# PRIVACY AND CIVIL LIBERTIES

# TOPIC OUTLINE

## 01 Privacy and the Law

- RICA
- POPI Act
- Privacy across the globe?

## 02 Privacy and Technology

- Data Sharing
- Browser Software and Cookies
- Privacy in the cloud
- Paying with your privacy

## 03 Freedom of Expression

## 04 Privacy and Ubuntu

# OBJECTIVES:

- Discuss the philosophical basis for the legal protection of personal privacy.
- Describe the role of data collection in the implementation of pervasive surveillance systems.

# OBJECTIVES:

- Investigate the impact of technological solutions to privacy problems.
- Exhibit awareness of the Legal foundations of privacy protection.

# 01 PRIVACY AND THE LAW

PRIVACY = “*privatus*”

- the state of being free from unauthorized observation.

## Reductionism

One cannot be entitled to a right to privacy because a right to privacy can be reduced to other fundamental issues of property and person.

## Coherentism

Privacy has value as a coherent and fundamental concept, and most individuals recognize it as a useful concept as well.

# CONTINUATION

- Thomson, argues that we should not be looking for a clear definition of privacy, as notions of privacy are derivative.

## Why privacy is important?

- Privacy gives us the power to choose our thoughts and feelings and who we share them with.
- Privacy protects our information we do not want shared publicly (such as health or personal finances).

# CONTINUATION

- Privacy helps protect our physical safety (if our real time location data is private).
- Privacy helps protect us as individuals, and our businesses, against entities we depend on or that are more powerful than us.
- Privacy is tied to Freedom

## CONTINUATION

# Tavani's three views on privacy:

- **Accessibility privacy:** One's physically being let alone, or being free from intrusion into one's physical space.
- **Decisional privacy:** Freedom from interference in one's choices and decisions.
- **Informational privacy:** Control over the flow of one's personal information, including the transfer and exchange of that information.

# PRIVACY AND THE LAW

- Governments has tools that enable them to collect information about civilians.
- The infringement of citizens' privacy by governments may also be done through the cooperation of telecommunications companies.
- They also have methods for dissemination of information in an easy manner. A significant number of these abilities are a result of the existence of the Internet.
- Generally, the reference point for the protection of privacy has been the 1948 Universal Declaration of Human Rights.

# CONTINUATION

- Paveshich V. New England Life Insurance Co, held that the right to privacy has its foundation in natural law and the instinct of nature.

## The foundation for privacy laws in South Africa

- O’Keeffe v Argus Printing and Publishing Co Ltd in 1954, where a journalist objected to the mass publication of her picture for the purpose of advertising, to which she did not consent.

# CONTINUATION

- Develop specific laws around the issue of privacy. The two existing acts are the Regulation of Interception of Communications and Provision of Communication Information Act (RICA) and the Protection of Personal Information (POPI) Act.
- The South African constitution, which was announced in 1996, states that everyone has the right to privacy, which includes the right not to have :

  (1) their person or home searched,
  (2) their property searched
  (3) their possessions seized, or
  (4) the privacy of their communications infringed.

# RICA

*Regulation of Interception of Communications and Provision of Communication Information Act (RICA)* seeks to regulate the interaction of certain communications, the monitoring of certain signals and radio frequency spectrums and the provision of certain communication-related information.

In order to be able to monitor communication the following steps must be taken:

(1) Law enforcement must be in possession of information or evident that electronic communications are being used in the commission of the crime.

# CONTINUATION

(2) They must approach the court and request an “interception direction”. The sitting judge will then decide on the merit of the evident present and will grant or refuse this directive, and

(3) once the interception direction is obtained, it can then be served to the relevant service provider who is then required by law to monitor any communication made by the individual or party concerned and then to forward all surveillance information to the law enforcement agency. Note that the person under surveillance needs not be informed.

# CONTINUATION

RICA provides that all forms of monitoring and interception of communications are unlawful unless the monitoring and interception takes place under one of the recognized exceptions in RICA.

Section 4 of the RICA allows a party to a communication to monitor and intercept the communication if he/she is a party to the communication.

# CONTINUATION

Section 5 allows for interception of any communication under any circumstances, that is, no special motivation or reason is required for it provided the person whose communication is being intercepted has consented to it in writing prior to such interception.

Section 6 contains a so-called “business purpose exception” which involves the interception of “indirect communications in connection with the carrying on of business”.

# POPI ACT

The **Protection of Personal Information Act (PoPI)** sets conditions for how you can process information. It has been signed by the President and is law and is run by the “Information Regulator”. In some sense this is a counterbalance to the Interception Act.

