

BELGIUM CAMPUS – ETH271

# IT LAW AND ETHICS





“

*Saying you don't need privacy because you have nothing to hide,  
is like saying you don't need freedom of speech because you  
have nothing to say.*

—

Edward Snowden

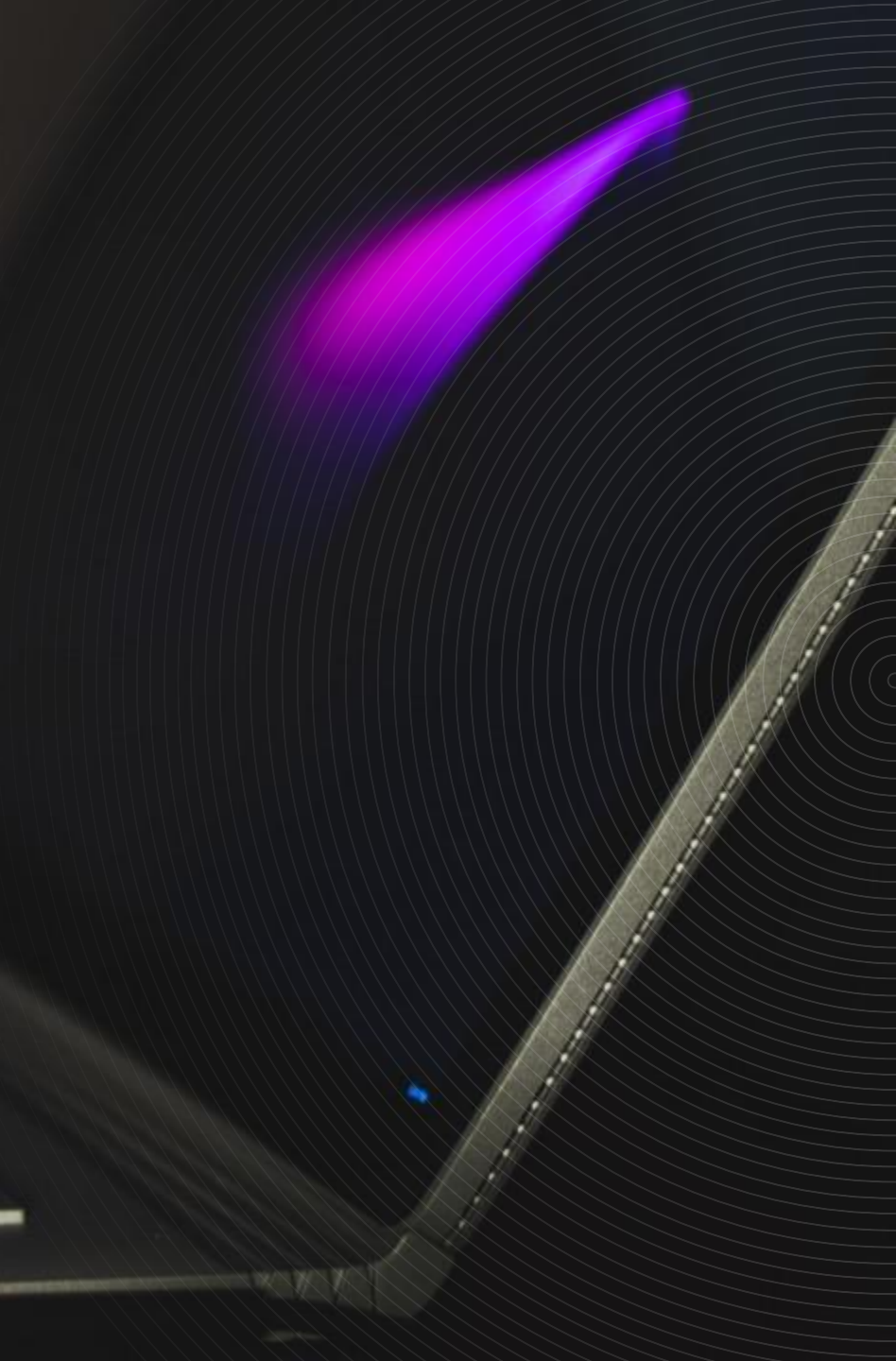
# Data privacy


---

## What information about you, would you consider private?

Data privacy is about access, use, collection of data, and the data subject's legal right to the data. This is further covered by:

- Freedom from unauthorized access to private data
- Inappropriate use of data
- Accuracy and completeness of a person's data
- Availability of data to the data subject
- The right to inspect, update, and correct this data.






ETHICS

There is no such thing as  
privacy on the internet...?

---

The background of the slide features a dark, low-key photograph of a laptop. The laptop is open, and its keyboard is visible in the lower-left foreground. A bright purple light source, possibly a screen or a light effect, is located in the upper-right area, casting a glow. Concentric white circles emanate from this light source, creating a ripple effect across the right side of the image. The overall mood is technological and mysterious.

