Office of the Data Commissioner on Twitter, trying to understand data protection law.

Manufacture One apologized to affected staff and paid them considerable compensation. The Regulator described the compensation as an 'unprecedented acknowledgement of corporate responsibility'* after a data protection incident.

Manufacture One also appointed a data protection coordinator, improved its IT systems,

and provided data privacy training to all staff. It also issues monthly data protection updates and communicates whistle-blower protection better, which makes the company more transparent.

Manufacture One emphasized its commitment to data protection compliance and reassured its customers and employees that the company takes privacy and the protection of all personal data as top priority via press statement, "Manufacture One strictly adheres to laws and regulations stipulated by the relevant data protection authorities, as well as the company's own high standards."

One day, in August, Zara woke up to congratulatory messages on WhatsApp and Facebook. She was bewildered and thought that maybe she had landed a Director role somewhere.

However, she received a message from her best friend Annie* congratulating her "engagement". The message was accompanied by a flier screenshot from Facebook that read "Zara weds Alfred".

Zara could not believe what she read. She went on Facebook and found out that the flier had been created and published by Alfred using the photograph taken on the day of her interview.

Additionally, he was announcing how they would be getting married at a church in his home village in eight months. Alfred also posted his number for people to confirm attendance as well as send wedding contributions and gifts. All her friends on Facebook were looking forward to the wedding and were even sending M-PESA contributions for the event. Everyone was happy to see Zara finally tying the knot as they had concerns "she was getting old."

Zara called her sister who was a lawyer and explained the situation. After calming her down, Zara's sister helped Zara report Alfred to the Police as well as Report Airline One to the Office of the Data Commissioners.

Zara had to deal with the embarrassment and shame of informing everyone what had really happened as well as the fact that there was no wedding and anyone who had sent any M-PESA donation to Alfred had essentially been scammed.

Zara's story may sound a bit sensational to some, but it reflects the reality of various women particularly in this digital age. Key statistics indicate:

- As more employees work outside the office, more employers are using digital surveillance tools to monitor them. In one 2021 survey conducted by the International Association of Privacy Professionals (IAPP), 78 percent of employers reported monitoring their employees' performance and online activity. [xviii]

- Nearly 1 in 3 women and 1 in 6 men have experienced stalking victimization at some point in their lifetime.[xix] More than 80% of survivors reported the person stalking them was known to them in some way. [xx]

> ***Zara's story may sound a bit sensational to some, but it reflects the reality of various women particularly in this digital age.***

3. Policy and Legal Framework on Data Protection in Kenya

We have various laws and policies that support data protection in Kenya as highlighted below:

a). The Constitution of Kenya, 2010

Article 31 of Kenya's 2010 Constitution[xxi] provides for the right to privacy for every person. This right includes the right not to have your body, home or property searched, your possessions seized, or the information relating to your family or private affairs unnecessarily required or revealed or the privacy of your communications infringed upon by the state or any other person.[xxii] These provisions set a foundation for the Data Protection Act 2019.

b). The Data Protection Act, 2019

The Data Protection Act 2019 (DPA)[xxiii] was enacted by Parliament in November 2019.[xxiv] Its overall objective is to protect the privacy of data subjects, by providing for data subject rights' and by ensuring processing of personal data with the data subject in control of how their data is processed.

The DPA establishes the Office of the Data Protection Commissioner (ODPC) to oversee the enforcement of the data protection framework in the country.[xxv]

c). The Data Protection (General) Regulations, 2021

The Data Protection General Regulations[xxvi] provide statutory forms that allow data subjects to exercise each right in the DPA. The regulations also state the restrictions on the commercial use of personal data by data controllers and data processors.[xxvii]

For instance, commercial entities are not allowed to use personal data for commercial purposes without the consent of the data subject.

The regulations also lay out guidelines for notification of personal data breaches [xxviii] and cross-border data transfers.[xxix] However, these regulations also provide exemptions where personal data is processed for the purposes of ensuring national security. [xxx]

d). The Data Protection (Complaint Handling and Enforcement Procedure) Regulations, 2021

The Data Protection Complaint Handling and Enforcement Procedure Regulations 2021 [xxxi] facilitate a fair, just, expeditious, affordable and proportionate determination of complaints lodged with the ODPC.

The complaints are to be heard and determined without strict procedure.[xxxii] Thus allowing a complainant to file a complaint in a form the deem best.

The regulations prescribe the statutory forms for complaints, timelines, investigation, outcomes, penalties and appeal grounds and processes. In chapter 7 of this guide, we will learn how to lodge complaints at the ODPC.

e). The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021

Section 21 of the DPA obligates the Office of the Data Protection Commissioner to keep a register of data controllers and data processors. Therefore, the Data Protection Registration of Data Controllers and Data Processors Regulations [xxxiii] provide for the procedure for registration of data controllers and data processors as provided under section 18 of the DPA. Registration fees are outlined in the regulations and the application for registration is to be accompanied by the following documents;

a). A copy of the establishment documents;

b). Particulars of the data controllers or data processors including name and contact details;

c). Description of the purpose for which personal data is processed; and

d). A description of categories of personal data being processed.

f). ODPC Guidance Note on Processing Personal Data for Electoral Purposes

This guidance note[xxxiv] was developed to assist data controllers and data processors who are handling voters' personal data, including sensitive personal data, and the personal data of members of political parties to understand their obligations under the DPA.

It applies solely to the processing of personal data on voters (or potential voters) and the processing

> ***The Data Protection Complaint Handling and Enforcement Procedure Regulations 2021 facilitate a fair, just, expeditious, affordable and proportionate determination of complaints lodged with the ODPC***

of personal data for the purposes of the creation and maintenance of member registers.

It also clarifies the duty imposed on processors during the electioneering period and the rights of data subjects whose personal data is being processed.

g). ODPC Guidance Note on Consent

The guidance note[xxxv] was published to help data controllers and processors understand their duties under the DPA and appreciate their obligations as relates to obtaining consent.

h). ODPC Guidance Note on Registration of Data Controllers & Data Processors

This guidance note was published to help guide entities on how to register with the ODPC as required under the DPA. It provides a step-by-step guide on the registration processes via the online registration portal set up by the ODPC[xxxvi]

4. Key Data Protection Principles & Why They Matter

The DPA provides key principles to guide processing of personal data. All data controllers and processors (in both private and public sector) are required to ensure that personal data is managed in accordance with principles under the Act. To help us better understand how these principles apply, we will discuss them in the context of Zara's Story.

Zara did not know much about data protection law but the turn of events from her Airline One job application has left her feeling violated by Alfred and convinced that Airline One has unethical data practices as revealed by the conduct of their employee Alfred. The care and affection she thought she was receiving from her employer is also now in doubt in view of the recent data breach at work.

What Zara is wrestling with in this scenario is what the law calls a violation of the principles of data protection.

The Data Protection Act sets out key principles that govern how individuals and organizations can process personal data.

These principles include: informed consent, lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality (security); and accountability.

We look at each in more detail below.
These principles lie at the heart of data protection law and inform everything in it. They embody the spirit of the general data protection regime in Kenya and globally - and as such there are very limited exceptions.

Compliance with the spirit of these key principles is therefore fundamental for compliance with the law as well as the preservation of individual and corporate reputations.

Failure to comply with the principles leaves one open to substantial fines of up to five million Kenyan shillings or 2% of your total annual turnover per violation.

In Zara's case, most data protection principles were violated as explained below:

a). Informed consent, lawfulness, fairness and transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

For processing to be considered lawful and fair,[xxxvii] the processing must include; an appropriate legal basis or legitimate interests clearly connected to the specific purpose of processing[xxxviii], purpose specific processing,[xxxvix] being given the highest level of autonomy possible with respect to control one's personal data, granting of informed consent and a simplified means to withdraw consent.[xli]

In Zara's case, data was collected by Airline One for purposes of recruitment only and lack of sufficient internal controls resulted in Alfred using the data to stalk Zara and harass and bully her with personal questions not related to recruitment and engaging her past normal working hours.

Airline One did not provide a privacy notice to Zara explaining how they process her information as well as who to escalate to in case of any issues or queries.

Alfred also did not have Zara's consent to use her personal information to pursue his personal interests.

b). Purpose limitation

Personal data should only be collected and processed for specified, clear and lawful purposes and not used for incompatible purposes. [xlii]

Zara's data was collected for recruitment purposes[xliii] *and Airline One should have designed and put in place organizational measures and safeguards including training of employees and clear escalation channels to ensure accountability of all staff.* [xliv]

Stalking or courting is not a purpose included in recruitment [xlv] *and from Zara's story, Airline One did not put in place any measures to limit the possibility of unlawful use of Zara's personal data.*[xlvi]

c). Data minimization

Collection and processing of personal data must be relevant and limited to what is necessary in relation to the specified purpose.[xlii]

Airline One and Alfred, should not collect or process Zara's personal data outside recruitment function. For example, all the questions Alfred asked Zara about her personal preferences and opinions about children, family planning and living with husband's relatives are irrelevant in the recruitment purpose, the reason for which she gave her personal data.

Data minimization requires individuals and entities to avoid the processing of personal data where it is irrelevant.[xliii] It limits the amount of personal data collected and how it is processed for the purpose in question. [xlix]

It also requires data processors to delete personal data where the function for which it was collected is no longer being carried out.

d). Integrity and confidentiality (security)

Personal data is to be collected only where a valid explanation is provided especially whenever information relating to family or private affairs is required.

Meaning personal data should be processed in a manner that encourages and ensures the highest level of security and confidentiality for data subjects, especially where the data concerned is sensitive personal data.

This data ought to be kept safe from unauthorized or unlawful access, loss or destruction. This extends to the equipment used in collecting, processing and storing the personal data.[li]

In Zara's case, this principle was infringed during Alfred's phone interview with Zara asking about her marital status, if she is dating, questions about men in her photos on Instagram, if she has kids, what she thinks of pregnancy, how many children she wants to have, whether she knows how to cook, if she washes her own clothes, what she thinks about living in the village and living with her husband's relatives.

The fact that this call was recorded without Zara's consent means there is a record of very personal details about her life unrelated to recruitment sitting on data storage infrastructure of Airline One.

On the side of her employer Manufacture One, the data breach exposed failures relating to the company's IT systems when the unknown employee monitoring database was made available to everyone in the organization for several hours.

Data processors and controller must always ensure the highest security and confidentiality for personal data collected.

e). Accuracy

Personal data that is collected and stored should be accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any incorrect personal data is deleted or corrected immediately.

In Zara's case, data collected about her was accurate as most of it came directly from her. However, Alfred stalking Zara's social media pages and drawing conclusions about her private life may lead to harmful conclusions and entries into Zara's personal recruitment file.

Airline One is required to take all considerable measures to ensure all incorrect personal data about Zara is deleted or corrected at the earliest opportunity [lii] *as well as to use relevant measures to reduce inaccuracies in their data sets.*[liii]

f). Storage limitation

The data controller ought to delete personal data once the purposes for its processing have been achieved, more so personal data which identifies the data subjects. Periodic review and erasure of data sets by the data controller is key in complying with this principle. [liv]

In Zara's case, Manufacture One, a data controller, had no business keeping a secret record of Zara's conversations with her line managers from the last 9 years. Most of the information from past years was irrelevant to employee or personnel management.

The Data Protection Act requires data controllers to have clear internal procedures for deletion of personal data collected;[lv] as well as appropriate controls to ensure that it is not possible to re-identify anonymised data or recover deleted data [lvi] and, determining which personal data and length of storage is necessary for back-ups and logs as relates to IT systems. [lvii]

g). International transfers require adequate safeguards.

