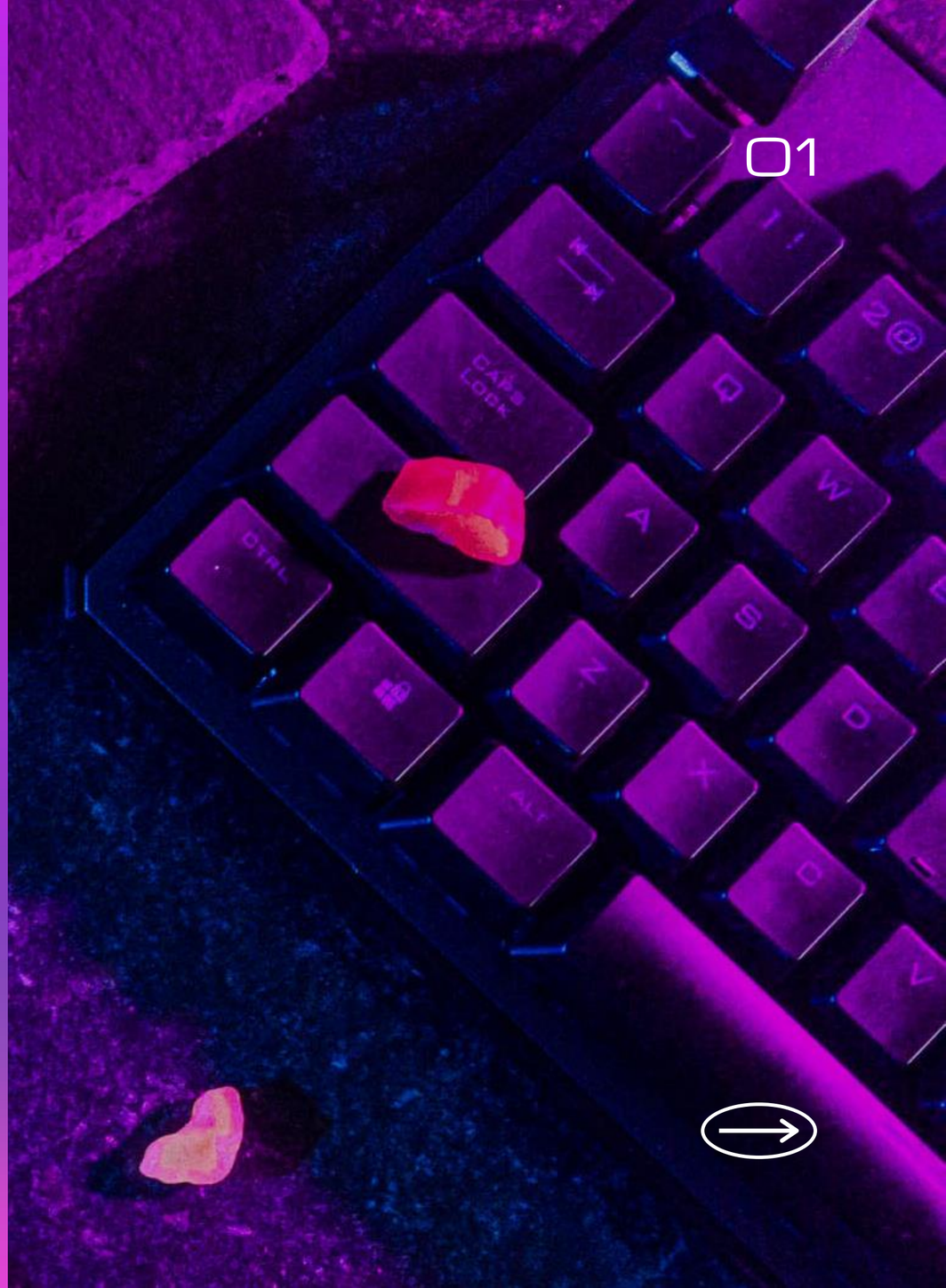
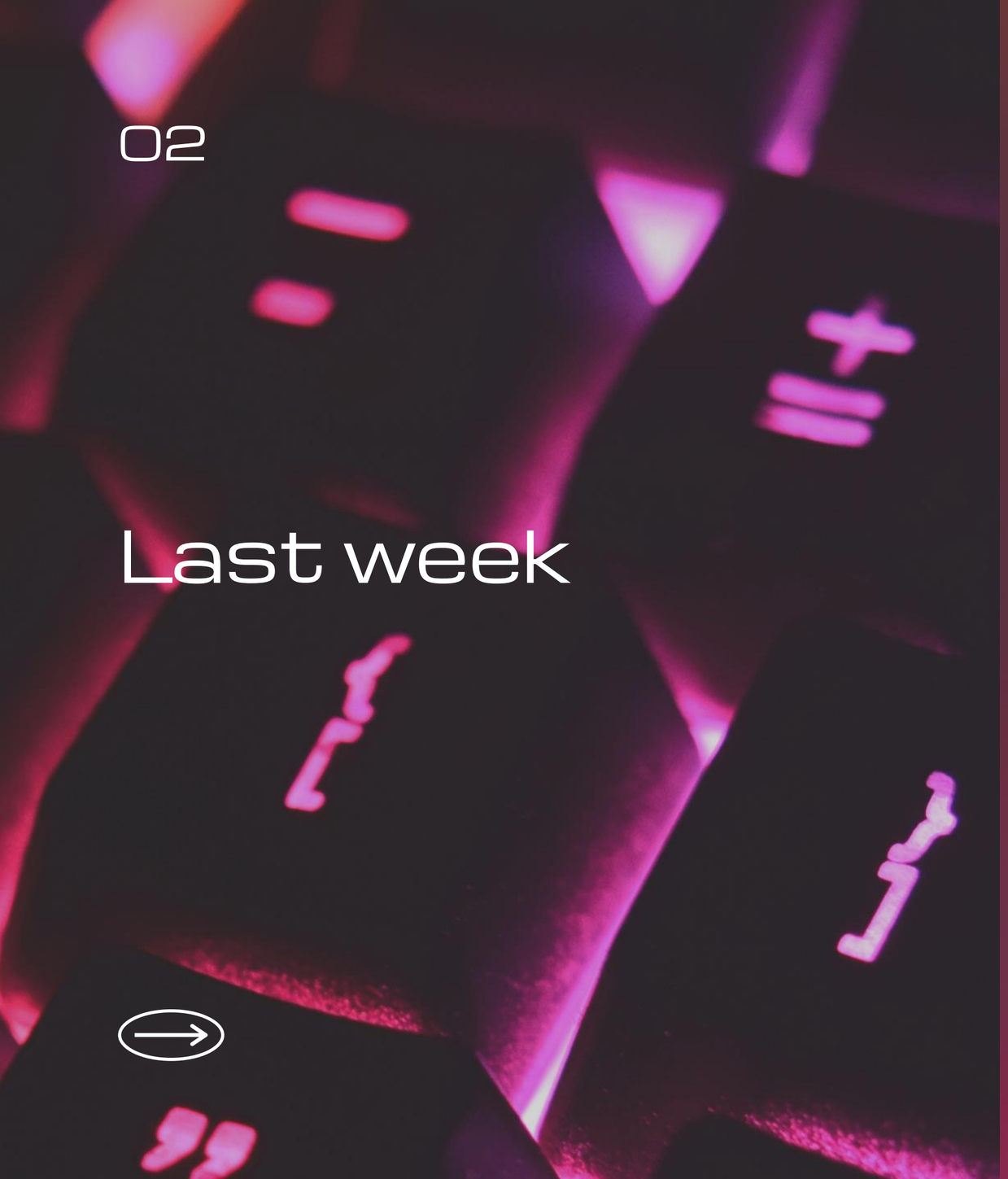
CRIM20007: CYBERCRIME & DIGITAL CRIMINOLOGY

