

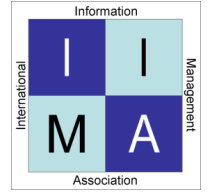
Keynote IIMA 2023: Tensions Between A Sustainable Technology- driven World And Today's Digital Utopia- Dystopia...

IIMA 2023 Lunch Keynote

Anand Sheombar

email: anand.sheombar@hu.nl

HU University of Applied Sciences Utrecht, The Netherlands



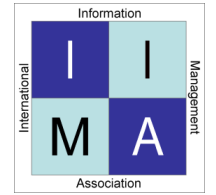
**IIMA 2023 Conference
Information Security, Business
Intelligence, and Technology
Innovations: Advancing with
confidence towards a sustainable
technology-driven world
October 23 – 25, 2023 Las Vegas**



Keynote abstract

Lunch – Keynote 23 October

Tensions between a sustainable technology-driven world and today's digital dystopia...



The keynote addresses the tensions we face in today's digital world where dis/misinformation, aka 'fake news' and cyber-surveillance, are present.

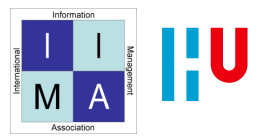
Drawing from examples of research projects on online hate speech in Europe and globally, and the impact on digital rights for African citizens by the digital surveillance capabilities of some African governments, Anand Sheombar will discuss the implications this has on Information Technology and Information Management research.

How can we address these challenges?

Are we even aware of them as researchers?

Can we ensure that a sustainable technology-driven world is also a just world?

Some digital trends and technologies in development sector/humanitarian aid



UNHCR Innovation
12 October 2017

We piloted a chatbot with Facebook to improve communication with refugees - here's what happened (what and didn't):



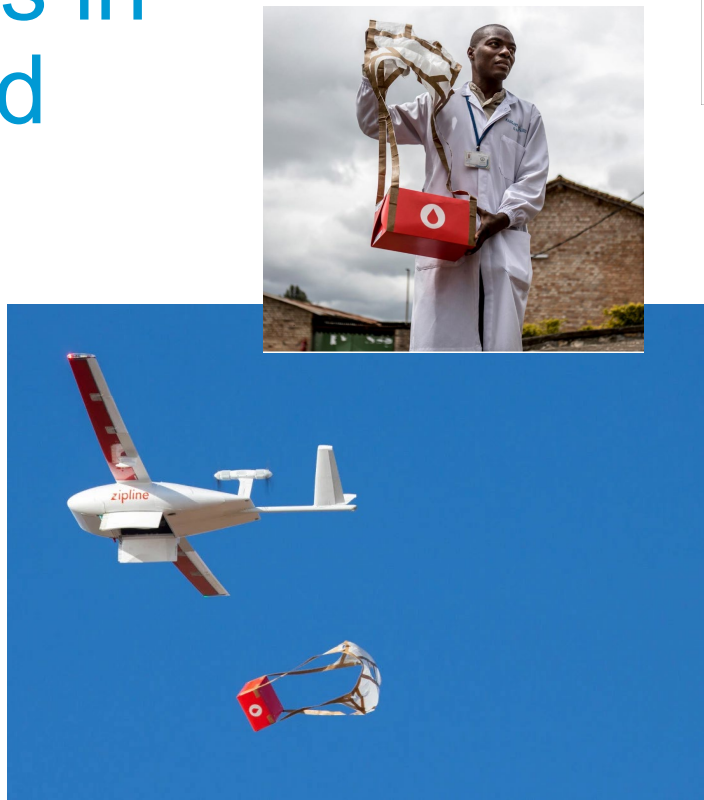
UNHCR.ORG

Chatbots in humanitarian settings: revolutionary, a fad or something in-between? - UNHCR Innovation

SOCIAL MEDIA FOR DEVELOPMENT



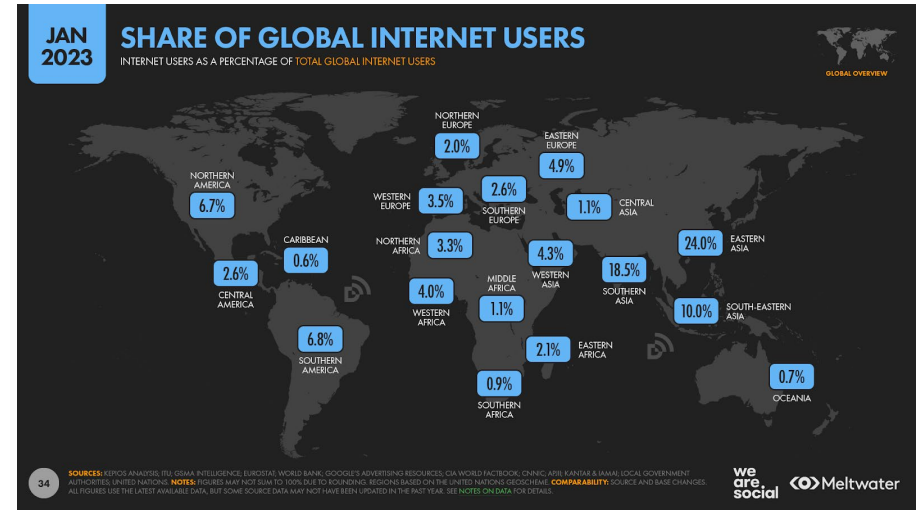
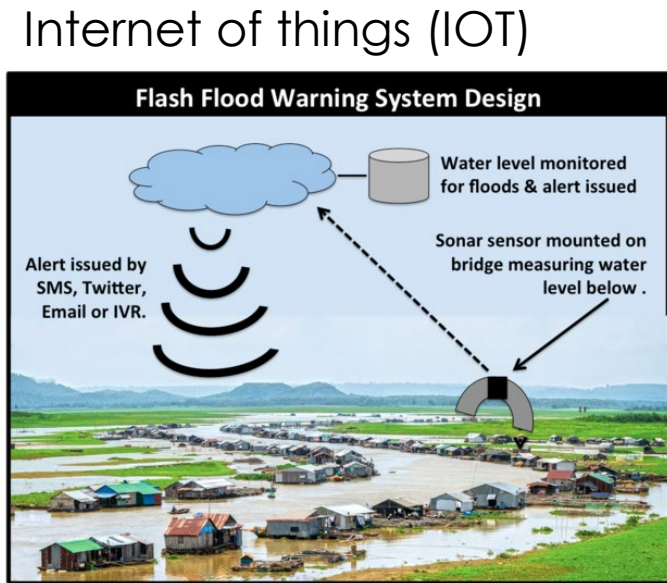
WaterAid use virtual reality to tell the story of the aftermath of Nepal's earthquakes