Personal data should not be transferred outside of Kenya unless the data controller has ensured there are sufficient and adequate technical and organizational measures in place to secure the data.

Where adequate safeguards do not exist, or where the data controller deems it necessary, data subjects should be given the opportunity to consent to international transfers of their data. In all cases, data subjects should be made aware of the countries in which their personal data is processed.

In Zara's case there is no mention of international transfers, but for organizations that have entities in various countries and use shared IT infrastructure, it is prudent to have privacy notices for customers, employees, agents, job applicants as well as suppliers that disclose any cross-border data transfers and appropriate safeguards in place.

Exercise

Imagine you sign up to a new social media platform and as part of their registration process you must consent to their Privacy policy. Kindly discuss and highlight what data protection principles you might be looking out for?

Takeaway

We have learnt about Data Protection Principles that include:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimization
- Integrity and confidentiality (security)
- Accuracy
- Storage limitation
- International Transfers require adequate safeguards

5. Rights of a Data Subject & Why They Matter

As Zara learnt more about the Data Protection Act, she discovered that she has rights that help her preserve and protect her privacy as explained below:

a). Right to be informed of how her personal data is being used

Zara exercised this right by asking her employer, Manufacture One, to provide her with an Employee Privacy Notice outlining all the personal data that her employer was collecting about her, how such data is used, with whom it is shared and for how long it is kept.[lviii]

The law requires the privacy notice to be provided to data subjects in a language they understand at the point of data collection. In Zara's case, this had not been done and it is one of the factors the Data Commissioner considered when fining Manufacture One.

b). Right to access personal data in the custody of the data controller or data processor

Zara also asked Manufacture One for a copy of all the personal data they held about her. She was keen to review her personal data from the employee database in order to understand why she was not promoted.

A data subject has the right to view data processed about them and they may request for a copy[lix] of their personal data.[lx]

Zara made the request using Form DPG 2 set out in the First Schedule of the Data Protection (General) Regulations, 2021.

Within seven days,[lxi] her employer had furnished her with a copy of the database records relating to her at no cost to her.[lxii] She also requested Airline

One for a copy of all the information they had about her including interviewer's comments on her performance.

c). Right to object to the processing of all or part of their personal data

Zara was happy to find out she has the right to object to the processing of her personal data entirely or in part.

Zara wrote to Airline One reporting Alfred's actions and objecting to the processing of her personal information by Alfred on social media.

d). Right to correction of false or misleading data;

Zara asked Alfred to take down the false post on their engagement as it was misleading to the public. She also demanded a public apology from Airline One for failing to protect her personal data appropriately.

Under the DPA, the data controller or data processor shall within 14 days of receiving such a request, rectify an entry of personal data in the database when satisfied that rectification is necessary. [lxiii]

Where applications for rectifications are declined, the data controller must notify the data subject, in writing within 14 days of their refusal and outline the reasons for refusal. [lxiv]

e). Right to deletion of false or misleading data

This right is also known as the right to be forgotten and includes instances where the data subject withdraws consent. [lxv]

Zara wrote to Airline One and Alfred requesting deletion of the false and misleading posts by Alfred regarding the non-existence engagement.

The DPA requires deletion to happen within 14 days of the request. [lxvi] If this is not done, Zara can file a complaint with the ODPC.

f). Right to Data Portability

Under the DPA, data subjects have a right to data portability. [lxvii] Data subjects have the right to receive their personal data in a commonly used structured manner that is machine-readable. Zara used this right to get a copy of data stored about her by her employer in the employee monitoring database.

Exercise

You walk into a commercial building. A guard asks you for your original national identity card, records your details in an A4 counter book, gives you a tag and retains your national Identity card at the reception desk until you exit the building. Highlight how you can exercise 3 of the rights outlined above in such situations.

Takeaways:

We have learnt the rights of a data subject which include:

- *Right to be informed of how personal data is being used*
- *Right to access personal data in the custody of the data controller or data processor*
- *Right to object to the processing of all or part of personal data*
- *Right to correct of false or misleading data*
- *Right to delete of false or misleading data*
- *Right to Data Portability*

6. Data Exempted from Application of the Data Protection Act

The processing of personal data is exempt from the provision of the DPA if:

a). It relates to the processing of personal data by an individual during a purely personal or household activities. [lxviii]

Personal activities in this regard have not been sufficiently explained. However, data processed by an individual for instance in a family WhatsApp group is exempted from the provisions of the DPA.

b). If necessary for national security or public interest. [lxix]

When state security organs process your personal data, they are acting in the public interest or for purposes of public security. There are human rights safeguards to protect individual data in custody of and under the processing of the state.

The provisions of the DPA do not apply to their processing of your personal data for public interest grounds where such processing exists as a permitted general situation [lxx] or a permitted health situation [lxxi] Examples of such grounds are discussed below.

i. Permitted general situation [lxxii] relates to the processing of personal data by a data controller or data processor for:

- Lessening or preventing a serious threat to the life, health or safety of any data subject, or to public health (e.g., COVID protocols) or public safety (e.g., anti-terrorism activities);
- Taking appropriate action in relation to suspected unlawful activity or serious misconduct;
- Locating a person reported as missing;
- Asserting a legal or equitable claim;
- Conducting an alternative dispute resolution process;
- Performing diplomatic or consular duties.

ii. Permitted health situation [lxxiii] relates to processing of personal data for:

- The collection of health information to provide a health service;
- For health research and related purposes;
- The use or disclosure of genetic information where necessary and obtained in course of providing a health service;
- The disclosure of health information for a secondary purpose to a responsible person for a data subject.

c). Where disclosure is required under written law or by an order of the court. [lxxiv]

This is where a data subject is required to provide their personal data for the purposes prescribed the law or court order. For instance, the disclosures required under Section 27 of the Kenya Citizenship and Immigration Act for the application and issuance of a passport and other travel documents, or the submission of personal data as evidence before a court of law.

Additionally, section 52 of the DPA provides that, principles of processing personal data shall not apply where -

a). Processing is undertaken by a person for the publication of literary or artistic material. [lxxv] This shall include both in print and digital form, for example, e-newspaper articles or biographies.

b). The data controller reasonably believes that the publication would be in the public interest.[lxxvi] However, if the controller believes that such publication is in the interest of the public, they must demonstrate that the processing is in compliance with the self-regulatory or issued code of ethics in practice and relevant to the anticipated publication. So, for example journalists would need to adhere to the Code of Conduct for the Practice of Journalism.

Exercise

Kindly give examples that may arise in day-to-day activities, where your personal data is processed without your consent, however, it does not result in a breach of your privacy?

Takeaways:

We have learnt about various situations where your personal data may be processed, and such processing may not result in violation of data protection laws. These situations include:

- The processing of personal data by an individual during a purely personal or household activities
- It is necessary for national security or public interest
- Disclosure required under written law or by an order of the court
- Processing is undertaken by a person for the publication of literary or artistic material
- The data controller reasonably believes that the publication would be in the public interest

7. Legal Remedies for Data Protection Breach

Where a data subject is aggrieved by the decision of any person regarding data protection, the data subject may make a complaint to the Data Commissioner. Such a complaint can be made either in writing or orally.

However, where the complaint is made orally, the Data Commissioner shall transfer it into writing.

The written complaint is made by filling-in Form DPC 1 and delivering it to the Data Commissioner[lxxvii] physically, through electronic means such as email or web form[lxxviii] or any other appropriate means.[lxxvix]

Additionally, the complaint may be delivered by the complainant themselves, a person acting on their behalf, or any other person authorized to act on behalf of the data subject or anonymously.[lxxx]

Once the complaint has been received, the Data Commissioner undertakes the following:

1. Record receiving the complaint stating the particulars of the complainant and the complaint filed with the Data Commissioner.

2. Review the complaint and where there is an issue raised under the DPA, admit the complaint.

3. Upon admission the Data Commissioner may;

- **a).** Conduct an inquiry;
- **b).** Conduct an Investigation;
- **c).** Facilitate alternative dispute resolution via mediation, conciliation or negotiation in accordance with the DPA and the regulations; or
- **d).** Use any other mechanisms to resolve the complaint.

4. Upon admission of the complaint, the Data Commissioner shall notify the Respondent of the complaint lodged against them in Form DPC 3 set out in the Schedule of the Data Protection (Complaint Handling and Enforcement Procedure) Regulations, 2021, and allow the Respondent

to make various submissions in support of their complaint.

5. Where the Data Commissioner concludes investigations, the Commissioner shall issue a determination in writing of their findings.

6. Where the determination includes remedies, such remedies may include:

a). An enforcement notice

Where the Data Commissioner is satisfied that a person has failed, or is failing, to comply with any provision of this Act, the Data Commissioner may serve an enforcement notice[lxxxi] on that person requiring that person to take such steps within the timeline specified in the notice.

This may for example include directions that an entity corrects specified data within 7 days of receipt of the Notice from the Commissioner.

b). A penalty Notice imposing an administrative fine

This may apply where the respondent fails to comply with the enforcement notice. The maximum amount of the penalty that may be imposed by the Data Commissioner in a penalty notice is five million Kenya Shillings **(Kshs. 5,000,000)**, or in the case of an undertaking, up to one per cent of its annual turnover of the previous financial year, which is ever is lower.[lxxxii]

The Commissioner may issue fines of various amounts depending on the circumstances and facts of the case at hand.

c). A dismissal of the complaint where it lacks merit

The Data Commissioner may dismiss a complaint where the Commission finds that the complaint lacks any issue for determination.

Such dismissal shall be justified in the Commissioner's decision, with the option for appeal where the complainant is dissatisfied.

d). A recommendation for prosecution

The Data Commissioner may recommend a criminal case against the data controller or processor where the Commission finds that a crime has been committed and criminal charges may be brought against the data processor or data controller or any other party.

e). An order for compensation to the data subject by the respondent .

Compensation is awarded when a data subject suffers damage from the processing of personal data by a data controller and the data processor is found liable for failing to observe the provisions of the DPA, and its regulations or where the Respondent acts outside, or contrary to the data controller's lawful instructions. [lxxxiii]

Damages include financial loss and damage not involving financial loss, including emotional distress. [lxxxiv]

Any person against whom any administrative action is taken by the Data Commissioner, including the enforcement of penalty notices, is not satisfied by the decision they may appeal to the High Court for a reprieve. [lxxxv]

Exercise

Go to the Data Commissioners Office at *https://www.odpc.go.ke/file-a-complaint/*, download the page as a form and help Zara file a complaint against Manufacture One and Airline One based on her story from Chapter 2.

Takeaway:

Where a data subject is aggrieved by the decision of any person regarding data protection, the data subject may file a complaint to the Data Commissioner in the prescribed manner.

8. Quasi-Judicial Redress & Reporting to Social Media Platforms

In this Chapter, we discuss the complaints mechanisms for social media platforms such as WhatsApp Facebook, Instagram and Twitter. These complaints mechanisms exist outside the formal legal complaints and enforcement frameworks and platform specific. They are put in place by platforms to ensure that their users' right to privacy is protected while using these platforms.

1. Reporting to the relevant Data Controller

Other remedies for data protection issues include reporting the issue directly to the relevant data controller via channels designated in their privacy policies usually email or telephone and the address of the Data Protection Officer.

Reporting to the Data Protection Officer or via a designated reporting channel for privacy concerns allows your issue to be remedied under the Data Protection Act. It also provides an opportunity for issues to be resolved without needing to litigate.