01

Algorithms, race & power

Algorithmic bias and inequality





02

Last week

CRIME CAUSATION THEORIES

Routine activity theory, subcultural theory, social learning theory and the general theory of crime

INNOVATIVE THEORIES OF CYBERCRIME

Cultural criminology, the philosophy of information and actor network theory

THE 'ONLIFE'

Onlife implications for harm and victimhood

03

This week

PART 1: BLACK CYBERCULTURES AND AFROFUTURISM

Web browsers as racial technology

PART 2: RACISM AND TECHNOLOGY

Algorithms and machine learning-facilitated bias

PART 3: DECOLONISATION AND DIGITAL SPACE

Data sovereignty and decolonising the Internet

PART 4: CYBERCRIMINOLOGY, DIGITAL CRIMINOLOGY AND RACE

Critiques and challenges for theorising digital harms

Black cybercultures

'Reflexivity has never been the benchmark for information technology industries; instead, these institutions focus on instrumental outcomes of “improving” computers and code, burying their cultural influences behind technical protocols and limited imaginiaries about users who are not themselves.'
(Brock, 2020: 28)

Culture to cyberculture

Brock (2020: 6) distinguishes between Black culture online and Black cyberculture

Black cyberculture: what does Blackness mean for technology use and design?

An informational identity premised on:
- Libidinal online expressions and practices of joy and catharsis about being black
- Expressed through semiotic and material relationships (Brock, 2020: 7)

Afrofuturism

Afrofuturism is a cultural theory/aesthetic that comments upon the intersections of black experience and technology.

Nelson (2002) “African American voices, with other stories to tell about culture, technology, and things to come.”

Brock (2020) warns that this perspective can come across as ‘utopian sentiments.’

Web browsers as racial technology

sexism:the idea that one gender is smarter/better than the other

Example that sexism are part of architecture and language of tech the iphone screen is too large and female fingers are not long enough to touch the whole screen. Multiple phone sizes should be produced

06

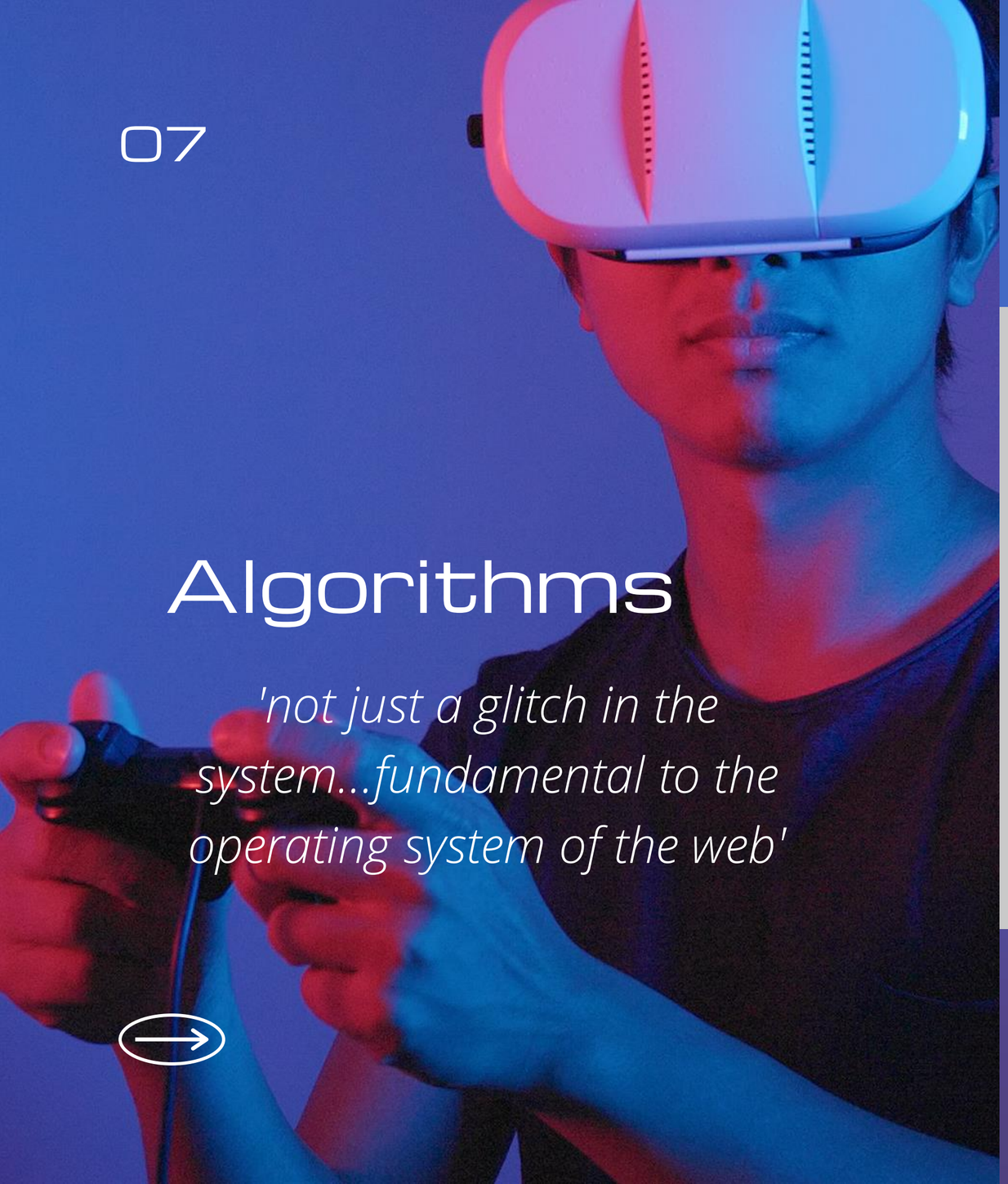
'These human and machine errors are not without consequence, and there are several cases that demonstrate how racism and sexism are part of the architecture and language of technology and issue that needs attention and remediation'
Noble, 2018: 9