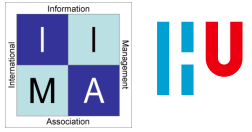
Drones



Drone/satellite images analyzed by artificial intelligence to 'harvest' statistical data from pictures



Technology for good? , ehh....



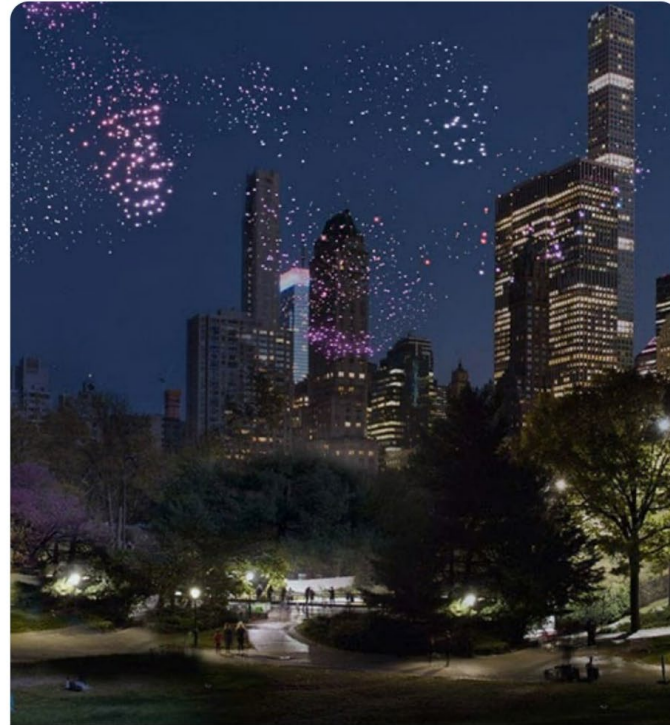
A.I. tools fueled a 34% spike in Microsoft's water consumption, and one city with its data centers is concerned about the effect on residential supply

BY [MATT O'BRIEN](#), [HANNAH FINGERHUT](#) AND [THE ASSOCIATED PRESS](#)

September 9, 2023 at 5:01 PM GMT+2



This is a VERY BAD IDEA 🚫 [#lightpollution](#) during peak [#birdmigration](#), which BTW is happening right now, poses a hazard for the millions of birds traveling over NYC on their migrations. COULD WE MOVE THIS to after fall migration? [@nycgov](#) [@NYCParks](#) [@NYCMayor](#) [@NYCMayorsOffice](#)?



central park will be shrouded in a flock of luminous drones by DRIFT this weekend

MOTHERBOARD
TECH BY VICE

Honolulu Police Used a Robot Dog to Patrol a Homeless Encampment

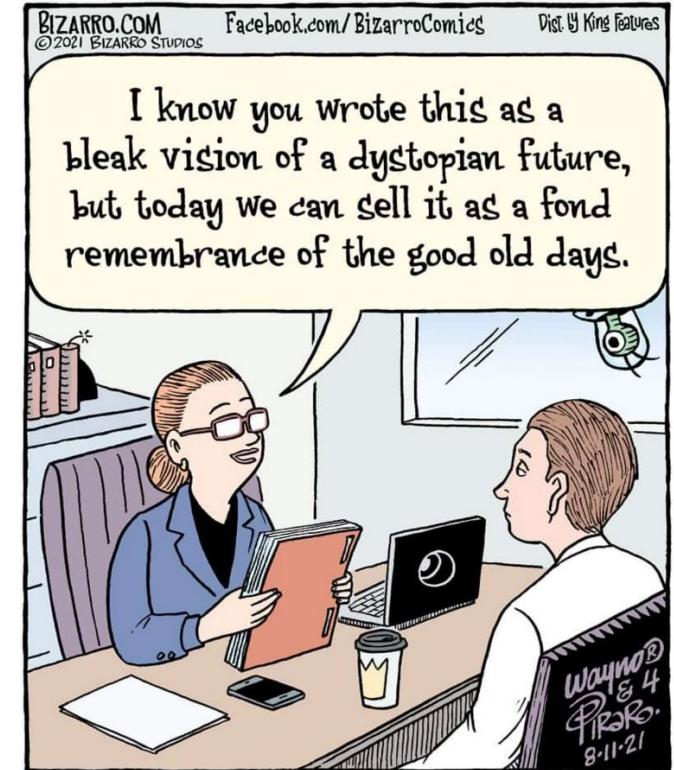
Local police used \$150,000 in COVID relief funds to purchase Boston Dynamics' four-legged robot, Spot.