2. Reporting to Social Media Platforms

In the context of the internet, social media platforms that often act as data processors provide channels for users to report privacy violations on the respective platform.

Reporting privacy violations that happen on social media is critical to ensure online safety and respect for privacy online. This segment highlights how to report issues on various social media platforms including Facebook, Twitter, and WhatsApp.

After what Zara endured on social media due to Alfred's indiscretions, Zara discovered that there were privacy controls on social media platforms that she was not aware of and began to explore privacy settings that she could use to protect herself better online.

a) Reporting on WhatsApp

For Android users:

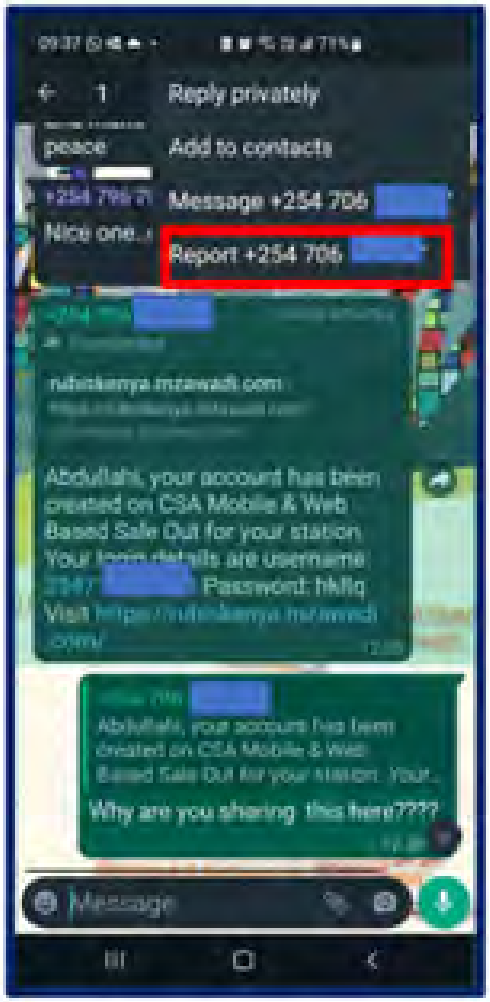
- Open the chat with the user you wish to report.
- Tap More options > More > Report.
- Check the box if you would like to also block the user and delete messages in the chat.
- Tap REPORT.

For iOS users:

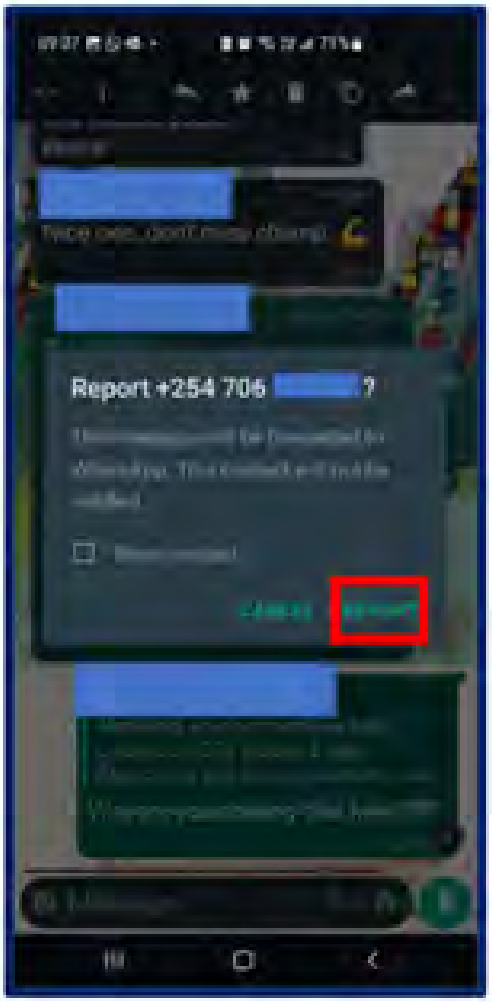
- Open the chat with the user you wish to report.
- Tap the contact name, then tap Report Contact.
- Tap Report and Block.

Note: WhatsApp receives the last five messages sent to you by the reported user or group, and they won't be notified. WhatsApp also receives the reported group or user ID, information on when the message was sent, and the type of message sent (image, video, text, etc.).[lxxxvi]

You can also choose to report an account by long pressing a single message. Long press an individual message and tap on the overflow menu. The option to report the contact will appear along with a confirmation notification and the option to block.



Step 1 long press message, press 3 dots top of page, choose report



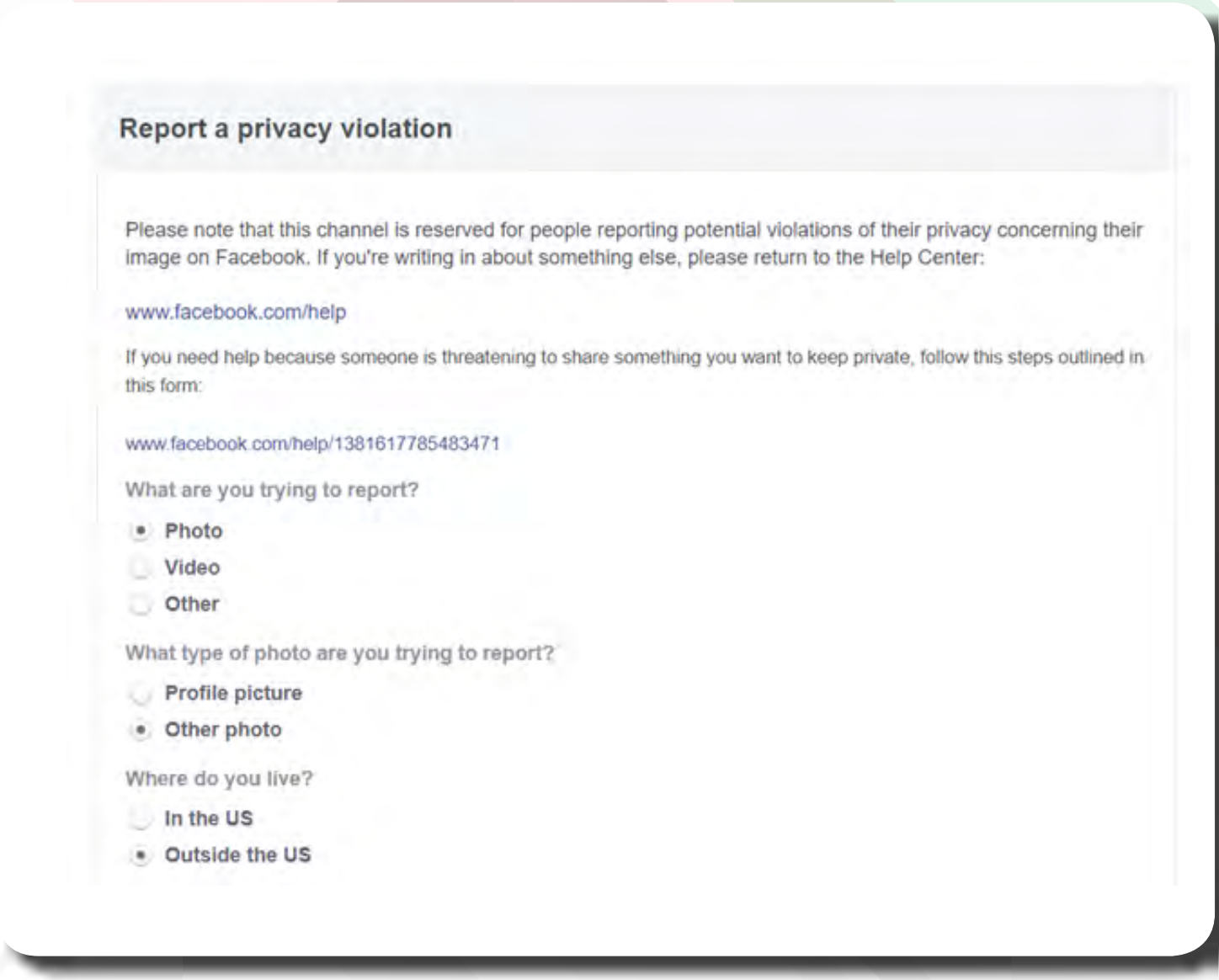
Step 2, select report

Further information on how to block and report contacts on WhatsApp is available on the WhatsApp FAQ page at https://faq.whatsapp.com/2798237480402991/?locale=fi_FI for Android and https://faq.whatsapp.com/455142541854847/?helpref=faq_content for iOS

b) Reporting Privacy Issues on Facebook

Zara discovered Meta allows Facebook subscribers to report various types of privacy issues on Facebook including: [lxxxvii]

I. Report a photo or video on Facebook that violates your privacy via the form available at *https://www.facebook.com/help/contact/144059062408922.*
Pick appropriate responses in the form. Example below:



Report a privacy violation

Please note that this channel is reserved for people reporting potential violations of their privacy concerning their image on Facebook. If you're writing in about something else, please return to the Help Center:

www.facebook.com/help

If you need help because someone is threatening to share something you want to keep private, follow this steps outlined in this form:

www.facebook.com/help/1381617785483471

What are you trying to report?

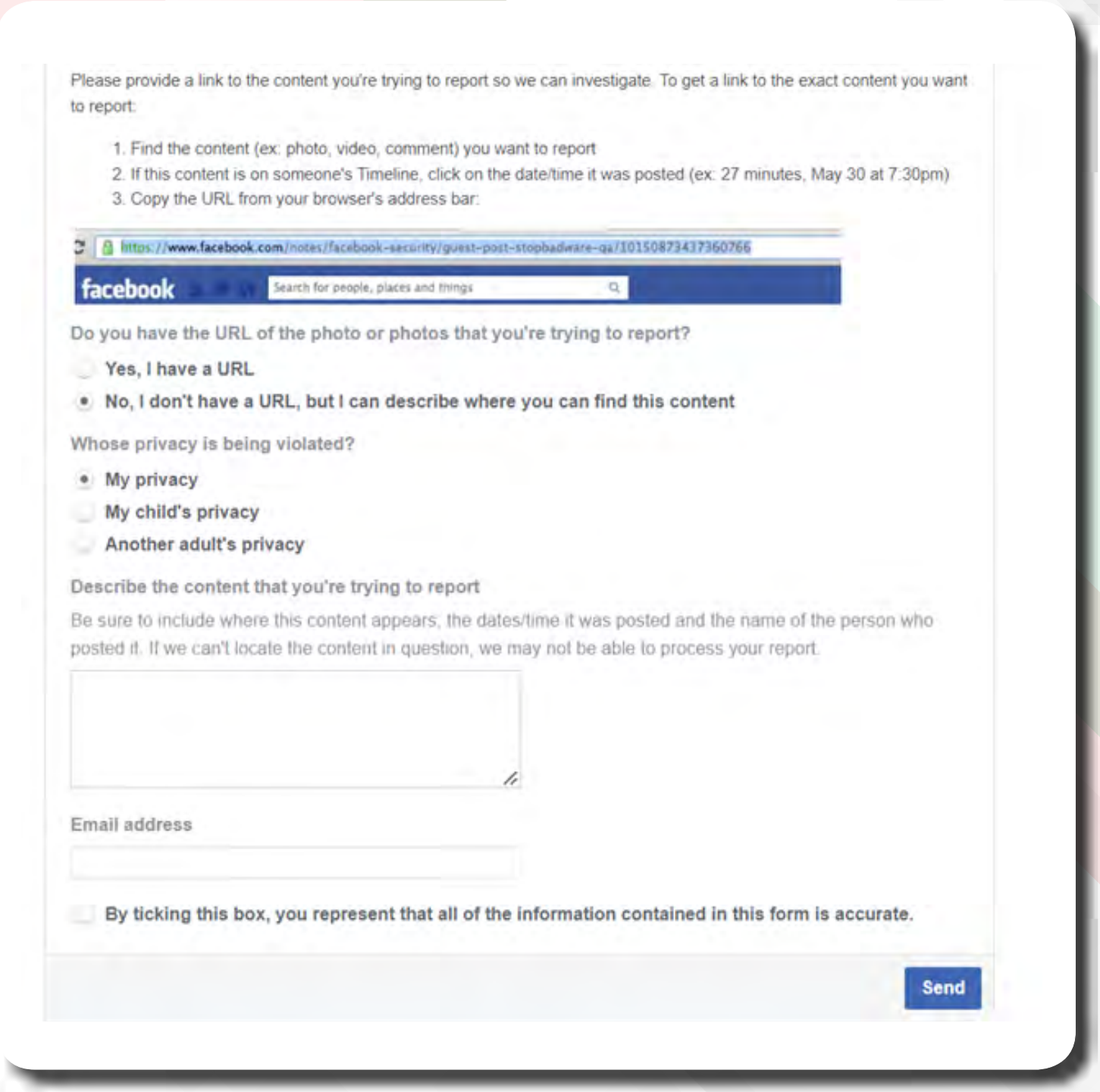
- (•) Photo
- ( ) Video
- ( ) Other

What type of photo are you trying to report?