ETHICS

# What can companies do to improve data privacy?

---





ETH271

# Achieving data privacy

---

There are three main ways to achieve data privacy. The main challenge with these is that, since cultures are so different, these are not internationally standardized. Yet.

1. Technical – using software and hardware to safeguard data.
2. Social – raising awareness among the internet userbase and the policy makers.
3. Regulatory – complying with regulations such as the GDPR or the Hong Kong regulations.

ETHICS

Should a country be allowed to  
spy on its citizens in the  
interest of safety?

---



## ETHICS

# THE NSA

---

The National Security Agency is an intelligence agency of the US government. They have a comprehensive telecommunications network capable of monitoring billions of emails and phone calls. They are continuing research on breaking AES encryption efficiently. In 2005 an article in the New York Times revealed that President Bush had authorized the NSA to conduct warrantless eavesdropping on thousands of Americans since 2002.

“

How far can the government go to protect national security?



ETHICS

# Why are websites asking you to accept cookies?



## ETHICS

# The GDPR

---

The General Data Protection Regulation is an EU law that is enforceable since May 2018. You may recall a period during which most websites asked you to accept a new privacy policy.

The GDPR is an EU law on data protection and privacy for all individual citizens of the EU. It also addresses transfer of data outside the EU. The aim of this is to shift power to the consumer. The GDPR focuses on ensuring that users **know, understand, and consent** to the data collected about them.

Under GDPR, pages of fine print won't suffice, neither will forcing users to click yes to sign up. Companies have to be clear and concise about what will be collected and why and also whether this data will be used to create profiles based on people's behaviour and habits.

For example, a social network has to comply to a user request to delete photos of them as a minor and must inform other websites and search engines that the photos must be removed. A ride-sharing app may ask your name, address, and credit card number, but cannot ask your race, political affiliation, religion, or sexual orientation.



## ETHICS

# Privacy in South Africa

---

The South African constitution states that we all have the right to privacy. This is an incredibly broad statement though, and with the advent of the Internet it has become much more difficult to describe.

The right to privacy is also mentioned in the Universal Declaration on Human Rights.

According to the South African constitution, everyone has the right to privacy, which includes the right not to have -

- their person or home searched;
- their property searched;
- their possessions seized;
- the privacy of their communications infringed.

## ETHICS

# Data protection in South Africa

---

The South African constitution states that we all have the right to privacy. This is an incredibly broad statement though, and with the advent of the Internet it has become much more difficult to describe.

The right to privacy is also mentioned in the Universal Declaration on Human Rights.

When it comes to privacy of data, we have the POPI Act. The Protection of Personal Information Act is essentially the South African Data Protection Bill or Data Protection Act.

It addresses a variety of communications including the processing of personal information, consent, and direct marketing.

The definition of processing is also quite broad and includes collection, recording, and use.



01

Personal information must be obtained in a lawful and fair manner.

02

The information can only be used for the specified purpose it was originally obtained for.

03

Processing may not be done for purposes beyond the original scope that was agreed to by the data subject.

ETHICS

## The eight principles of the POPI Act.

---

04

The person who processes the information must ensure that the information is complete, not misleading, up to date and accurate.

05

There should be open communication between the information regulator and the data subject.

06

The person processing the data is accountable to ensure that the measures that give effect to these principles are complied with when processing personal information.

ETHICS

## The eight principles of the POPI Act.

---

07

The data subject must be able to participate. The data subject must be able to access the personal information that a responsible party has on them and must be able to correct the information.

08

The person processing data must ensure that the proper security safeguards and measures to safeguard against loss, damage, destruction and unauthorised or unlawful access or processing of the information, has been put in place.

ETHICS

## The eight principles of the POPI Act.

---



## ETHICS

# Accessing your communication info

South Africa's main communications surveillance law is known as RICA. This act deals with protecting the constitutional right to privacy. It also limits the circumstances under which the act is limited. For example, this act does not prohibit your employer from checking your emails, but this type of monitoring must abide by the rules set out by RICA.

Rica states that, no person may intentionally intercept, attempt to intercept, authorize, or procure any other person to intercept or attempt to intercept at any place, any communication during its occurrence or transmission.

There are exceptions:

1. If you are a part of the conversation
2. If there is written consent,
3. If it is necessary for the conduction of business.

There are further restrictions that apply to these as well.