TF By [Todd Feathers](#)

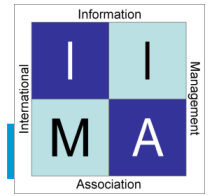
June 14, 2021, 6:00am



Information Systems, Sustainability, Technology and Digital Dystopian Present?



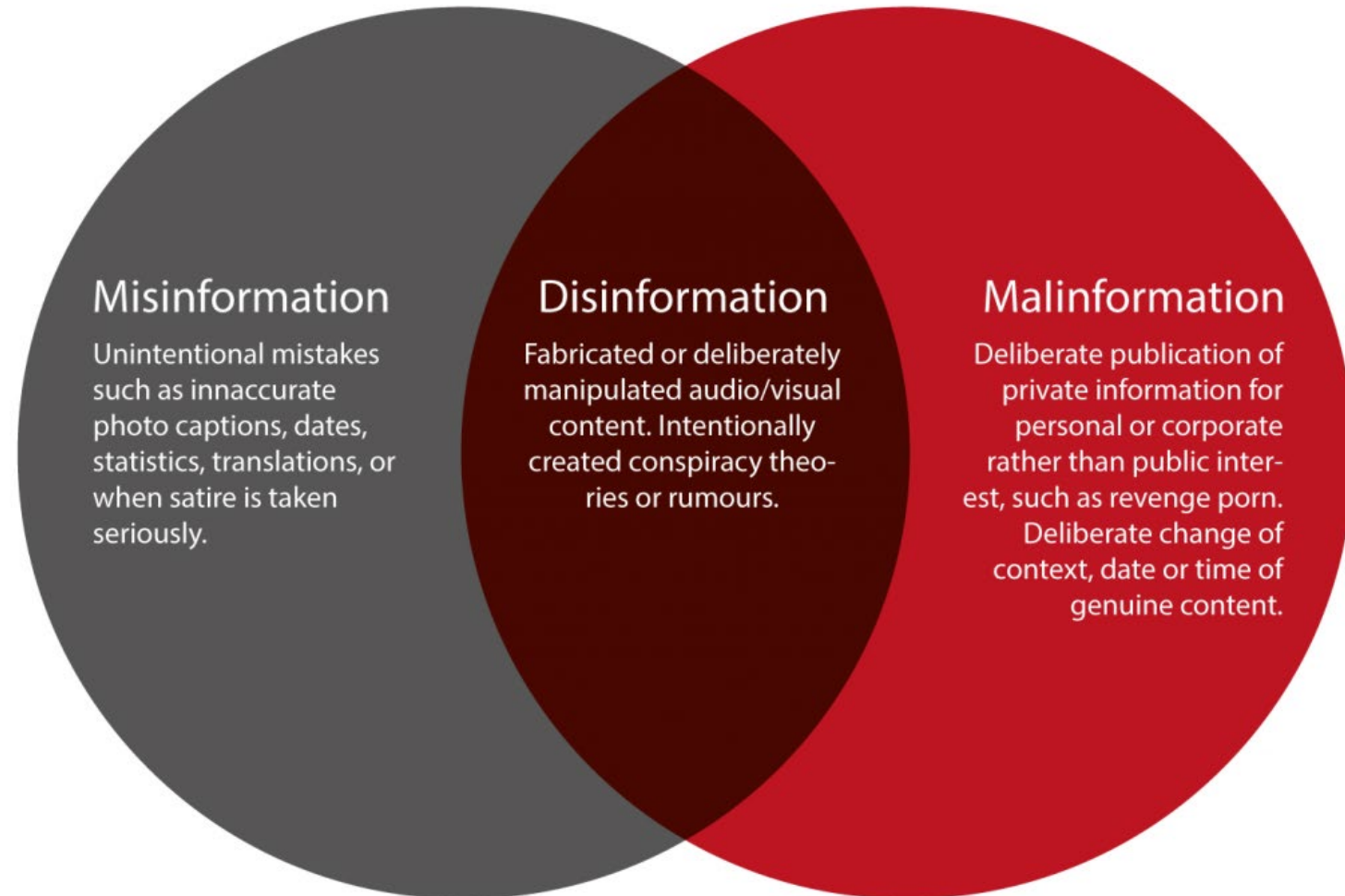
Part 1: Challenges And Threats Posed By Dis/Misinformation And Online Hate Speech In Today's Digital World



FALSENESS

INTENT TO HARM

Information disorder is an umbrella term for the various types of false, misleading, manipulated, or deceptive information (Wardle C., 2019).