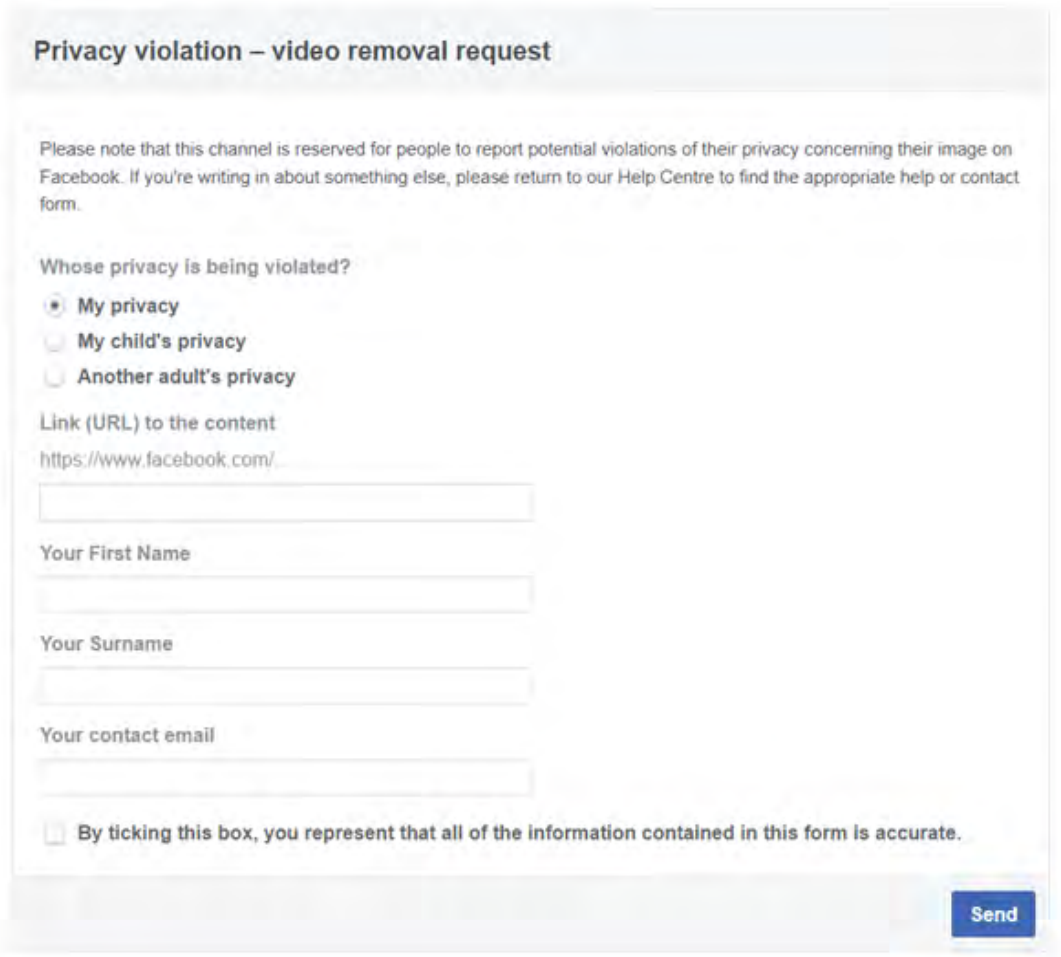
- ( ) Profile picture
- (•) Other photo

Where do you live?

- ( ) In the US
- (•) Outside the US



A Uniform Resource Locator (URL) is used to help identify content available on the internet accurately in order to enable the social media platform to find the content you are referring to. It is often available on the tab of your computer browser and often begins with *"https://www.platformexactaddress."* If you have the URL of the content you're reporting, then reporting is rather straightforward:



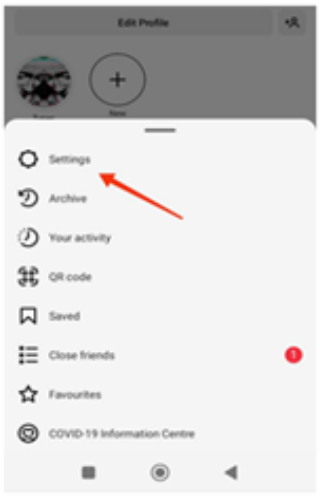
You can read Facebook's policy on privacy violations on their page available at https://transparency.fb.com/en-gb/policies/community-standards/privacy-violations-image-privacy-rights/

Once the report has been made one can review their privacy settings to ensure that content they share on Facebook is only available to the intended audience.[lxxxviii]

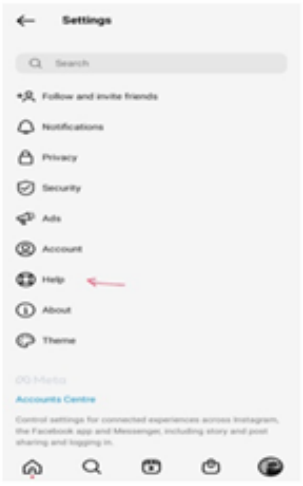
c). Reporting Privacy Issues on Instagram

Instagram, like other Meta platforms, allows its users to report privacy breaches for immediate resolution.

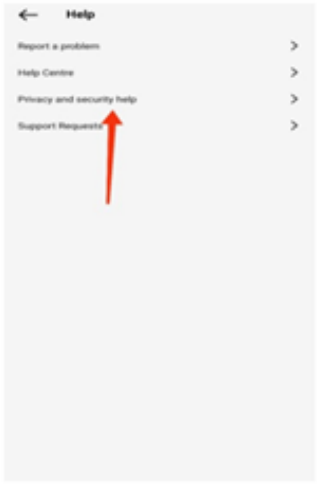
More so intimate images that expose any user without their consent. In order to make the report you are required to follow the steps below:



Step 1: On the top right Select Settigns



Step 2: Select the Help Icon



Step 3: Select the Privacy and Security Option

Step 4: Select the Report Intimate Images Option

Step 5 : Select the Report Form

Step 6: Select the best Option and report the particular post

One may also report a post from the timeline

d). Reporting Privacy Issues on Twitter

Twitter allows subscribers to report privacy-related violations. Anyone can report (to Twitter) private information that has been shared in a clearly abusive way (whether they have a Twitter account or not). In cases where the information has not been shared with a clearly abusive intent, Twitter needs to hear directly from the owner of this information (or an authorized representative, such as a lawyer) before taking enforcement action.

Twitter prohibits sharing the following types of private information, without the permission of the person to who it belongs to : [lxxxix]

- Home address or physical location information, including street addresses, GPS coordinates or other identifying information related to locations that are considered private;
- Identity documents, including government-issued IDs and social security or other national identity numbers –

Note: We may make limited exceptions in regions where this information is not considered to be private;

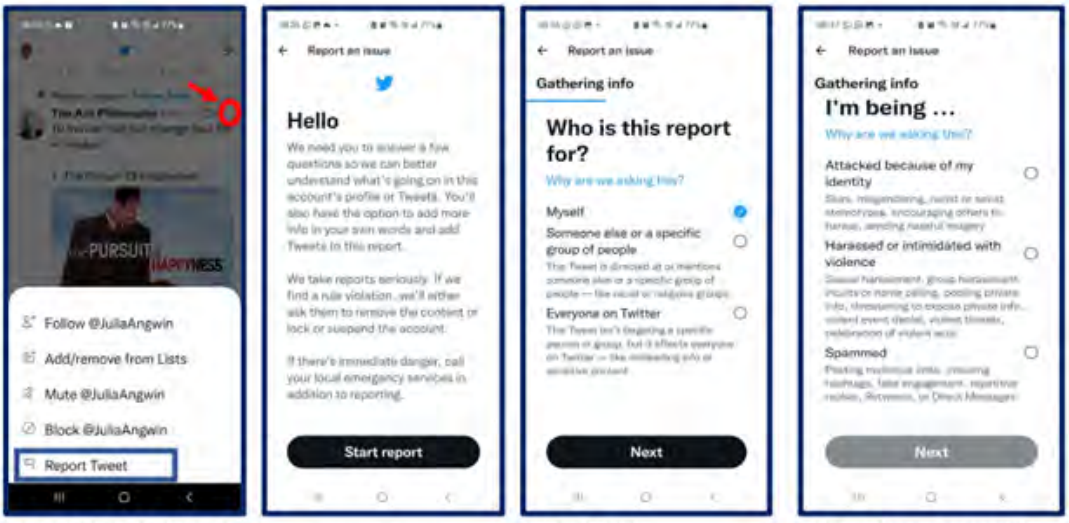
- Contact information, including non-public personal phone numbers or email addresses;
- Financial account information, including bank account and credit card details;
- Other private information, including biometric data or medical records;
- Media of private individuals without the permission of the person(s) depicted; and
- Media depicting prisoners of war posted by government or state-affiliated media accounts on or after April 5, 2022.

The following behaviours are also not permitted:

- Threatening to publicly expose someone's private information;
- Sharing information that would enable individuals to hack or gain access to someone's private information without their consent e.g., sharing sign-in credentials for online banking services;
- Asking for or offering a bounty or financial reward in exchange for posting someone's private information;
- Asking for a bounty or financial reward in exchange for not posting someone's private information, sometimes referred to as blackmail.

Policy violations can be reported via the Twitter App as well as via Twitter on the desktop.
In-app: You can report this content for review in-app as follows:

- Select Report Tweet from the icon.
- Select It's abusive or harmful.
- Select Includes private information.
- Select the type of information that you're reporting.
- Select the relevant option depending on who owns the information you are reporting.
- Select up to 5 Tweets to report for review.
- Submit your report.