# CONTINUATION…

In South Africa, General Information Protection Principles (GIPP), applies to those who process personal information (generally, anyone with customers, partners or staff who store their personal information in some way)

- Collect only information needed for a specific purpose;
- Apply reasonable security measures to protect information;
- Ensure such security measures are relevant and up-to-date;
- Only hold as much information as needed;

# CONTINUATION…

- Only hold information for as long as it is needed; and
- Allow the subject of the information to view it upon request.
- If information is transferred across borders must ensure compliance with the restrictions in terms of the PoPI Act (similar to EU)
- If information is used for direct marketing the data subject has to give his or her consent or be a customer

# PRIVACY ACROSS THE GLOBE?

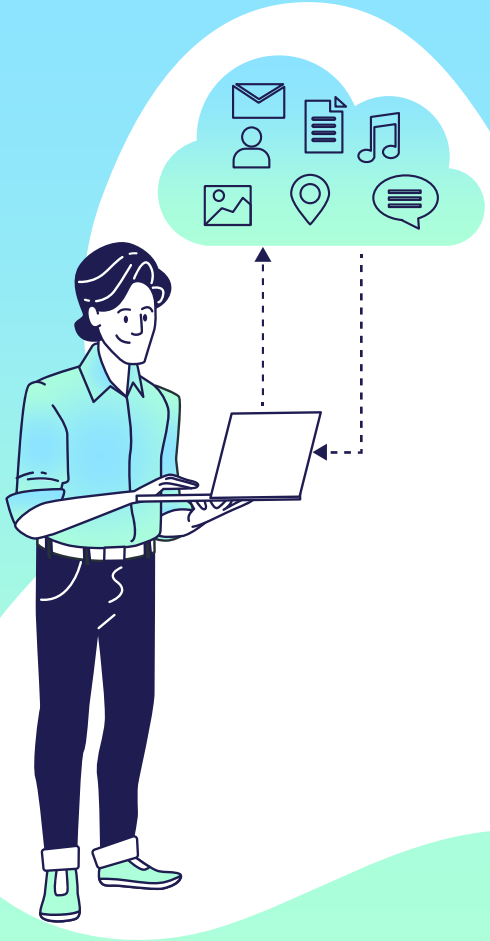
Besides the South African constitution, RICA and the POPI Act, there are other laws on privacy that affects anyone to a greater or lesser extent. A continental view and assessment on data privacy laws in Africa can be found in the collection edited by A.B. Makulilo [72].

# CONTINUATION…

Why consider laws in other countries than the one where you live? The internet is a global network of computers. This causes some issues of jurisdiction of regulations. For instance, your UCT student emails are stored in Microsoft's cloud somewhere in the world, the servers with the actual email storage are probably those located in their data center Dublin in Ireland (part of the European Union), whereas Microsoft as organization is registered in the USA. Whose privacy rules apply? Those from South Africa, Ireland, the EU, or the USA?

02

# PRIVACY AND TECHNOLOGY



The term ***“privacy”*** is used frequently in ordinary language as well as in philosophical, political and legal discussions, yet there is no single definition or analysis or meaning of the term. The concept of privacy has broad historical roots in sociological and anthropological discussions about how extensively it is valued and preserved in various cultures.

# CONTINUATION

Human beings value their privacy and the protection of their personal sphere of life. They value some control over who knows what about them. They certainly do not want their personal information to be accessible to just anyone at any time. But recent advances in information technology threaten privacy and have reduced the amount of control over personal data and open up the possibility of a range of negative consequences as a result of access to personal data.

# DATA SHARING

There are now technologies that enables governments and companies to collect large amount of data, online stores methods tracks the products we buy view and search. This is to improve their services and ads based on personalized data, then the data is often stored and transferred between companies data centers, which makes it possible to intercept the data and use it for other reasons.