JAN
2023

ESSENTIAL DIGITAL HEADLINES

OVERVIEW OF THE ADOPTION AND USE OF CONNECTED DEVICES AND SERVICES



GLOBAL OVERVIEW

TOTAL
POPULATION



we
are
social

8.01
BILLION

URBANISATION

57.2%

UNIQUE MOBILE
PHONE USERS



Meltwater

5.44
BILLION

vs. POPULATION

68.0%

INTERNET
USERS



KEPIOS

5.16
BILLION

vs. POPULATION

64.4%

ACTIVE SOCIAL
MEDIA USERS



4.76
BILLION

vs. POPULATION

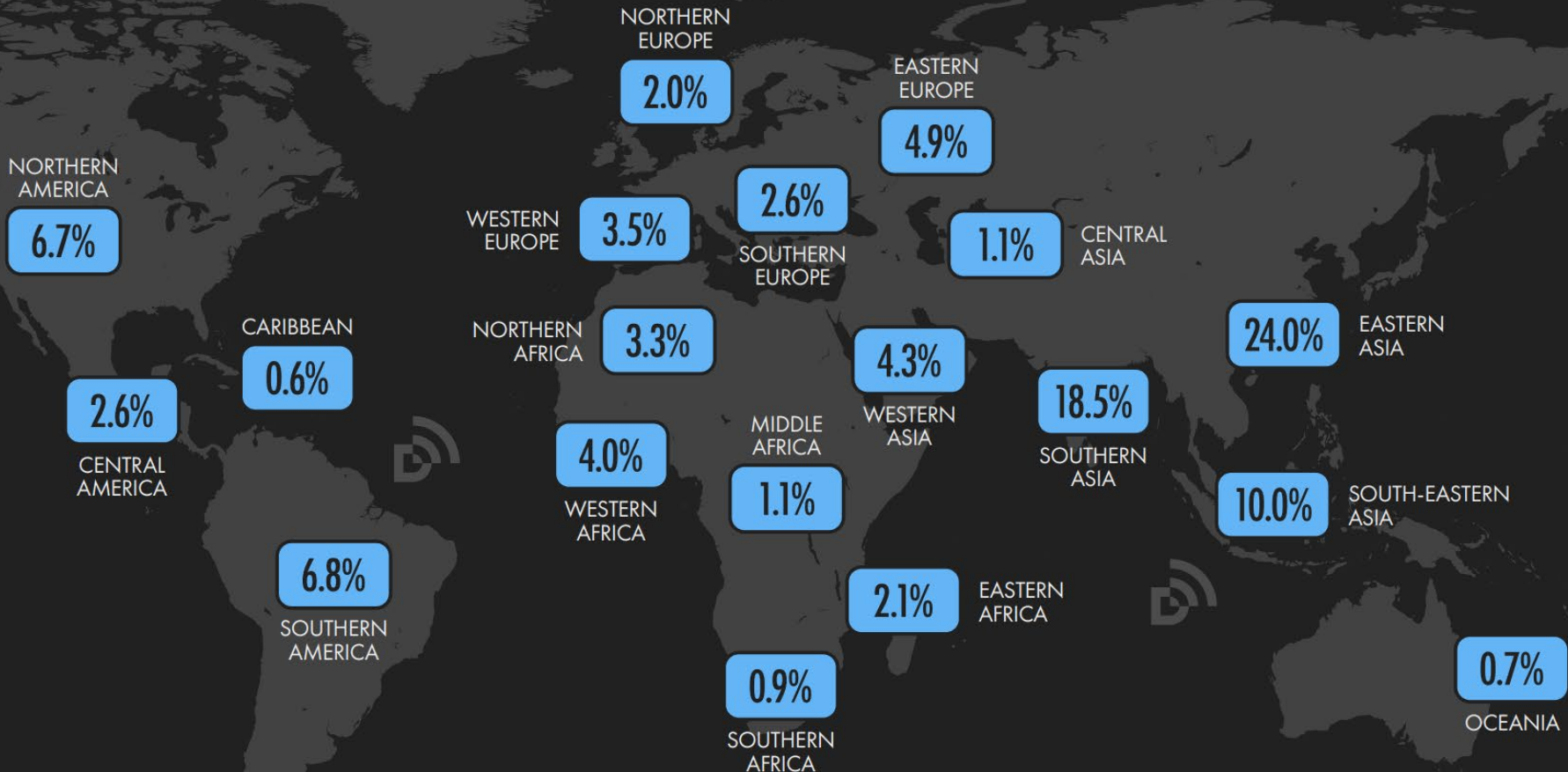
59.4%

SOURCES: UNITED NATIONS; GOVERNMENT BODIES; GSMA INTELLIGENCE; ITU; WORLD BANK; EUROSTAT; CNNIC; APJII; IAMAI & KANTAR; CIA WORLD FACTBOOK; COMPANY ADVERTISING RESOURCES AND EARNINGS REPORTS; OCDH; BETA RESEARCH CENTER; KEPIOS ANALYSIS. **ADVISORY:** SOCIAL MEDIA USERS MAY NOT REPRESENT UNIQUE INDIVIDUALS. **COMPARABILITY:** SIGNIFICANT REVISIONS TO SOURCE DATA, INCLUDING COMPREHENSIVE REVISIONS TO POPULATION DATA. FIGURES ARE NOT COMPARABLE WITH PREVIOUS REPORTS. ALL FIGURES USE THE LATEST AVAILABLE DATA, BUT SOME SOURCE DATA MAY NOT HAVE BEEN UPDATED IN THE PAST YEAR. SEE [NOTES ON DATA](#) FOR FULL DETAILS.