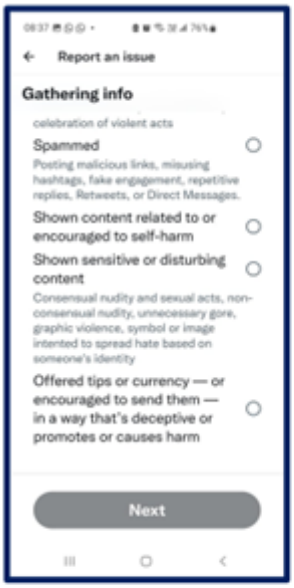


Step 1 click on 3 dots next to tweet for pop up then choose report tweet

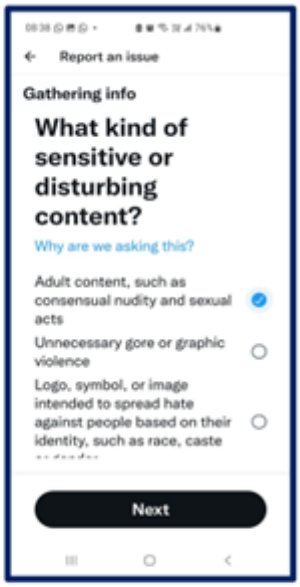
Step 2- click start report

Step 3: Pick appropriate answer then click next

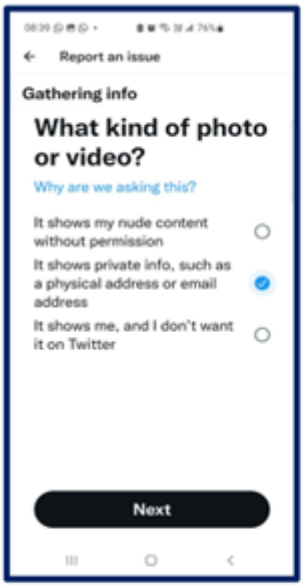
Step 4: Choose appropriate answer for your situation then click next



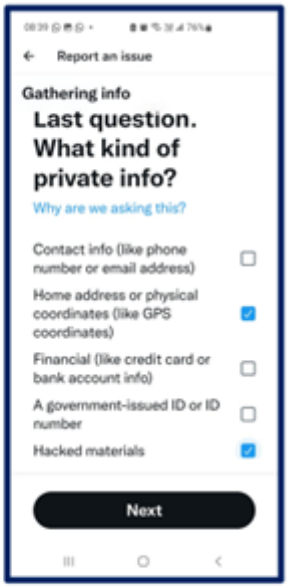
Step 5: Choose appropriate answer for your situation then click next



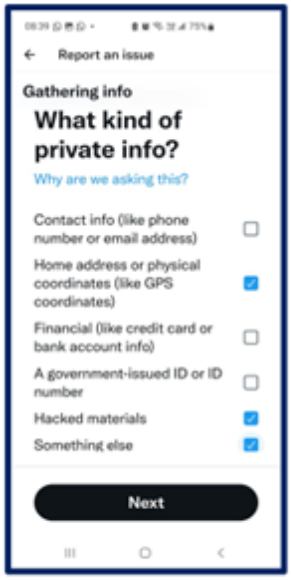
Step 6: Choose appropriate answer for your situation then click next



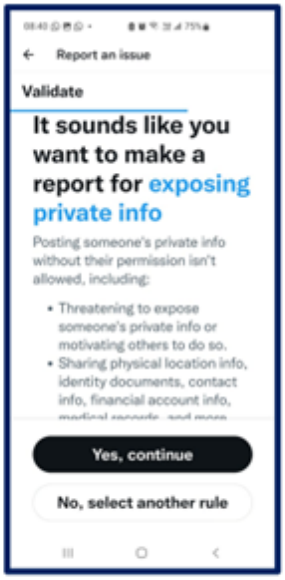
Step 7: Choose appropriate answer for your situation then click next



Step 8: Choose appropriate answer for your situation then click next



Step 9: Choose appropriate answer for your situation then click next



Step 10: Review prompt and if accurate summary of your intention click yes continue to complete reporting.

Step 10 other options if you scroll down.

Takeaway

How to practically report privacy issues on

- WhatsApp
- Twitter
- Facebook
- Instagram

9. Tips for Safeguarding Data Protection Online

Protecting personal data online is an important issue that cannot be overlooked. Headlines of online hacking and violations of privacy are increasing every day. There are steps you can take to help manage and protect your personal data online as you use various websites and social media platforms. This segment offers tips on how to protect or enhance privacy online as well as on several social media platforms.

a). Limit the personal information you share on social media

The best way to keep your personal data safe is to stop yourself from oversharing online.

Providing too much information on Facebook, Twitter, WhatsApp Status and Instagram could make it easier for cybercriminals to obtain personally identifying information, making it easier to steal your identity or to access your sensitive data.

For example, could a stranger identify your mother's maiden name, the name of your first pet or the first school you went to from digging through your Facebook account?

This information is sometimes used as a security question to change passwords on banks or other financial accounts. If such security questions apply with your banker, ensure this information is not available online by simply not sharing it.

Where possible refrain from sharing online any information about your children, your location or the banking services you use. To protect your personal data online, be selective on what you fill in the "About Me" fields in your social media profiles, where possible, leave them blank or with super general information.

It is advisable not to publicly share your year of birth or exactly where you were born to avoid being an easy target for identity theft.

b). Always use privacy settings available on online media platforms to limit who can view your posts.

Do not idly send out or accept friend requests simply to 'grow your following' put some careful

thought into who has access to your wall or timeline.

For example, accepting Facebook friend requests from strangers exposes the personal information you share with "Friends" to being viewed by strangers.

More on this point when we discuss privacy settings across some of the most popular social media platforms.

c). Create strong and unique passwords

Create strong and unique passwords for your social media accounts to help prevent others from logging into them in your name.

This means using a combination of at least 8 characters including, numbers, special characters (*&%$#@!+=?/><.,), and upper- and lower-case letters. Do not use personal information that is easy to guess — such as your date of birth, ID number, name or the word password — as your password.

d). Use a password manager

Use a password manager to help you store and manage your passwords. Password managers support you to have unique passwords for your various online accounts increasing the privacy and security of your personal data online.

Do not use the same passwords across multiple emails and social media platforms. Using the same password may make it "easier for you to remember" but it also makes it much easier for you to be hacked across all your accounts.

Using unique strong passwords for each of your social media accounts helps mitigate the severity of damage or harm that could occur should your credentials be compromised.

e) Browse in incognito or private mode.

If you do not want your browsing history, temporary internet files, or cookies saved on your computer, do your web surfing in "private mode" on your browser of choice.

In Chrome, private mode is called "Incognito Mode". Firefox calls its setting "Private Browsing", and Internet Explorer uses the name "InPrivate Browsing" for its privacy feature.

When you search with these modes turned on, others won't be able to trace your browsing history from your computer. But these private modes are not completely private.

When you're searching in incognito or private mode, your Internet Service Provider (ISP) can still see your browsing activity. If you are searching on a company computer, your employer can see your browsing history.

The websites you visit can also track you. If you want more privacy, online consider using anonymous search engines and virtual private networks instead.

Additionally, browsers such as Chrome Browsers by Google have Safety Centers that enable users to learn and navigate the browsers safely.

f). Use and download authentic apps

Authentic applications can be downloaded from online stores such as Google Play store, Apple App Store, Microsoft App store or from the legitimate developer's website. Avoid downloading applications from unverified, or untrusted sources on the internet.

g). Regularly conduct privacy check-ups across platforms you use

Several social media platforms have privacy check-up centres or privacy centres that provide step by step guidance on how to review privacy settings or adjust your privacy settings on the platforms.

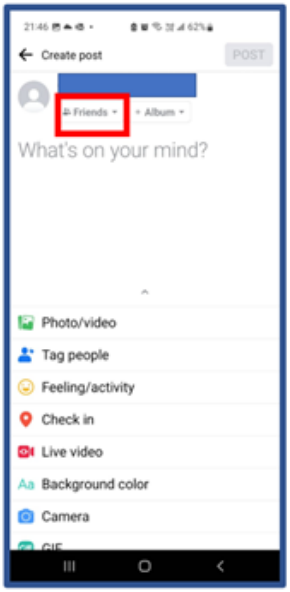
Please regularly visit them and review your account settings and privacy protections.

- Google: *https://safety.google/*
- Facebook: *https://www.facebook.com/help/443357099140264*
- Twitter: *https://help.twitter.com/en/rules-and-policies/personal-information*

10. Annex: Exercises on further Social Media Controls

a) Privacy Features on Facebook When Sharing Posts

Exercise: Create a new post on Facebook and apply different privacy settings



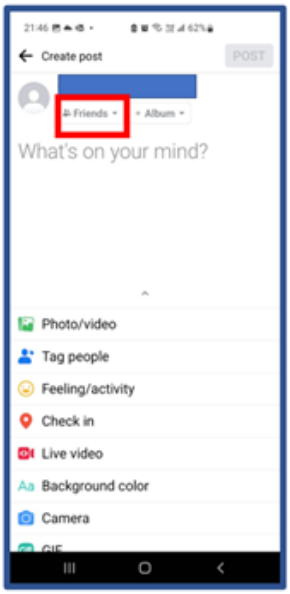
Create new post, select Friends box

Choose appropriate audience based on what you are sharing to protect your privacy

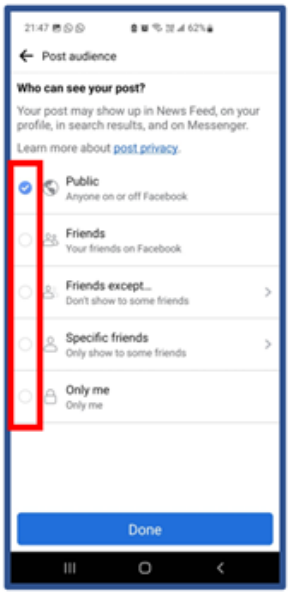
Privacy features when sharing posts on Facebook

b). Privacy Features in Facebook Account Settings

Exercise: Edit your Facebook privacy Settings

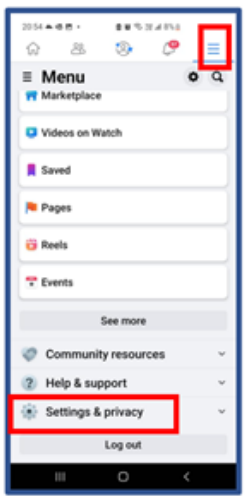


Create new post, select Friends box

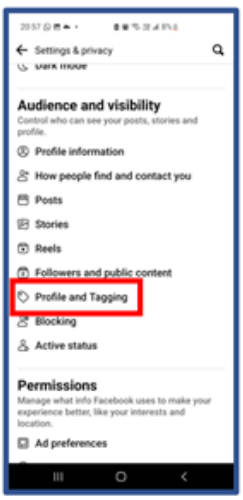


Choose appropriate audience based on what you are sharing to protect your privacy

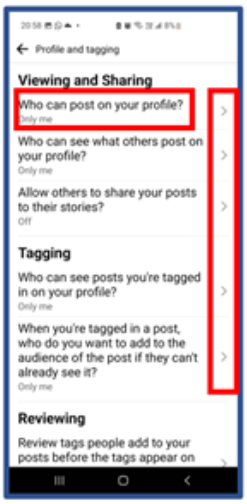
Privacy features when sharing posts on Facebook



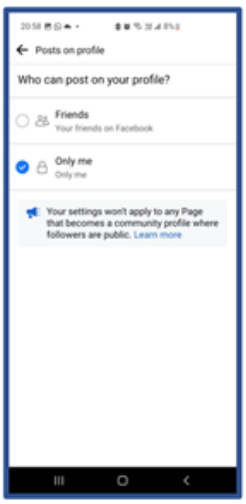
Privacy features in Account Settings Step1: Click on 3 dots at top right/bottom of Facebook App Menu and select Settings & Privacy