RACISM AND TECHNOLOGY

07

Algorithms

'not just a glitch in the system...fundamental to the operating system of the web'



08

Algorithm has its functional ways in perpetuating sexism and racism online.

- example that algorithm /tech produces racism

some users found that the posts relating to Black Live Matters have lower interactions, possible hidden from explore on Insta/Tick Tok).
- recruitment Algorithm has racial bias (its facial recognition assumed that ppl with fair skin tone (white ppl) are more trustworthy than black ppl).
- Racist Stereotypes coming from web searches. (Search for "beautiful", "successful" on Google and it is interesting to see stereotypes Google give you).

Algorithms

'not just a glitch in the system...fundamental to the operating system of the web'

POWER IN DIGITAL SOCIETY

Algorithms are one tool that shape digital society to mirror terrestrial society in terms of racism, sexism and classism (Noble, 2018).

Algorithm follows the human guidance and humans are imperfect in their behaviours (they can be racist, discriminate women)

TECHNOLOGICAL REDLINING

The digital decisions of algorithms reinforce oppressive social relationships, and allow for racial profiling

Mathematical formulations that shape algorithms are ultimately designed by human beings.

ALGORITHMIC OPPRESSION

Noble (2018) highlights how earlier iterations of Google’s algorithm presents a fetishization of women of colour.

09

Racial surveillance

Simone Browne, Dark Matters (2015)

Technology is increasingly used as a tool of surveillance.

Browne argues that this technology is deployed differently against people of colour – particularly through biometric technologies that assert a ‘prototypical whiteness’.

Canella (2018): the way that the state surveils black activists participating in Black Lives Matter is not necessarily ‘new’, “they have simply taken new forms.”

Go to menti.com

Use the code 1143 8532

Decolonising the Internet

Who's knowledge? Who's Internet?

TECHNOLOGY COLONIALISM by Anjuan Simmons

'If Silicon Valley is allowed to become the central repository of information about people around the world, then there is a danger of setting up a form of imperialism based on personal data. Just as the royal powers of old reached far into the lives of distant colonized people, technology companies gain immense control with every terabyte of personal data they store and analyse'

Data sovereignty

Data sovereignty is a growing discipline that posits that Indigenous people have inherent and inalienable rights relating to the collection, ownership and application of data about them, and about their lifeways and territories

What does data sovereignty look like online and in the face of algorithmic oppression? Control over health data, compliance choice with government websites, apps and surveillance, oversight on projects that utilise the data of Indigenous communities.

See Kukutai, T., & Taylor, J. (2016). Indigenous Data Sovereignty: Toward an Agenda. ANU Press.

Cybercrime and race

EMPIRICAL LIMITATIONS

A lot of cybercrime research is quantitative and uses crime causation theories that have been critiqued as highly limited (such as routine activities theory) (see Yar, 2005).

The result is these kinds of statements in research:
Holt and Bossler (2009: 16) “our model indicates that race, age, and employment do not appear to act as indicators of target attractiveness for online harassment.”

LIMITED SCOPE

Cybercriminology has (for the most part) failed to see race or acknowledge any relevance.

PROMOTES DAMAGING STEREOTYPES

Hackers are “rebels” (Furnell, 2002)