JAN
2023

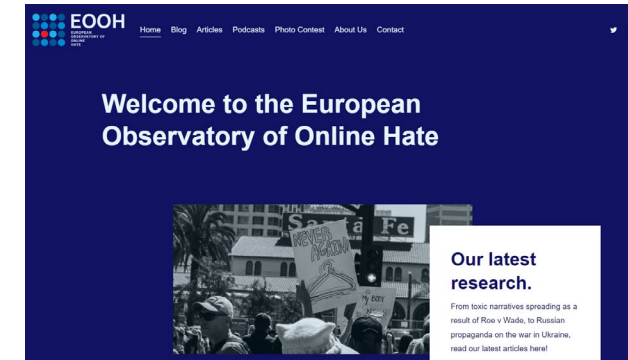
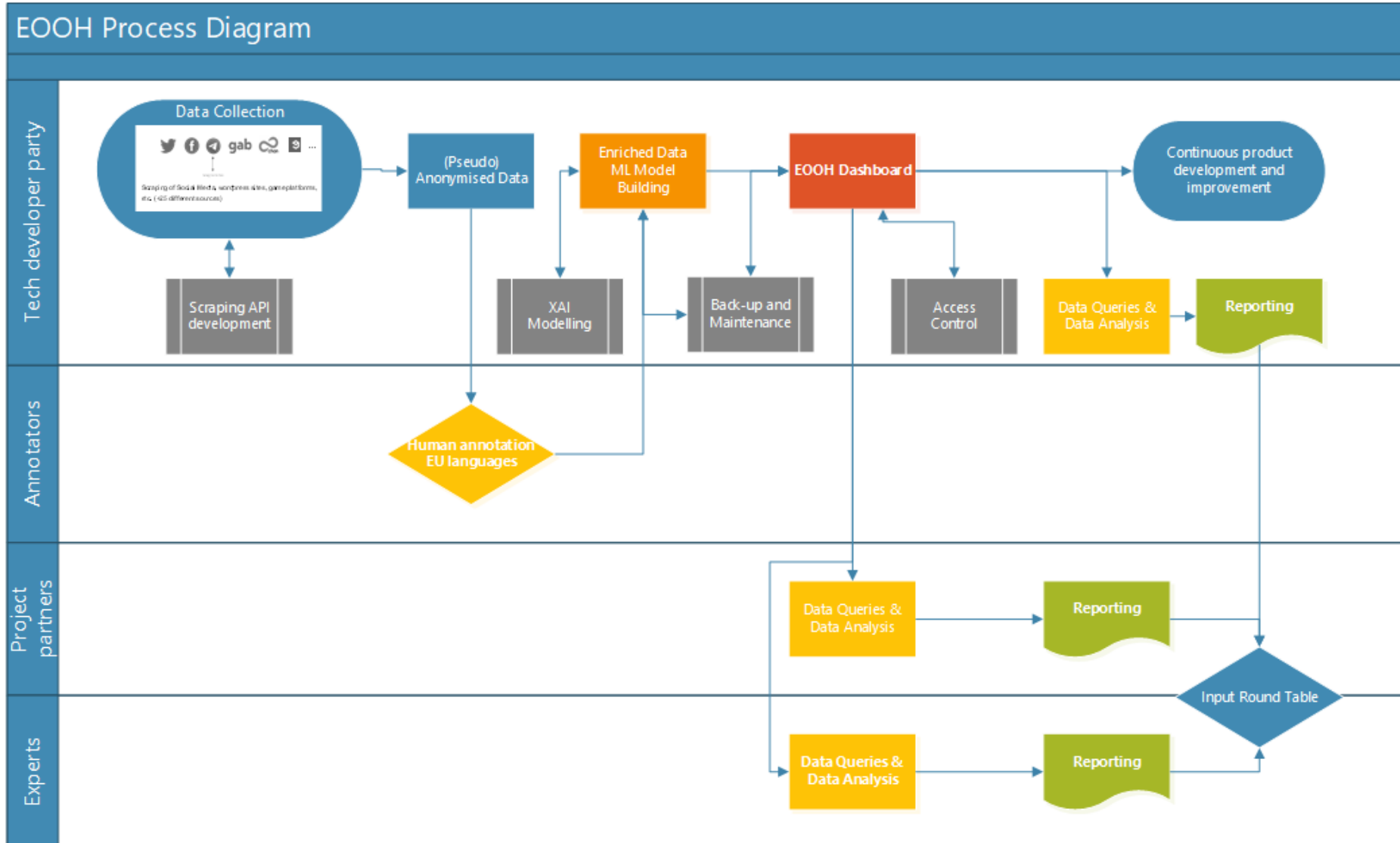
SHARE OF GLOBAL INTERNET USERS

INTERNET USERS AS A PERCENTAGE OF TOTAL GLOBAL INTERNET USERS



SOURCES: KEPIOS ANALYSIS; ITU; GSMA INTELLIGENCE; EUROSTAT; WORLD BANK; GOOGLE'S ADVERTISING RESOURCES; CIA WORLD FACTBOOK; CNNIC; APJII; KANTAR & IAMAI; LOCAL GOVERNMENT AUTHORITIES; UNITED NATIONS. **NOTES:** FIGURES MAY NOT SUM TO 100% DUE TO ROUNDING. REGIONS BASED ON THE UNITED NATIONS GEOScheme. **COMPARABILITY:** SOURCE AND BASE CHANGES. ALL FIGURES USE THE LATEST AVAILABLE DATA, BUT SOME SOURCE DATA MAY NOT HAVE BEEN UPDATED IN THE PAST YEAR. SEE [NOTES ON DATA](#) FOR DETAILS.

- Visualisation of online hate speech collection and processing.