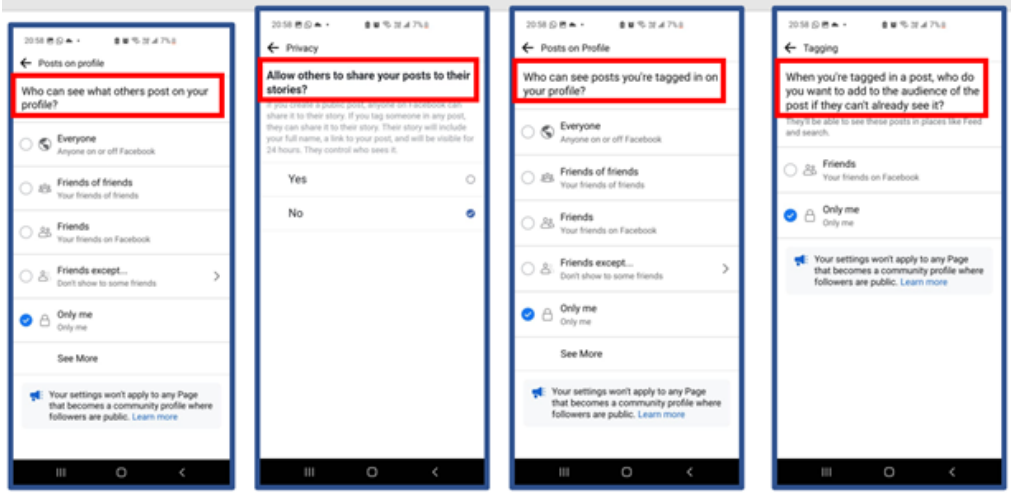
Step 2: Select profile & tagging



Our Step 3 choose who can post on your profile. You can explore any option via clicking on arrow on the right. We explore the rest after step 4

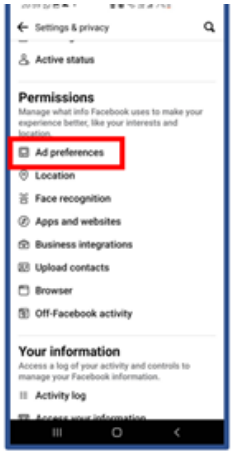


Step 4: adjust privacy setting to your liking. Choose "me only' to limit others posting on your profile.

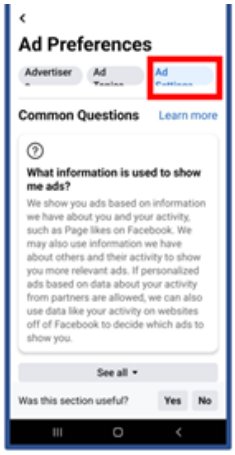


Steps 5 to 8 adjust settings as appropriate for your case by answering question highlighted.

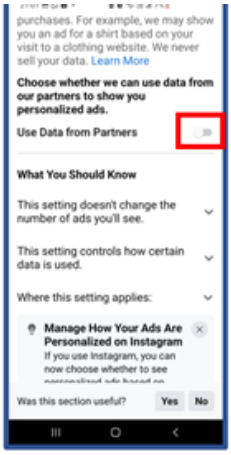
Step 9 adjust settings as appropriate for your case by answering question highlighted.



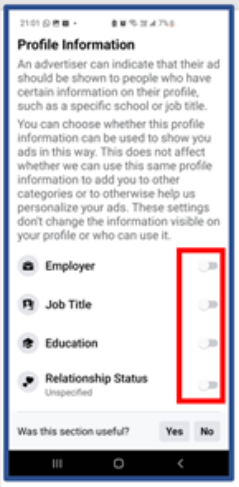
Step 10 : Use step 1&2 to go back to settings menu and select Ad preference



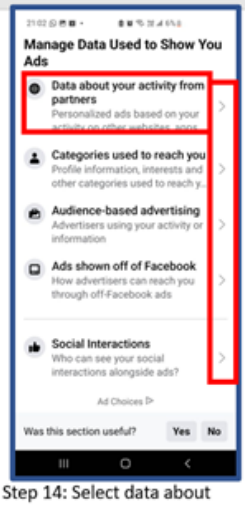
Step 11: select Ad settings



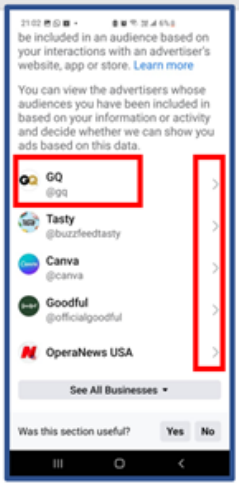
Step 12: Disable use of data from partners to increase your privacy, so platform stops tracking you on partner sites



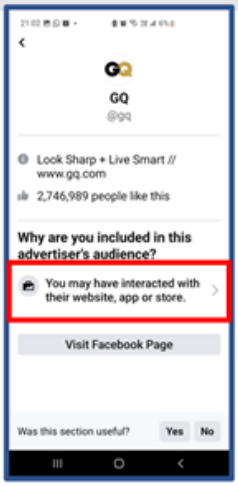
Step 13: disable boxes highlighted to limit ad profiling based on mention data sets



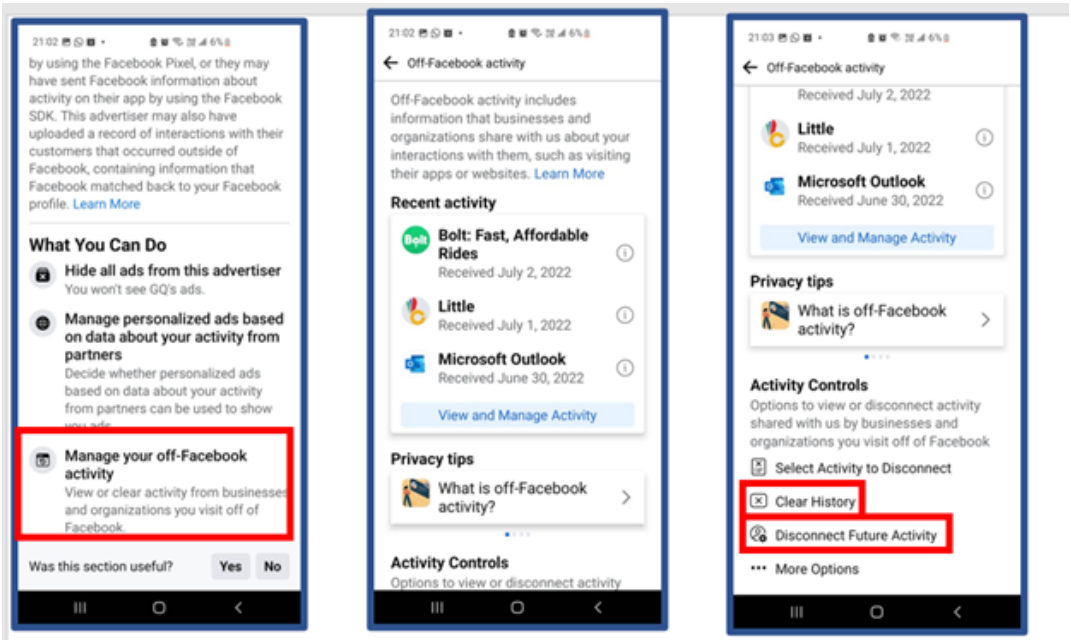
Step 14: Select data about your activity from partners to see activities platform tracks about you for ad profiling purposes.



Step 15: Choose partner to explore as highlighted above



Step 16: click on highlighted box to find out how Platform tracked your activity with Partner



Step 16- Click Manage your off Facebook activity to limit platform tracking you on your phone.

Step 17: Scroll down and choose clear history and then choose disconnect future activity to prevent Facebook App monitoring your activity outside Facebook App

c) Report a photo or video on Facebook that violates the privacy of your child

Exercise: Report Photo on Facebook that violates child privacy

This can be done via the form available at *https://www.facebook.com/help/contact/144059062408922.* Fill in wi
responses. Example below:

Report a privacy violation

Please note that this channel is reserved for people reporting potential violations of their privacy concerning their image on Facebook. If you're writing in about something else, please return to the Help Center:

www.facebook.com/help

If you need help because someone is threatening to share something you want to keep private, follow this steps outlined in this form:

www.facebook.com/help/1381617785483471

What are you trying to report?

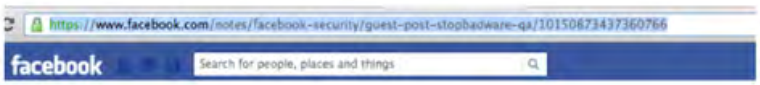
- Photo
- (•) Video
- Other

Where do you live?

- In the US
- (•) Outside the US

Please provide a link to the content you're trying to report so we can investigate. To get a link to the exact content you want to report:

1. Find the content (ex: photo, video, comment) you want to report
2. If this content is on someone's Timeline, click on the date/time it was posted (ex: 27 minutes, May 30 at 7:30pm)
3. Copy the URL from your browser's address bar:



Do you have the URL of the video or videos you're trying to report?

- Yes, I have a URL
- (•) No, I don't have a URL, but I can describe where you can find this content

Whose privacy is being violated?

- My privacy
- (•) My child's privacy
- Another adult's privacy

How old is your child?

- (•) Under 13
- 13 or older

Describe the content that you're trying to report

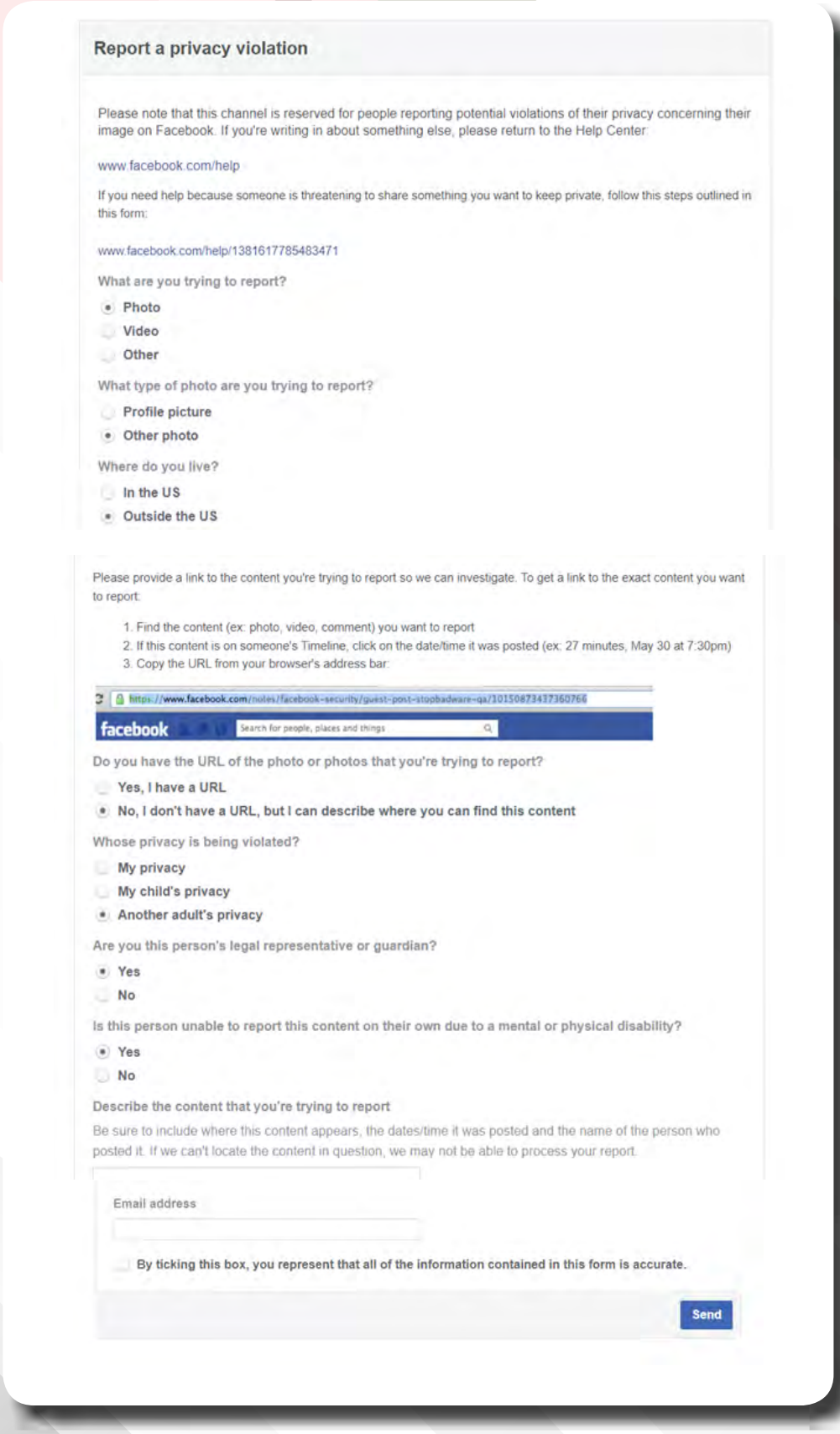
Be sure to include where this content appears, the dates/time it was posted and the name of the person who posted it. If we can't locate the content in question, we may not be able to process your report.