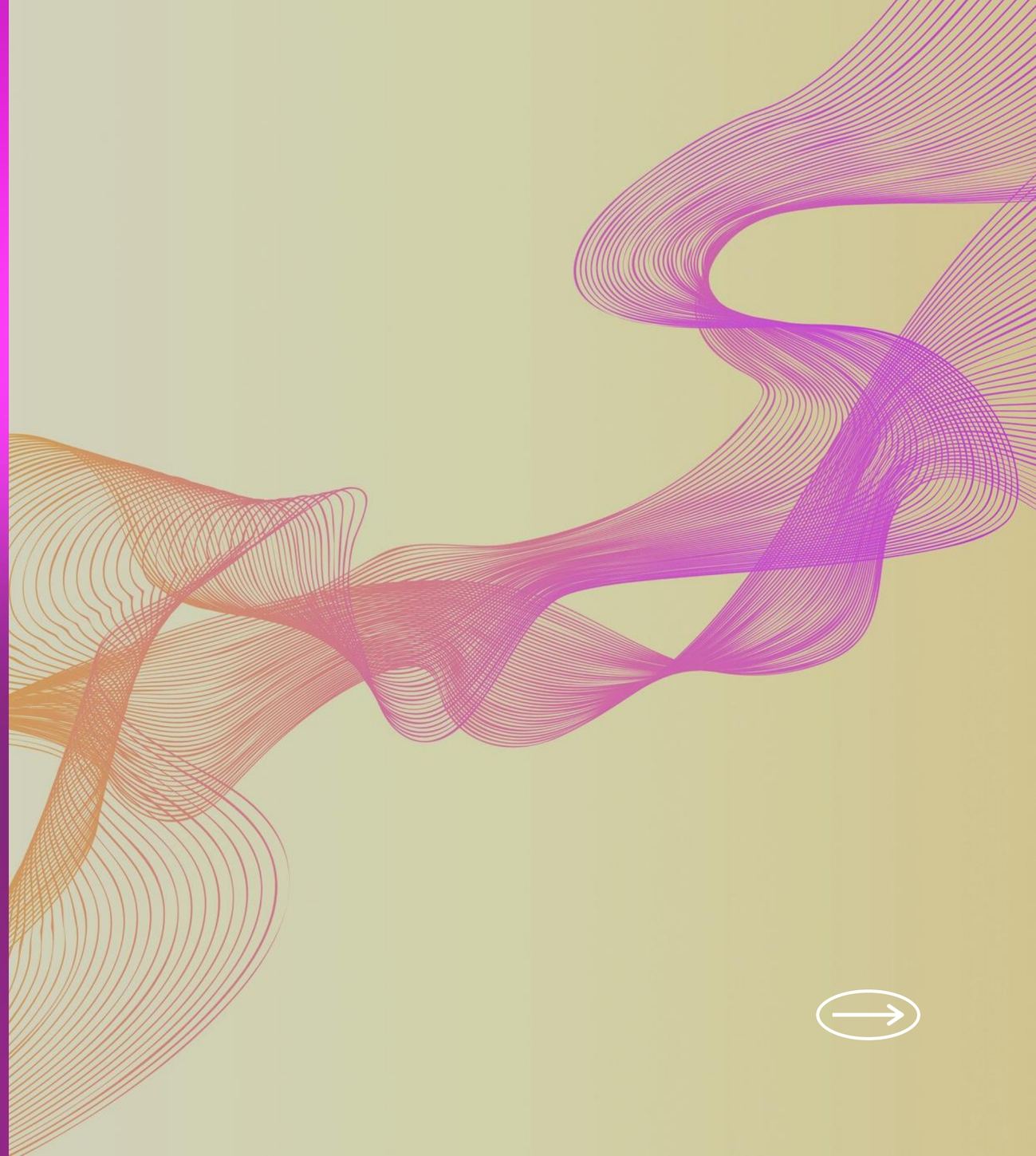
Cyberterrorists are “dangerous” (Wykes and Harcus, 2010)

Digital criminology and race

Largely empirical as well, digital criminology has so far been limited in incorporating critical race theory or scholarship into analyses of digital society.

Digital life is an extension of terrestrial life: digital criminology provides a space where analyses of race and cyberculture can more readily apply to cybercrime and digital harm.

Powell Stratton and Cameron (2018) on digital social inequalities between the Global South and the Global North. If access to technology differs in different places, how does this impact participation in digital society?



How to write a policy brief

Assessment #1

What is a policy brief?

A written piece of work that aims to communicate potential policy responses to a general audience and public servants

Policy:

- Includes and extends beyond laws
- Generally includes a program or course of action
- Public Policy – term used to describe government programs
- Bacchi (2009: ix) “there is an underlying assumption that policy is a good thing, that it fixes things up”
- A policy brief, compared to an essay, should have particular outcomes or advice in mind for a ‘problem’ or issue.

1. NEED TO FIGURE OUT WHO IS UR TARGETED AUDIENCE
2. THINK ABOUT WHAT IS THE MISSING CYBER CRIME PROBLEM IN YOUR SPACE ?
FOR EXAMPLE: FOR IMAGE SPACE SEXUAL ABUSE, WHAT IS A KEY PROBLEM PREVENTING THIS ISSUE FROM STANDING OUT ?