## RICA

Regulation of Interception of Communications and  
Provision of Communications Related Information Act





## ETHICS

# Accessing your financial info

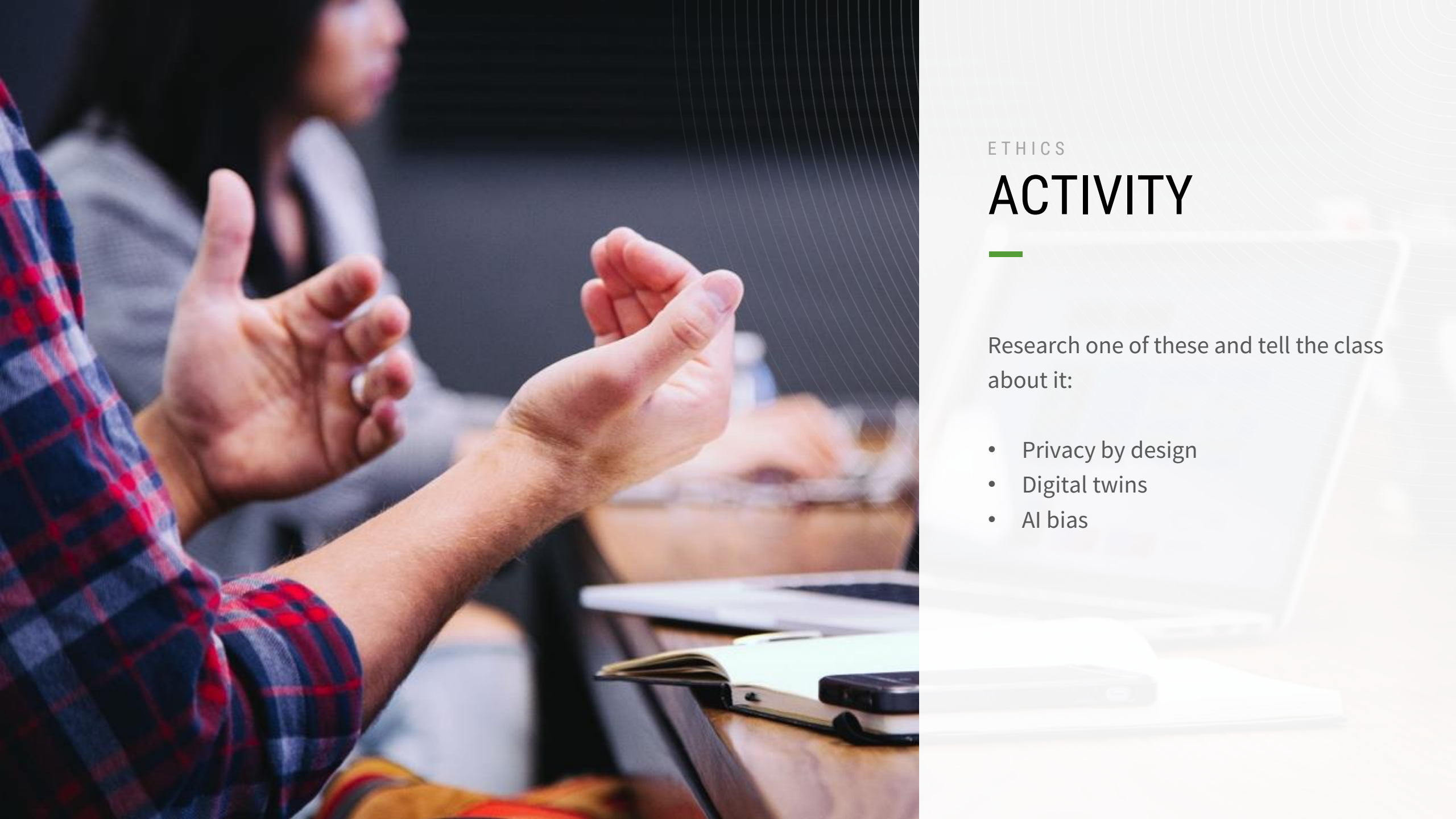
---

In South Africa we have the FICA (Financial Intelligence Centre Act) laws which govern financial information. It was originally created to prevent crimes such as money laundering, tax evasion, and other illegal financial acts. This act also helps protect the citizens' money.

According to FICA, financial institutions must be aware of whom they are dealing with and paper trails of all transactions should be kept.

FICA applies differently depending on which type of business you are in. Some of these include:

- Gambling institutions
- Foreign exchange
- Money lending
- Attorneys and more



ETHICS

# ACTIVITY

---

Research one of these and tell the class about it:

- Privacy by design
- Digital twins
- AI bias



## DIGITAL TWINS



A virtual representation of a product or process. Recently it has been speculated that some companies who already possess large amounts of personal information, could create digital users in order to test marketing.

Digital models of human organs and the human body are being used for research in medical fields as well.

## PRIVACY BY DESIGN



Embedding data privacy into product design and development.

There are 7 principles:

1. Proactive not reactive
2. Privacy is the default
3. Embed privacy into design
4. Retain full functionality
5. Ensure E2E security
6. Maintain visibility and transparency
7. Keep it user-centric

## AI BIAS



AI systems are only as good as the data they are given. Badly chosen data can contain racial, ideological, or gender bias.

A possible solution is to use contractual ethics where machines are taught certain principles and decision-making skills to apply certain values.

# Data breaches

---

Data breaches are sometimes caused by hackers breaking into a database but more often than you think, they are caused by carelessness or failure to follow good security practices.