Email address

- By ticking this box, you represent that all of the information contained in this form is accurate.

Send

III. Report a photo or video on Facebook that violates the privacy of someone who is sick, hospitalized or otherwise incapacitated via the form available at *https://www.facebook.com/help/contact/144059062408922.* Fill in with appropriate responses. Example below:



Report a privacy violation

Please note that this channel is reserved for people reporting potential violations of their privacy concerning their image on Facebook. If you're writing in about something else, please return to the Help Center:

www.facebook.com/help

If you need help because someone is threatening to share something you want to keep private, follow this steps outlined in this form:

www.facebook.com/help/138161785483471

What are you trying to report?

- (•) Photo
- ( ) Video
- ( ) Other

What type of photo are you trying to report?

- ( ) Profile picture
- (•) Other photo

Where do you live?

- ( ) In the US
- (•) Outside the US

Please provide a link to the content you're trying to report so we can investigate. To get a link to the exact content you want to report:

1. Find the content (ex: photo, video, comment) you want to report
2. If this content is on someone's Timeline, click on the date/time it was posted (ex: 27 minutes, May 30 at 7:30pm)
3. Copy the URL from your browser's address bar:

https://www.facebook.com/notes/facebook-security/guest-post-stopbadware-qa/10150873417360766

facebook Search for people, places and things

Do you have the URL of the photo or photos that you're trying to report?

- ( ) Yes, I have a URL
- (•) No, I don't have a URL, but I can describe where you can find this content

Whose privacy is being violated?

- ( ) My privacy
- ( ) My child's privacy
- (•) Another adult's privacy

Are you this person's legal representative or guardian?

- (•) Yes
- ( ) No

Is this person unable to report this content on their own due to a mental or physical disability?

- (•) Yes
- ( ) No

Describe the content that you're trying to report

Be sure to include where this content appears, the dates/time it was posted and the name of the person who posted it. If we can't locate the content in question, we may not be able to process your report.

Email address

[ ] By ticking this box, you represent that all of the information contained in this form is accurate.

Send

d). Reporting Privacy Issues on Twitter via Desktop

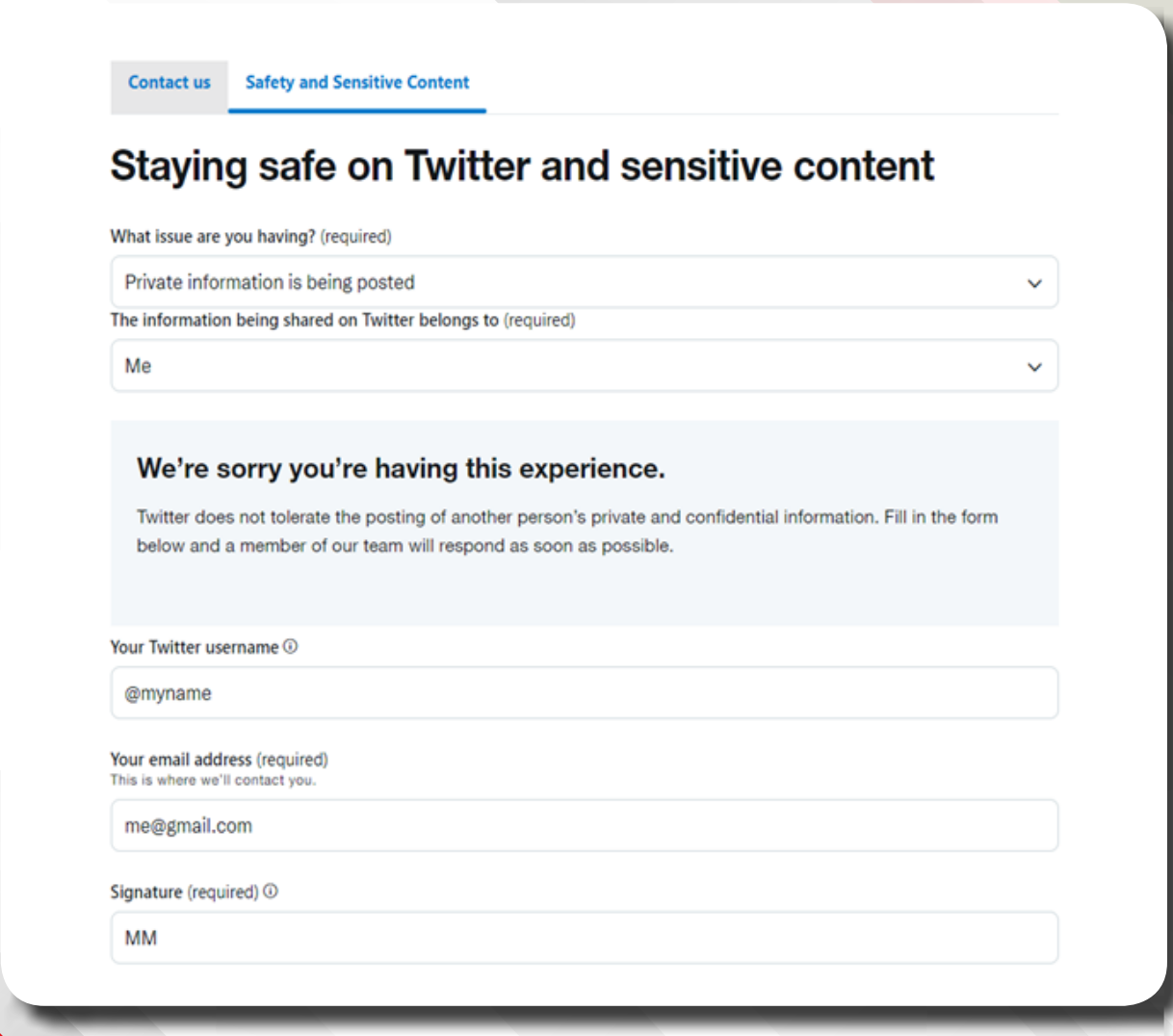
Exercise: Report privacy derogation on Twitter via computer desktop

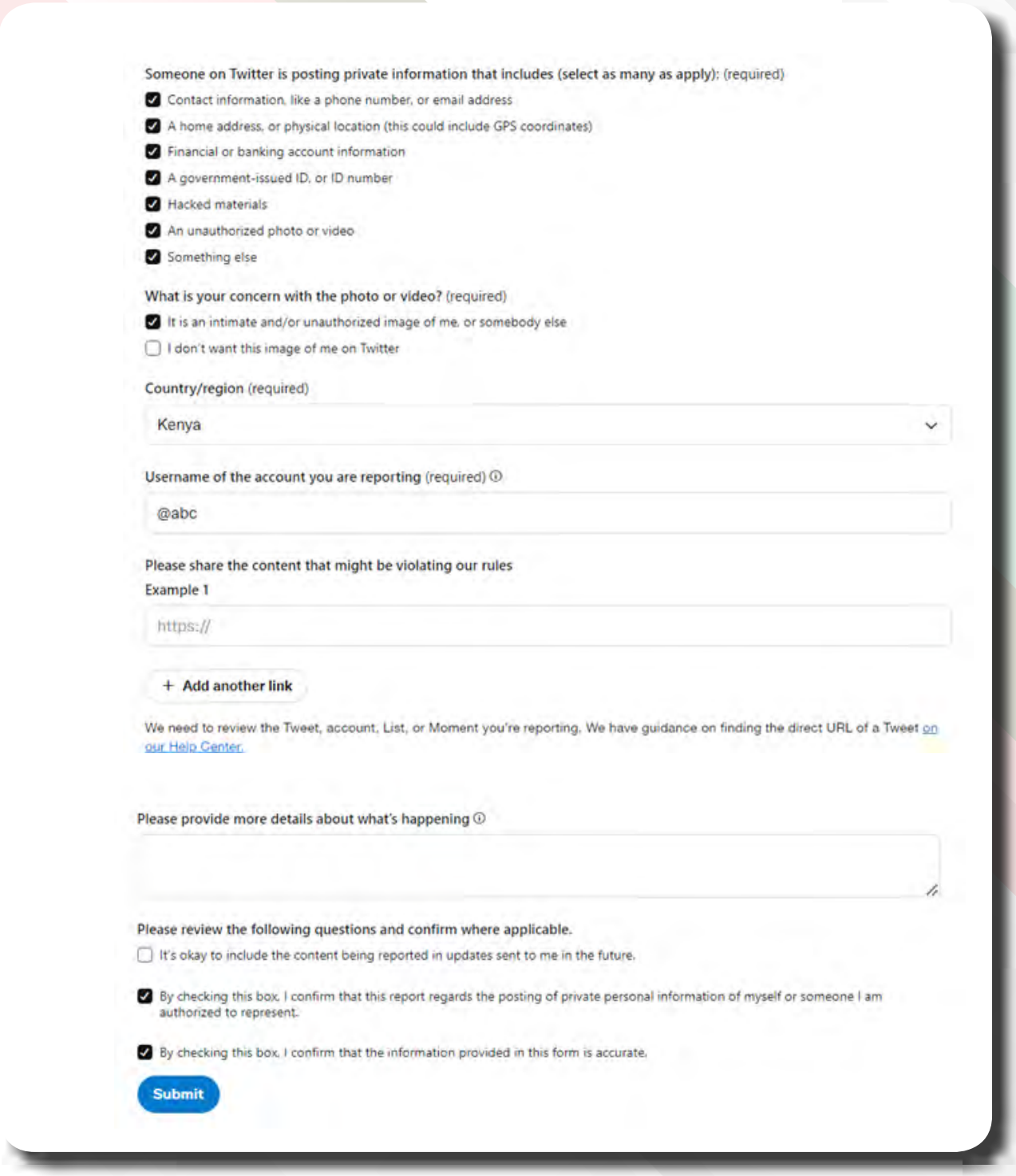
You can report violating content for review via desktop as follows:

- Select Report Tweet from the icon.
- Select It's abusive or harmful.
- Select Includes private information.
- Select the type of information that you're reporting.
- Select the relevant option depending on who owns the information you are reporting.
- Select up to 5 Tweets to report for review.
- Submit your report.