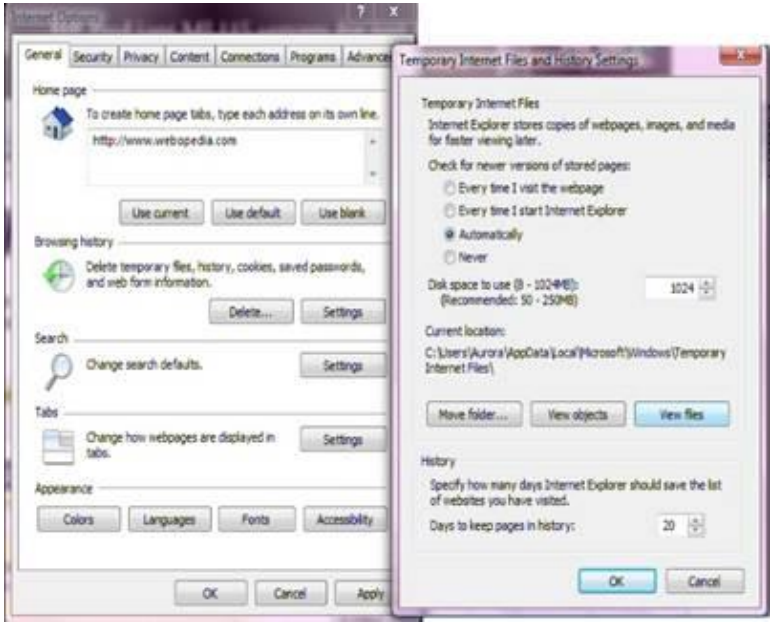
# CONTINUATION

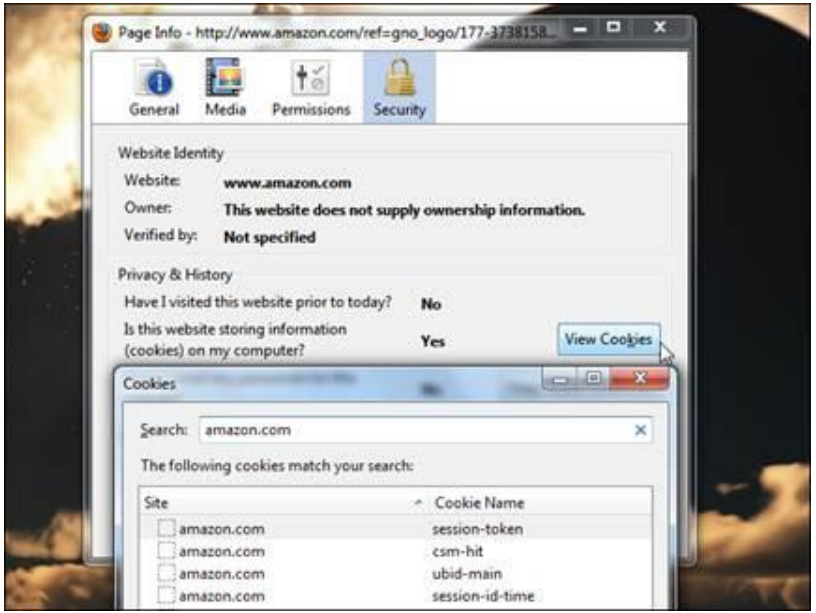
**Surveillance systems** used by governments also has additional ethical problems and can exploit faults in smartphones and other technologies when building modern surveillance systems.

# BROWSER SOFTWARE AND COOKIES

A **cookie** is information that a website puts on a user's computer. Cookies store limited information from a web browser session on a given website that can then be retrieved in the future. Cookies can be accessed by the browser user, the site a user is on or by a third party that might use the information for different purposes. Common use cases for cookies include session management, personalization and tracking. Cookies first appeared in 1994 as part of the Netscape Navigator web browser. They helped the browser understand if a user had already visited a given website.

# CONTINUATION…



# PRIVACY IN THE CLOUD

Data privacy in cloud computing allows collecting, storing, transferring and sharing the data over the cloud without putting the privacy of personal data at a risk. Many times customer even does not have knowledge about how their personal information over the clouds is processed. With the increasing popularity of the cloud, data privacy is becoming a crucial factor in cloud computing**.** Cloud security, also known as cloud computing security, consists of a set of policies, controls, procedures and technologies that work together to protect cloud-based systems, data.

# PAYING WITH YOUR PRIVACY

Many of us have become used to the idea that information and apps from the web are made for free and some used to get good deals and reductions on products in the supermarket. The typical business model is to exploit the data you give them about yourself, so that they can improve advertisement (those advertisers pay those companies) or can sell your data onward to other companies on the data market. Essentially, the currency you pay in for using those ‘free’ services, is data about yourself. Privacy is a piece of your data as valuable as the money they can make from it.

# Do’s

- Be  wary of face-to-face meetings.
- Use a “real” internet service provider for your main account, and to examine their privacy policies and terms of service, as some “free mail” services may have poor privacy track records.
- Keep private data and private Net usage private, at home.
- Good encryption.

# Don’ts

- If you get a spammed advertisement, certainly don’t take the sender upon whatever offer they are making.
- Never submit a credit card number or other highly sensitive personal information without first making sure your connection is secure (encrypted)
- There are other privacy threats besides abusive marketers, nosy bosses, spammers and scammers. Some of the threats include:

  ✓ industrial espionage, government

  ✓Surveillance

  ✓identity theft

  ✓disgruntled former associates, and system crackers.