For example, 26 million records were stolen from the US Veteran's Affairs and none of the information was encrypted. There were several other major breaches such as the PlayStation Network breach in 2011 and the Yahoo breach in 2015 where 500 million accounts were compromised.

An online shoe store named Zappos (a subsidiary of Amazon) had a major data breach where a cybercriminal gained access to names, email addresses, and phone number. They also gained access to encrypted passwords. Zappos immediately emailed all 24 million customers and suggested they change their passwords.





# Data breaches

---

This is the main question: **how soon should affected people be informed that their information has been compromised, if at all?**

According to the GDPR, data breaches only need to be reported if they “pose a risk to the rights and freedoms of natural living persons”. Regardless of whether it needs to be reported, you are still mandated to maintain a record of all breaches

Companies are often tempted to keep quiet about a breach if the possibility exists to remain undiscovered. Breaches can be very harmful to the company reputation and their profits – by some estimates nearly \$200 per record lost. Ethical behaviour, however, requires companies to adhere to policies similar to those posed by the GDPR.



ETHICS

# Data breaches

---

If data from a data breach is available online freely, should researchers be able to use that information?





## ETHICS

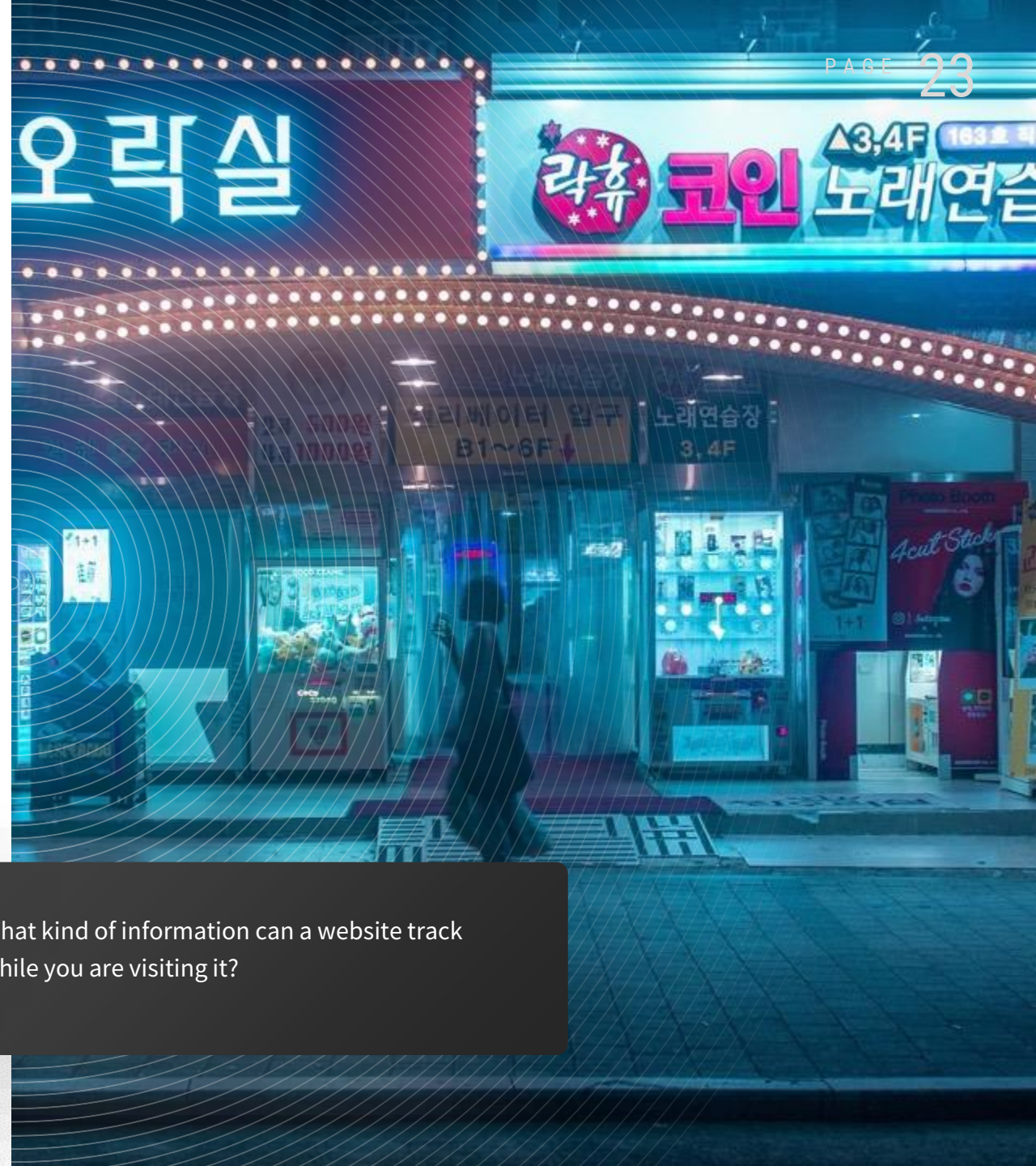
# Consumer profiling

Companies can obtain information about your web activity through [cookies](#) – text files that are stored on a user's computer so that users can be identified on subsequent visits.