Project website EOOH.eu

EOOH project: Annotation Process - ongoing - categorising toxic language

SCORE 0 = no problem, 4 = very problematic

| 1 | ★ | # | WORD | | 🤔 | 💩 | 🐸 | 😬 | 👩 | 🐷 | 👤 | ✊ | 👉 | 💣 |
|------|-----|-----|--------------------------------|--------------------------|-------------------------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|-------------------------------------|
| | | | NL | EN | | | | | | | | | | |
| 2 | 0-4 | 1M | | | | | | | | | | | | |
| 9007 | 1 | 2 | <u>nen blaffer</u> | ▼ a gun | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 9008 | 2 | 0 | <u>noten op uw zang</u> | ▼ talk tough | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 9009 | 4 | 0 | <u>stuur ze naar de goelag</u> | ▼ send them to the camp | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 9010 | 4 | 0 | <u>stuur ze naar de kampen</u> | ▼ send them to the camps | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 9011 | 1 | 142 | <u>uitgelachen</u> | ▼ laughed at | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9012 | 3 | 0 | <u>die zemmertje</u> | ▼ that little dick | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9013 | 3 | 0 | <u>die zehma</u> | ▼ that dick | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9014 | 2 | 24 | <u>putain</u> | ▼ whore | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 9015 | 2 | 0 | <u>denkt dat hij cool</u> | ▼ thinks he's cool | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

thousands of known expressions

universal translation

Online Gender-Based Violence

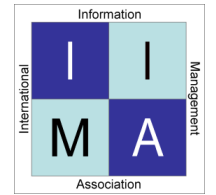
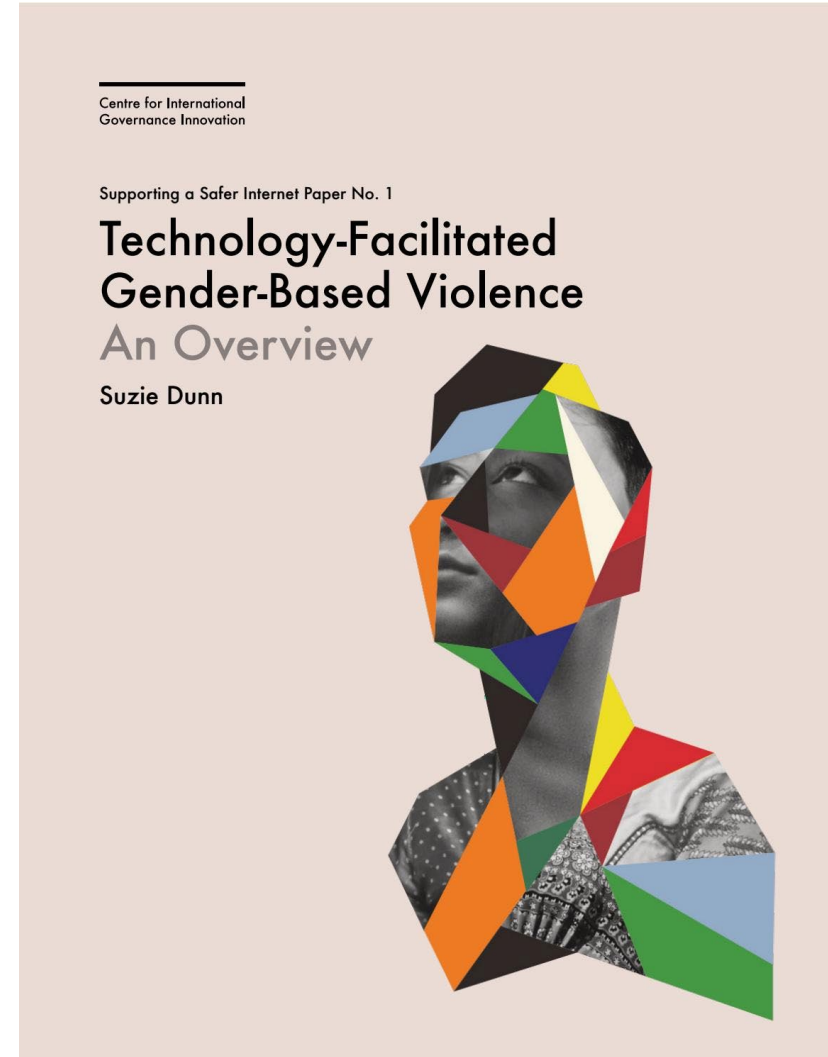
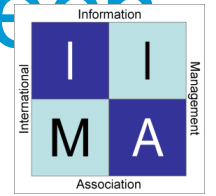


Image source: UNESCO



Human in the loop...for AI-based hate speech classification...annotation bias



Results of human annotation

- Annotators label **sexism** as **less toxic** than other forms of hate speech
- Annotators do **not agree** on **sexism being hate speech** in the first place
- Annotators seem to be **biased** against sexism
- **Sexism** seems to be one of the most **normalized/accepted** forms of hate speech