You can also report this content for review via Twitter's private information report form, by selecting the type of private information that you want to report.

The form is available at *https://help.twitter.com/en/forms/safety-and-sensitive-content/private-* information and reports can be made as below:





Takeaway

How to practically:

- Apply privacy settings on Facebook on posts and on account settings
- Report violations of child privacy
- Reporting privacy issues on Twitter via desktop

e) Additional Resources

1. What is Privacy *https://privacyinternational.org/explainer/56/what-privacy*
2. How To Improve Your Online Privacy and Security *https://helpdeskgeek.com/how-to/how-to-improve-your-online-privacy-and-security/*
3. Women's rights online: tips for a safer digital life *https://edri.org/our-work/womens-rights-online-tips-for-a-safer-digital-life/*
4. Data Protection and Privacy. A Gender Perspective *https://www.kictanet.or.ke/mdocs-posts* /data-protection-and-privacy-a-gender-perspective/

END NOTES

[i] Ibid

[ii] Ibid

[iii] Ibid

[iv] Ibid

[v] Universal Declaration of Human Rights available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights

[vi] Section 2, Data Protection Act 2019

[vii] What is Privacy by Privacy International, available at: https://privacyinternational.org/explainer/56/what-privacy

[viii] https://privacyinternational.org/explainer/56/what-privacy

[ix] Section 2 Data Protection Act

[x] Current World Population by Worldometer available at: https://www.worldometers.info/world-population/

[xi] Gender Ratio in the World by Statitistic Times, available at: https://statisticstimes.com/demographics/world-sex ratio.php#:~:text=Gender%20ratio%20in%20the%20World&text=The%20population%20of%20females%20in,101.68%20males%20per%20100%20females.

[xii]The Human Right to Privacy: A Gender Perspective by Office of the High Commissioner for Human Rights, available at: https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf

[xiii] Data Reportal, Digital 2021: Kenya by Simon Kemp, 11th February 2021, available at: https://datareportal.com/reports/digital-2021-kenya

[xiv] Ibid

[xv] Kenya Population 2022 live by World Population Review, available at: https://worldpopulationreview.com/countries/kenya-population

[xvi]Male to female ratio of the total population in Kenya from 2000 to 2021(in male births per 100 female births) by Statista, available at: https://www.statista.com/statistics/1226942/male-to-female-ratio-of-the-total-population-in-kenya/#:~:text=As%20of%202020%2C%20Kenya's%20population,the%20country%20registered%20minimal%20increases.

[xvii] What Do Women Do Online? Organisation for Economic Co-operation and Development available at: https://www.oecd.org/gender/data/what-do-women-do-online.htm

[xviii]What Global Employers Need Know About Employee Monitoring Tools and Laws by VISTRA available at: https://www.vistra.com/insights/what-global-employers-need-know-about-employee-monitoring-tools-andlaws#:~:text=As%20more%20employees%20work%20outside,employees'%20performance%20and%20online%20activity.

[xix] Stalking Factsheet by Stalking Awareness, available at: https://www.stalkingawareness.org/wpcontent/uploads/2019/01/SPARC_StalkngFactSheet_2018_FINAL.pdf

[xx] Stalking Statistics and Facts by Safe Horizons available at: https://www.safehorizon.org/get-informed/stalking-statistics-facts/#statistics-and-facts/

[xxi] Constitution of Kenya, 2010 available at: http://kenyalaw.org/lex/actview.xql?actid=Const2010

[xxii] Article 31 Constitution of Kenya 2010

[xxiii] Data Protection Act, 2019, available at: http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2024%20of%202019

[xxiv] Short Title Data Protection Act 2019

[xxv] Section 8 Data Protection Act 2019

[xxvi]Data Protection General Regulations 2021, available at: https://www.odpc.go.ke/wp-content/uploads/2021/06/L.N-263-265-THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021FIN....pdf

[xxvii] Part III Data Protection (General) Regulations, 2021

[xxviii] Part VI Data Protection (General) Regulations, 2021

[xxix] Part VII Data Protection (General) Regulations, 2021

[xxx] Section 51(2) (b) Part IX Data Protection (General) Regulations, 2021

[xxxi]Data Protection General Regulations 2021, available at: https://www.odpc.go.ke/wp-content/uploads/2021/06/L.N-263-265-THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021FIN....pdf

[xxxii] Regulation 3 (a) Data Protection (Regulations, 2021

[xxxiii] Data Protection General Regulations, 2021 available at: https://www.odpc.go.ke/wp-content/uploads/2021/06/L.N-263-265-THE-DATA-PROTECTION-GENERAL-REGULATIONS-2021FIN....pdf

[xxxiv]Guidance Note for Electoral Purposes, available at: https://www.odpc.go.ke/download/guidance-notes-for-electoral-purposes/

[xxxv]Guidance Note on Electoral Purposes, available at: https://www.odpc.go.ke/download/guidance-notes-for-electoral-purposes/

[xxxvi]Guidance Note on Registration of Data Controllers and Processors, available at: https://www.odpc.go.ke/download/guidance-note-on-registration-of-data-controllers-and-data-processors/

[xxxvii] Principles of Data Protection, available at: https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data protection#:~:text=Purpose%20Limitation%3A%20Personal%20data%20should,is%20incompatible%20with%20those%20purposes .

[xxxviii] Regulation 29 (a) Data Protection (General) Regulations, 2021

[xxxix] Regulation 29 (b) Data Protection (General) Regulations, 2021

[xl] Regulation 29 (c) Data Protection (General) Regulations, 2021

[xli] Regulation 29 (d) Data Protection (General) Regulations, 2021

[xlii] Principles of Data Protection, available at: https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection#:~:text=Purpose%20Limitation%3A%20Personal%20data%20should,is%20incompatible%20with%20those%20purposes.

[xliii] Regulation 31 (a) Data Protection (General) Regulations, 2021

[xliv] Regulation 31 (b) Data Protection (General) Regulations, 2021

[xlv] Regulation 31 (d) Data Protection (General) Regulations, 2021

[xlvi] Regulation 31 (f) Data Protection (General) Regulations, 2021

[xlvii] Principles of Data Protection, available at: https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection#:~:text=Purpose%20Limitation%3A%20Personal%20data%20should,is%20incompatible%20with%20those%20purposes.

[xlviii] Regulation 33 (a) Data Protection (General) Regulations, 2021

[xlix] Regulation 33 (b) Data Protection (General) Regulations, 2021

[l] Regulation 33 (e) Data Protection (General) Regulations, 2021

[li]Principles of Data Protection, available at: https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection#:~:text=Purpose%20Limitation%3A%20Personal%20data%20should,is%20incompatible%20with%20those%20purposes

[lii]Principles of Data Protection, available at: https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection#:~:text=Purpose%20Limitation%3A%20Personal%20data%20should,is%20incompatible%20with%20those%20purposes.

[liii] Regulation 34 (i) Data Protection (General) Regulations, 2021

[liv]Principles of Data Protection, available at: https://www.dataprotection.ie/en/individuals/data-protection-basics/principles-data-protection#:~:text=Purpose%20Limitation%3A%20Personal%20data%20should,is%20incompatible%20with%20those%20purposes .

[lv] Regulation 35 (a) Data Protection (General) Regulations, 2021

[lvi] Regulation 35 (d) Data Protection (General) Regulations, 2021

[lvii] Regulation 35 (f) Data Protection (General) Regulations, 2021

[lviii] Privacy: Right to Information, available at: https://privacy.web.cern.ch/right-information

[lix] Regulation 9 (3) (a) (b) (c) Data Protection (General) Regulations, 2021

[lx] Right to Information, Privacy Notice available at: https://advisera.com/eugdpracademy/knowledgebase/8-data-subject-rights-according-to-gdpr/

[lxi] Regulation 9 (4) Data Protection (General) Regulations, 2021

[lxii] Regulation 9 (6) Data Protection (General) Regulations, 2021

[lxiii] Regulation 10 (4) Data Protection (General) Regulations, 2021

[lxiv] Regulation 10 (5) Data Protection (General) Regulations, 2021

[lxv] What are the Data Subject's Rights under the GDPR? Luke Irwin, 10th March 2021.
Available at: https://www.itgovernance.co.uk/blog/what-are-the-data-subject-rights-under-the-gdpr

[lxvi] Regulation 12 (3) (e) Data Protection (General) Regulations, 2021

[lxvii] Section 38 Data Protection Act 2019

[lxviii] Section 51 (2) (a) Data Protection Act 2019

[lxix] Section 51 (2) (b) Data Protection Act 2019

[lxx] Regulation 55 (a) Data Protection (General) Regulations 2021

[lxxi] Regulation 55 (b) Data Protection (General) Regulations 2021

[lxxii] Regulation 56 Data Protection (General) Regulations 2021

[lxxiii] Regulation 57 Data Protection (General) Regulations 2021

[lxxiv] Section 51 (2) (c) Data Protection Act 2019

[lxxv] Section 52 (1) (a) Data Protection Act 2019

[lxxvi] Section 52 (1) (b) Data Protection Act 2019

[lxxvii] Section 56(1) Data Protection Act 2019

[lxxviii] File a Complaint, available: https://www.odpc.go.ke/file-a-complaint/

[lxxix] Regulation 4 (2) (a) (b) & (c) The Data Protection (Complaints Handling and Enforcement) Regulations 2021

[lxxx] Regulation 4 (3) (a) (b) (c) & (d) The Data Protection (Complaints Handling and Enforcement) Regulations 2021

[lxxxi] Section 58 Data Protection Act 2019

[lxxxii] Section 63 Data Protection Act 2019

[lxxxiii] Section 65 (2) Data Protection Act 2019

[lxxxiv] Section 65 (3) Data Protection Act 2019

[lxxxv] Section 64 Data Protection Act 2019

[lxxxvi] How to Block and Report Contacts, available at:
https://faq.whatsapp.com/2798237480402991/?locale=fi_FI

[lxxxvii] Reporting a Privacy Violation, Facebook, available at:

https://www.facebook.com/help/1561472897490627

[lxxxviii] Facebook Privacy Check Up, available at: https://www.facebook.com/help/443357099140264

[lxxxix] Twitter Private Information and Media Policy, available at:
https://help.twitter.com/en/rules-and-policies/personal-information

[xc] Ways to Protect Your Personal Information Online, CHUBB available at: https://www.chubb.com/us-en/individuals-families/resources/6-ways-to-protect-your-personal-information-online.html

[xci] How to Protect Your Privacy Online, Norton, available at: https://us.norton.com/internetsecurity-privacy-protecting-your-privacy-online.html

[xcii] How to Protect Your Privacy Online, Norton, available at: https://us.norton.com/internetsecurity-privacy-protecting-your-privacy-online.html

[xciii] Google Safety Centre, available at: https://safety.google/

KICTANet
The Power of Communities

Email: info@kictanet.orke
Web: www.kictanet.or.ke
Twitter: @kictanet

german cooperation
DEUTSCHE ZUSAMMENARBEIT

Implemented by
giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

DIGITAL TRANSFORMATION CENTER KENYA

Co-funded by EU