From these cookies, a website can tailor the ads and promotions presented to you. Some types of cookies can also track what other sites a user has visited, allowing marketers to use that data to make educated guesses about suitable ads. Since the EU privacy laws came into place, websites are required to ask permission before storing cookies on your device.

“

What kind of information can a website track while you are visiting it?





## ETHICS

# Consumer profiling

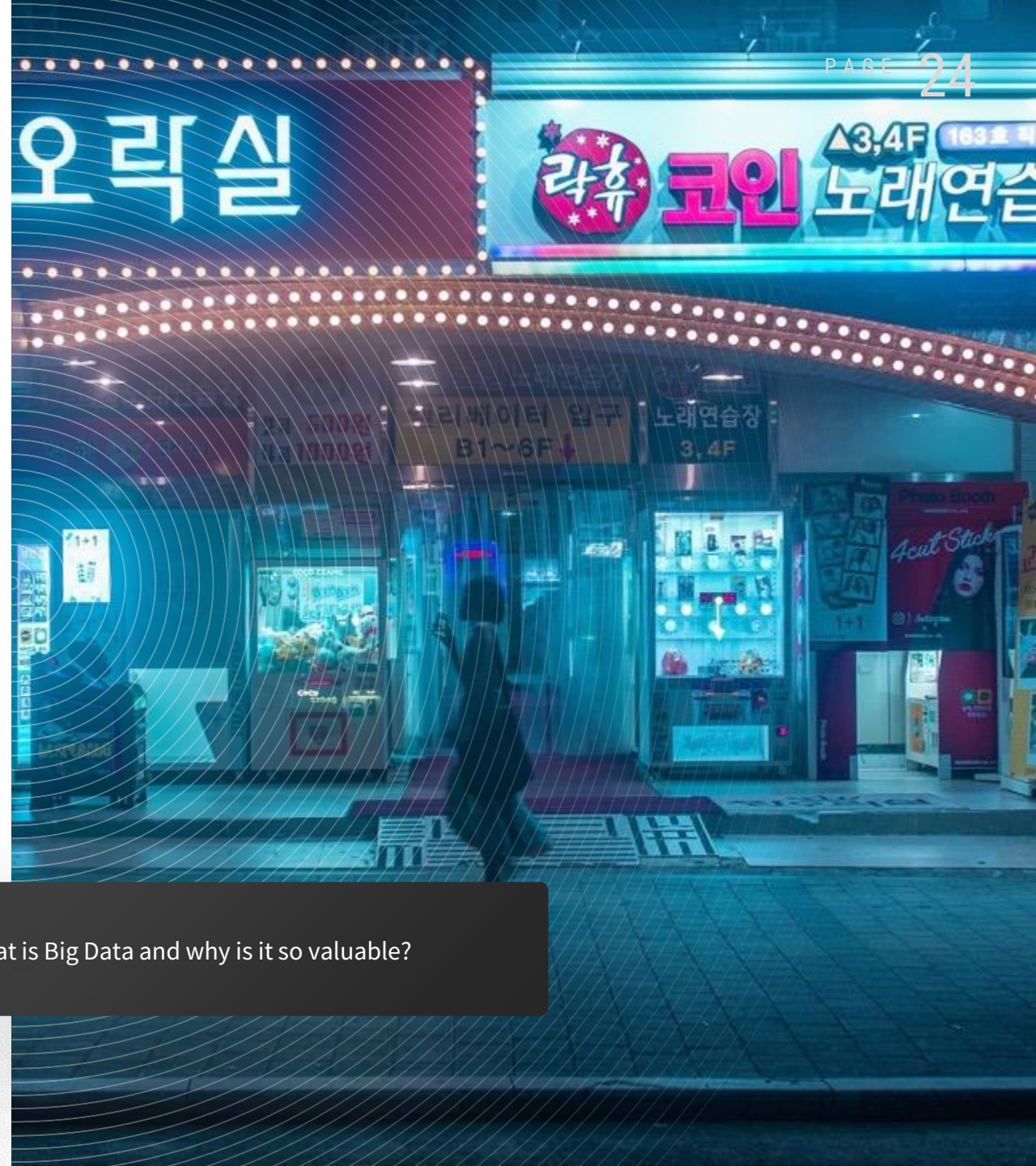
---

Browsing with cookies is anonymous as long as the data is not linked with personal information. Online marketers cannot capture personal information, such as names or addresses unless people provide them. But sometimes, if you volunteer some personal information, it can be used to find additional information you might not want to share.

[Consumer data privacy](#) is a major marketing issue with Big Data being a large part of technological analysis and research. The concerns here are, of course, that data might be sold to other companies and the consumer then has no way of knowing who is using it or how it is being used.