Source: misogyny online study from EOOH project

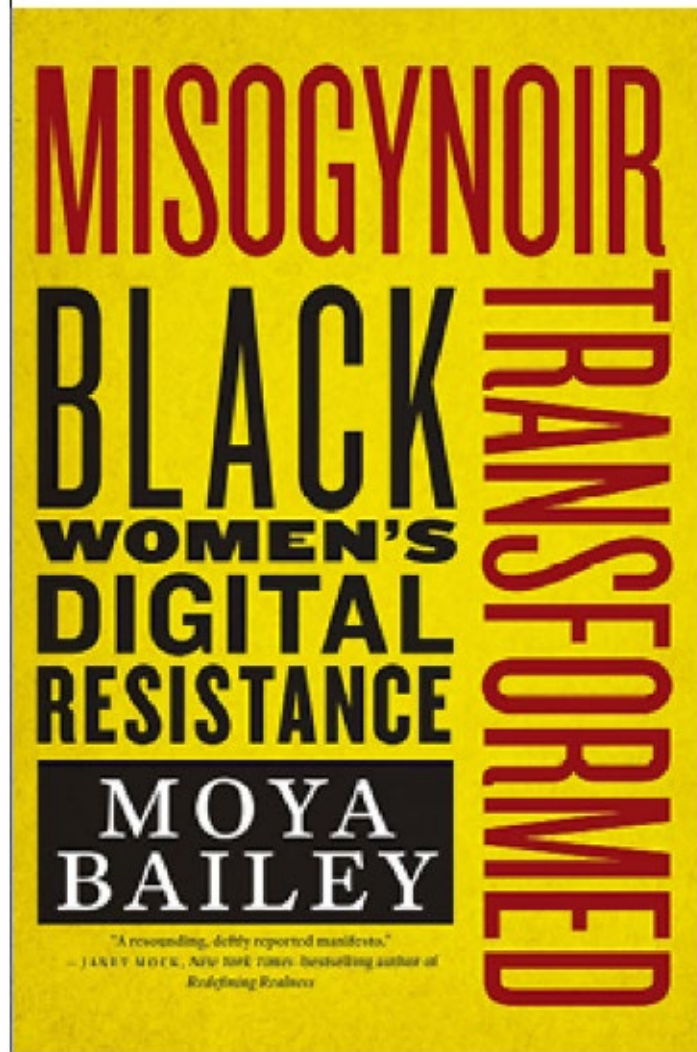
“Tech companies need to include expertise from a **variety of lived experiences** in AI annotation, implementation and interpretation.” Glitch – Digital Misogynoi Report

seen alongside content that mocks Black LGBTQ+ women.

Black women are also targeted with Islamophobic abuse, particularly when related to wearing a hijab. Black Muslim women are described as 'extraordinary evil', demonstrating dangerous narratives that feed hate and violence against Black women.

Black Muslim women are described as 'extraordinary evil'

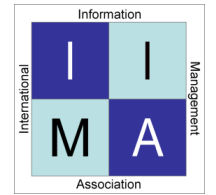
Examples: Misogynoir & Anti-Palestinian Racism are not well detected or toxicity levels too low (bias)



| | |
|--|--|
| <h3>Pro-Palästinensische Aktivisten erhalten falsche Anschuldigungen von Holocaust-Leugnung oder von Antisemitismus (Bewaffnung umstrittener IHRA-Beschreibung)</h3> <p>Twitter screenshots showing tweets with false accusations against pro-Palestinian activists.</p> | <h3>Angstmacherei und Terrorvorwürfe</h3> <p>Twitter screenshots with threats and terrorism allegations against individuals.</p> |
| <h3>Verweigerung des Rechts auf Widerstand gegen die Besetzung (Teil der internationalen Rechte) & BDS</h3> <p>Twitter screenshots discussing the right to resistance and BDS.</p> | <h3>Entmenschlichung der Palästinenser</h3> <p>Twitter screenshots depicting dehumanization of Palestinians.</p> |
| <h3>Leugnung der Existenz Palästinas oder des palästinensischen Volkes oder des Auftretens ethnischer Säuberungen, der Nakba</h3> <p>Twitter screenshots denying the existence of Palestine or the Nakba.</p> | <h3>Islamophobie und andere Formen der Diskriminierung überschneiden sich mit antipalästinensischem Rassismus</h3> <p>Twitter screenshots showing the overlap of Islamophobia and anti-Palestinian racism.</p> |

- #### Folgefragen zur Erstanalyse
- Wird anti-Palästinensischer Rassismus im EOOH Dashboard effektiv erkannt?
 - Würden einigen antisemitischen Tweets zu Unrecht antiisraelische Kritik (wegen IHRA) zugeschrieben?
 - Wird Islamophobie verbreitet oder verstärkt durch pro-israelische Social-Media-Konten die anti-palästinensischen Rassismus verbreiten?

AI and Data Collection



When developing system that collects social media data for analysis using artificial intelligence, **ethical considerations** need to be taken into account (Kiritchenko and Nejadgholi, 2020)

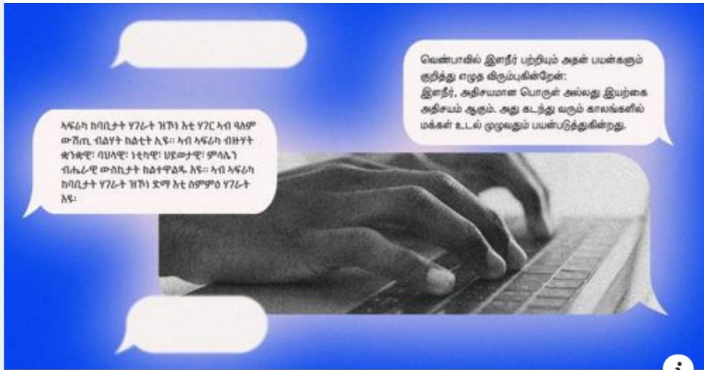
- Mitigation of unintended biases
- What constitutes hate speech
- Sampling/topic bias
- Annotator bias
- Transparency and explainability

Hate speech



- The concept of (online) hate speech has **arbitrary definitions**.
- **European Union's definition** (EC, 2022): "hate speech is defined in EU law as the public incitement to violence or hatred on the basis of certain characteristics, including race, colour, religion, descent and national or ethnic origin."