Purpose

To communicate the ***practical implications of research*** to a specific audience. Therefore, should be research-based, but not necessarily theory-based

- To assist readers in making a decision about a ‘problem’
- Will often relate to findings in contemporary policy debates

For example: if you are discussing drug cryptomarkets, then your policy will likely also refer to broader drug policy approaches

•While an essay should present research into an argument, a policy brief should synthesize research to present outcomes

Style and audience

Tone: clear language and avoiding unnecessary jargon is crucial in writing a policy brief

- Direct language
- Active voice rather than passive voice
- Formal, but not ‘academic’

PASSIVE VOICE: IT COULD BE SEEN RESEARCH SUGGEST

ACTIVE/DIRECT VOICE: RESEARCH INDICATES THAT

Format: tends to be more segmented than a traditional essay

- Might include these sections – title, executive summary, context or scope of the ‘problem’, policy alternatives and recommendations, reference list.
- Audience: policy makers, public servant, general readers, stakeholders (ie: not academic!)

IT IS VERY IMPORTANT THAT IN THE INTRODUCTION OF YOUR ESSAY, YOU SPECIFY WHO YOUR STAKEHOLDERS ARE.

What about theory?

While you can use theory to inform your policy brief, **it should be more in the background to the empirical research** that you present.

Some theories will be more appropriate than others

Think about theories that present outcomes in more specific ways

Although you are welcome to use an idea like Floridi's infra-ethics, ***how*** does this relate to specific policy outcomes?

Important to apply theory/concepts in a tangible way

Suggested format

- Title

- **Executive summary:** two to three sentences summing up the entire brief (50-75 words).

Summarizes the topic you are looking at, your stakeholders , a very brief summary of the recommendations you are going to outline.

- **Introduction:** explain the policy issue and why it is particularly important or current (200-300 words).

- **Research and evidence:** provide details from literature/articles, government reports, on the problem (750-850 words).

- How the cyber problem has emerged,
- Any Past / present policies have been performed.
- Evaluate whether those policies are successful or failed
- Include statistics to talk about the scale of the problem.
- Stakeholder can be government/organisations who are capable of bringing your policy into effects (dont need to limit to Australian context,).
- make sure your source is respectable
- need to make sure the evidence you provide in "Research And Evidence" related to your recommendations.
- For evidence, search on unimelb library for academic articles.
- in-text citation: Harvard

- **Policy recommendations:** discuss and justify your reasons for how the problem(s) should be addressed (600-700 words).

- **Conclusions:** reinforce the key message to take away from the policy brief (250-350 words).

You need to specify how your stakeholder can bring your recommendations will into effect .
You need to explain that ur key stakeholders have to take action urgently or within the certain timeframe, ...

- Be creative , are there any ways that technology can get involved to address your chosen cybercrime problem ? Are there ways that social media/network can review usage of users to resolve harrassment on their sites ?
- Your recommendations need to be explained in great detail, what new changes you have, why do you think it is effective
- limited to 2 (deep over broad)
- your recommendations dont have to be realistic to the real world.
- if u bring up a short-term solution, u need to say why it is a short-term

REFERENCES

- Bossler, A. M., & Holt, T. J. (2009). On-line activities, guardianship, and malware infection: An examination of routine activities theory. International Journal of Cyber Criminology, 3(1).
- Brock, A., & Brock, J. A. (2020). Distributed blackness. New York University Press.
- Browne, S. (2015). Dark Matters. Duke University Press.
- Canella, G. (2018). Racialized surveillance: Activist media and the policing of Black bodies. Communication Culture & Critique, 11(3), 378-398.
- Furnell, S. (2002). Cybercrime: Vandalizing the information society (pp. 3-540). London: Addison-Wesley.
- Kukutai, T., & Taylor, J. (2016). Indigenous Data Sovereignty: Toward an Agenda. ANU Press.
- Nelson, A. (2002). Introduction: Future Texts. Social Text, 20(2), 1-15.
- Noble, S. U. (2018). Algorithms of Oppression. New York University Press.
- Powell, A., Stratton, G., & Cameron, R. (2018). Digital criminology: Crime and justice in digital society. Routledge.
- Simmons, A. (2015). Technology Colonialism. Model View Culture, 27.
- Wykes, M. & Harcus, D. (2010). Cyber-terror: construction, criminalisation and control. In Y. Jewkes & M. Yar (Eds.), Handbook of Internet Crimes (pp. 214 - 229). Cullumpton: Willan Publishing.