“

What is Big Data and why is it so valuable?





## ETHICS

# Oh Facebook

---

Facebook is one of the biggest culprits in playing fast and loose with consumer data. In April 2018, Facebook's Chief Technology Officer Mike Schroepfer said he believes most users on Facebook could have had their public profile data harvested by third parties through contact information. An interesting offshoot from this is that consumers do not seem to realise or care when their personal data is shared as long as they do not experience any material loss.

After the Cambridge Analytica story Facebook lost about 2.8 million U.S. users under age 25 last year, but it still boasts more than 1 billion daily active users.

“

How do you feel about your information being shared if it does not have any negative impact on you?



# Your data online

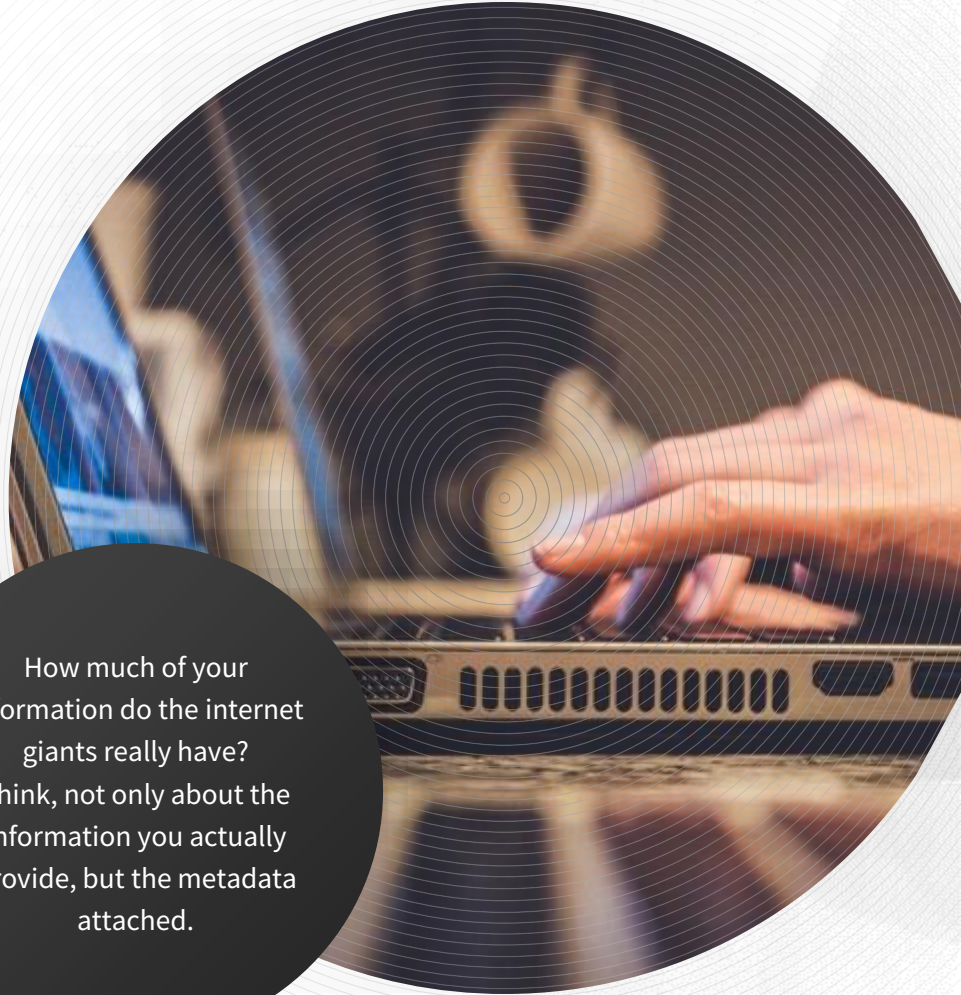
---

## We often do not realise how much of our data is being stored.

Google is one of the largest internet companies. In April 2014, Google confirmed that they go through your personal content to provide you with customized search results. This includes the actual content of your emails. Would you rather refuse such tailored results if it meant your personal information was compromised?

In 2010 a man named Max Schrems sent an email to Facebook for all his information. Facebook, surprisingly, responded with a PDF file of 1200 pages that contained even deleted messages, locations (which were not specified on Facebook), and an assumed list of best friends.

This is all specified in the terms and conditions but is it ethical to expect people to dig through all the legalese?



How much of your information do the internet giants really have? Think, not only about the information you actually provide, but the metadata attached.



## ETHICS

# Workplace monitoring

---

A study by Welch et al revealed that between 60 and 80 percent of employees go online for non-work related matters. Another source says that workers spend on average four or five hours per week online on personal matters. This leads to some companies blocking websites such as Twitter or Facebook.

The potential for decreased productivity has caused some employers to monitor internet usage of their employees. With a few exceptions, this is perfectly legal as long as employees were informed of such monitoring taking place.