# 03 FREEDOM OF EXPRESSION

**Your voice matters**. You have the right to say what you think, share information and demand a better world. You also have the **right to agree or disagree** with those in power, and to express these opinions in peaceful protests.

# CONTINUATION…

**Freedom of expression** is a class of rights that exists so that individuals are able to make their opinions heard, and hear the opinion of others. This freedom is **characteristic of democracies**. It generally extends to numerous forms of expression. Films, books, expressions by actions such as vigils, burning a flag, etc. are all generally protected.

# CONTINUATION…

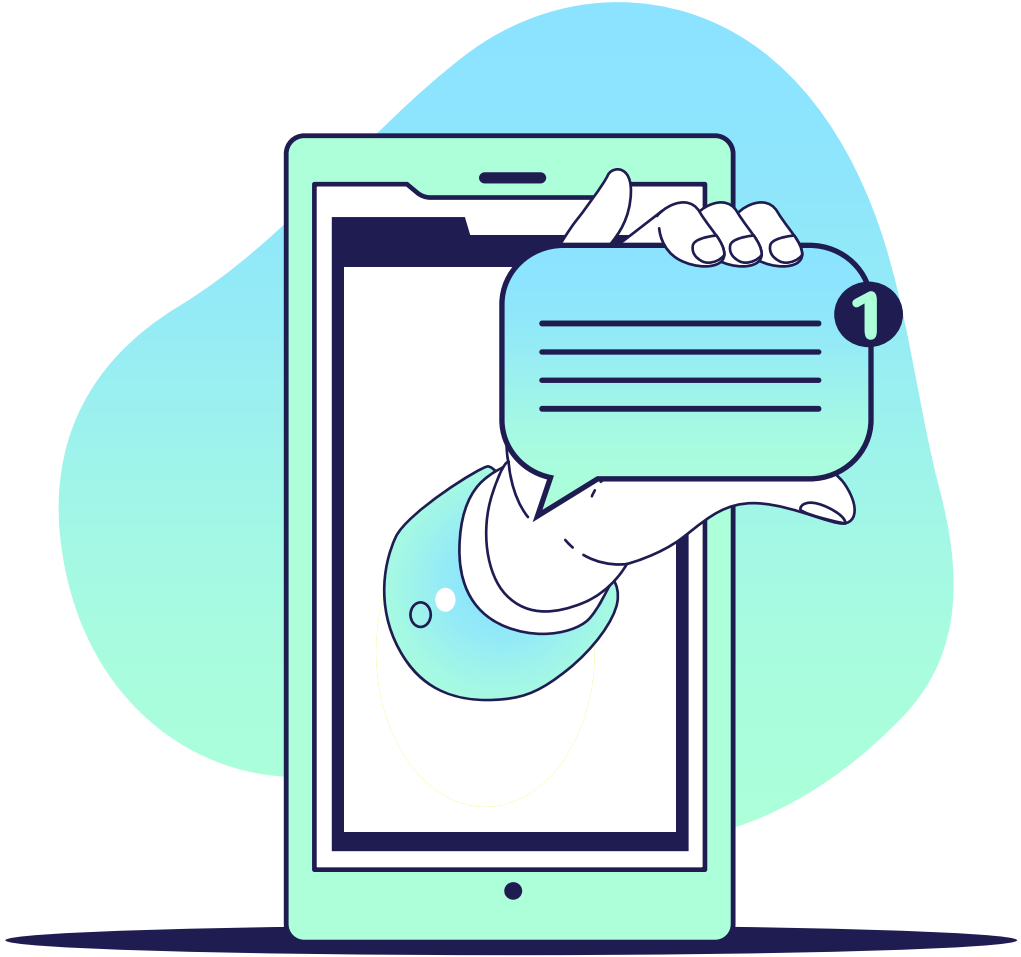
**Expression** can also be offensive, and may result in reputational injury, etc. and examples are that denying the Holocaust is a crime in Germany, one should not insult the Dutch King in the Netherlands, and some presidents of countries are not to be defamed. These are among the reasons why freedom of expression has limitations. Generally, its limitations are for **preventing the infringing of other important rights.**


04
PRIVACY
AND
UBUNTU

- Ubuntu is a broader community-based mindset, whereas privacy arises in a tradition with a strong emphasis on the rights of the individual in order to protect and empower them.
- Ubuntu has less of a concept of privacy — leaves a vacuum in this regard. At the same at the core of privacy is the call to protect dignity, which is in harmony with ubuntu.

# THANKS!





# REPORTERS

- ENANOR, JAYVA P.
- DE LEON, LAIZA
- DAWAMI, HESAM
- GASPAR, SHEILA
- FLORES, JOSHUA
- CHAN, PHILIP LEANDER
- LAYSAM, KENNETH LOUIE