“

Should a company be allowed to track its employees' internet usage? Or should certain sites rather be blocked outright?





## ETHICS

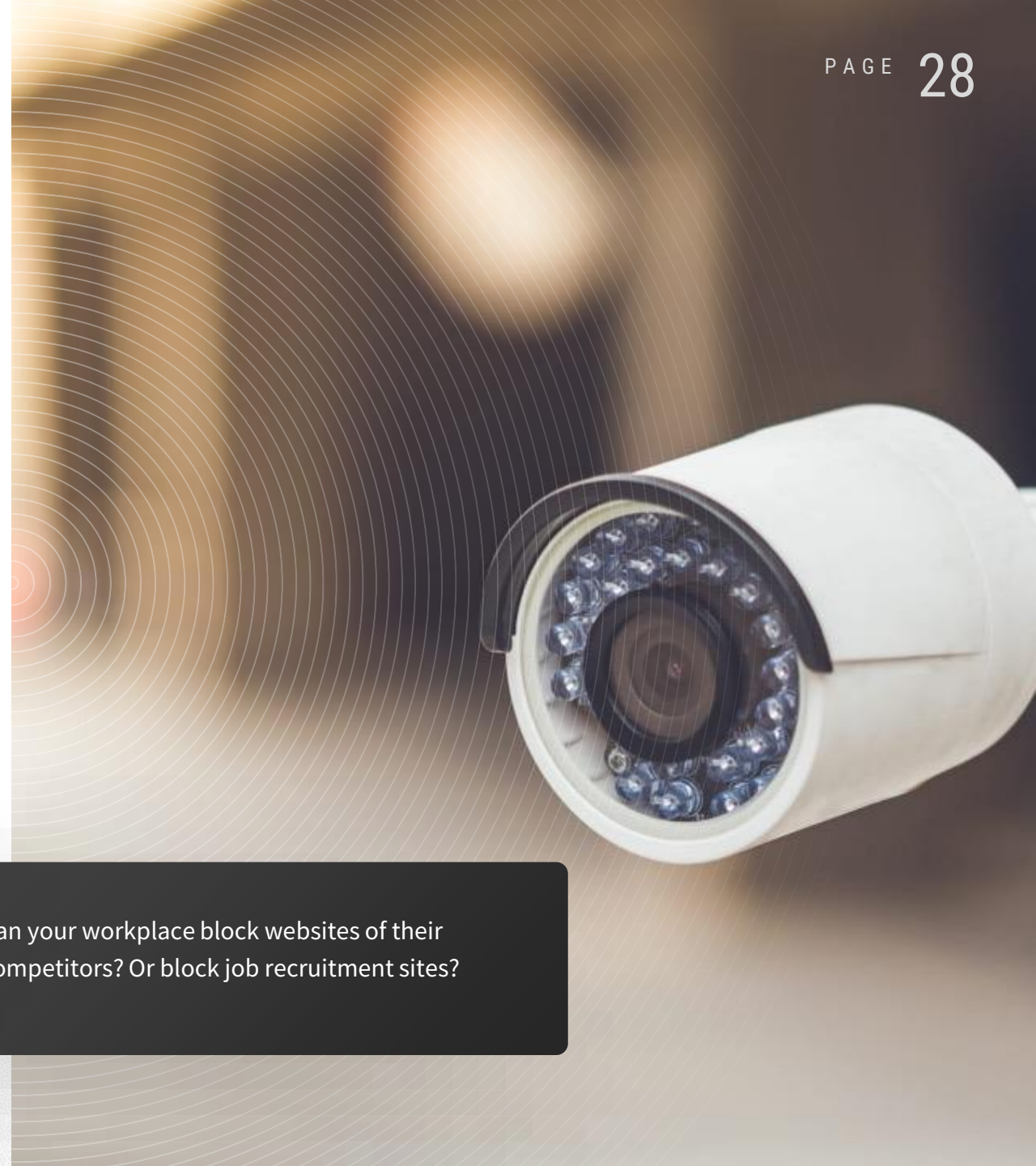
# Workplace monitoring

Preventing legal issues when monitoring

1. Explicit monitoring
2. Goal of monitoring
3. No personal data monitoring
4. Corporate property application
5. No content or keystrokes monitoring

“

Can your workplace block websites of their competitors? Or block job recruitment sites?





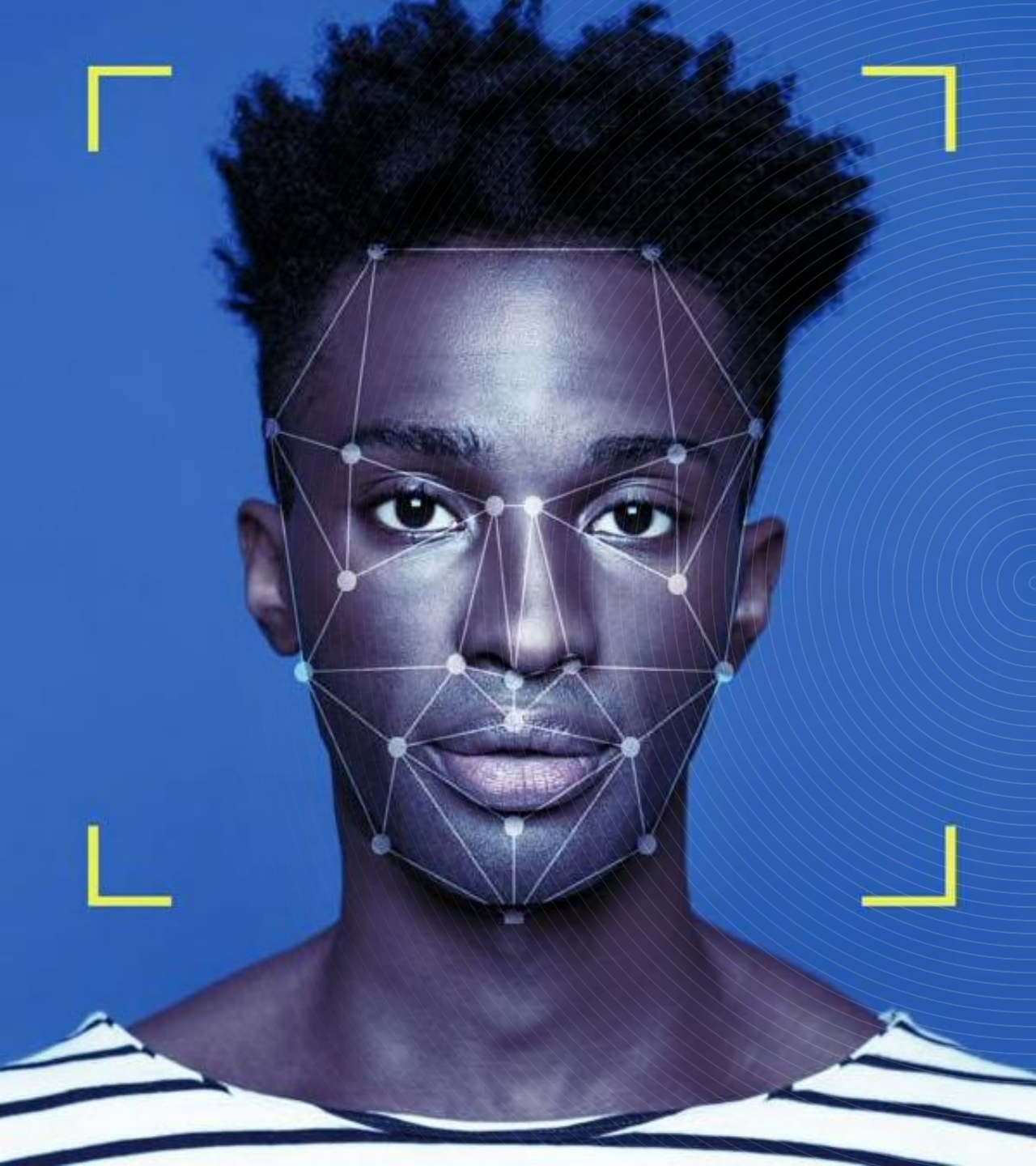


ETH271

# Facial recognition

---





ETH271

# Facial recognition

---

Facial recognition is one of the biometric technologies that are becoming increasingly common.

When it comes to public safety, however, the technology has had a tentative roll-out. Only China has widely deployed facial recognition, which debuted in train stations during the Lunar New Year high season. Some nations, such as Japan, plan to use the technology for high profile occasions, like the Olympics or other major sporting events. There have been two major ethical concerns: development bias and facial recognition ethics of use.



# 01

ETH271

## Ethical issues

---

### Development bias

Obviously, the technology needs to be developed first before it can be used. However, facial recognition uses machine learning which requires massive amounts of data to refine and perfect the algorithm. Unfortunately, these datasets are quite limited in their diversity.

Middle-aged, Caucasian men are overrepresented which could cause false matches with people of colour, women, the elderly, and persons with disability. Countries where the majority of people are a specific ethnicity could cause the minority to be unfairly treated.





## Ethics of use

Issues have arisen in areas of necessity, complicity, bias, accountability, and supervision. Since this development is still being done standalone by various companies, patchwork development may also lead to a lack of oversight or regulations. There is also the question of, are people able to “opt out” of having their faces being scanned without their permission?

There are also concerns with privacy. Who will own facial image data? How will criminal and civil departments share this data? How will this data be handled across borders? Will this data be securely stored? What are the dangers of this data leaking due to a malicious attack?

02

ETH271

## Ethical issues

---



# WHAT WOULD YOU DO?

---

Your friend is going through a tough time with his current significant other and believes they are cheating. He is aware of your technical prowess and has asked you to help him purchase and install a stalking app on her phone.

What would you say?