Part 1B: ChatGPT, LLMs and other generative AI tools...and AI bias



RESTOFWORLD.ORG
 We tested ChatGPT in Bengali, Kurdish, and Tamil. It failed.
 Outside of English, ChatGPT makes up words, fails logic tests, and can't do basic information r...

Systemic bias in data models is a human rights issue

The tech industry must engage with those affected by data errors and embedded discrimination to avoid systemic bias in data models.

By: Isabel Laura Ebert & Thorsten Busch

Español | Français



AI was asked to create images of Black African docs treating white kids. How'd it go?

October 6, 2023 · 7:44 AM ET
 By Carmen Drahl



A researcher typed sentences like "Black African doctors providing care for white suffering children" into an artificial intelligence program designed to generate photo-like images. The goal was to flip the stereotype of the "white savior" aiding African children. Despite the specifications, the AI program always depicted the children as Black. And in 22 of over 350 images, the doctors were white.
 Midjourney Bot Version 5.1. Annotation by NPR.

ChatGPT proves that AI still has a racism problem

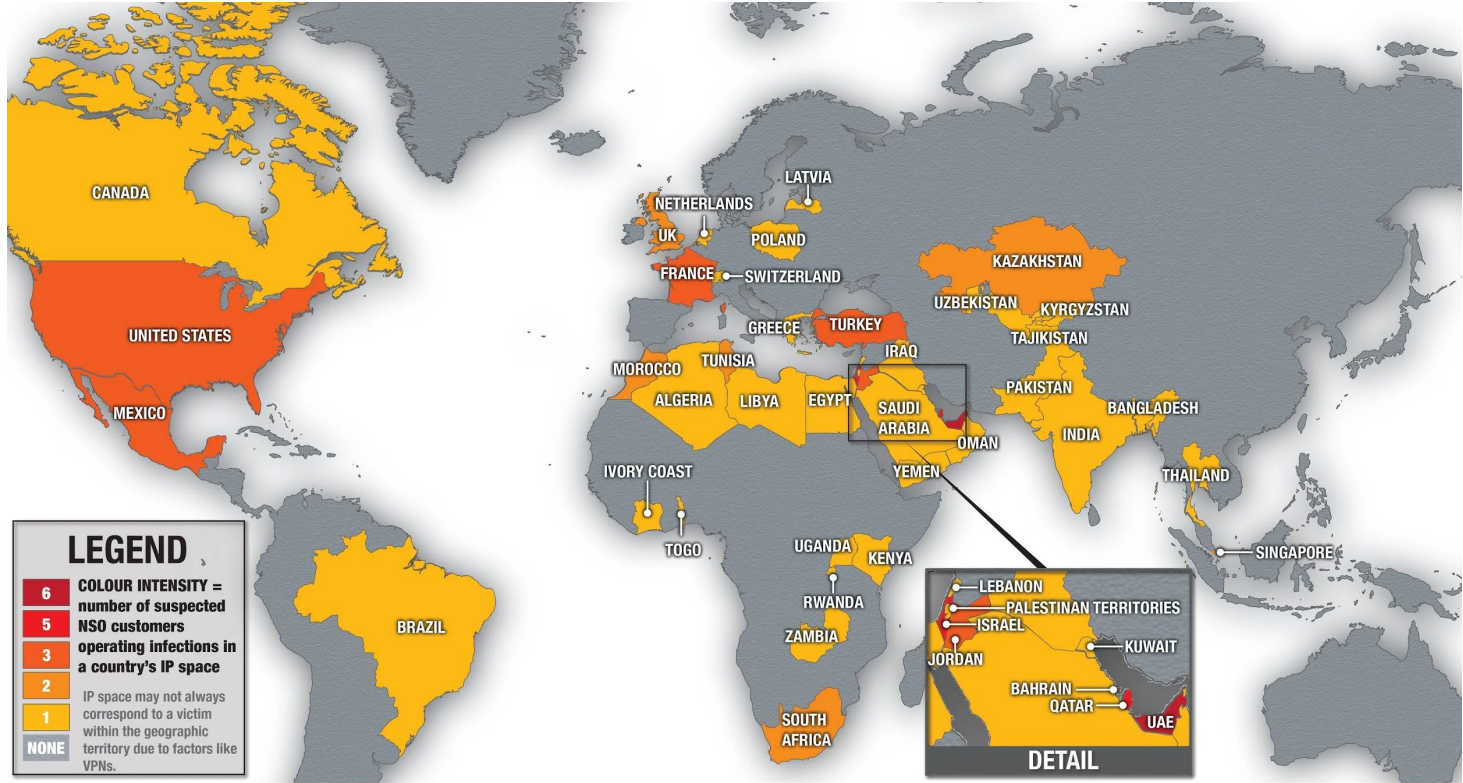
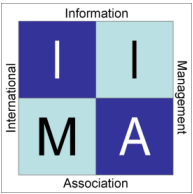
Even the most advanced artificial intelligence is hindered by the inherently racist data it's trained on.

<https://restofworld.org/2023/ai-image-stereotypes/>



TECHNOLOGYREVIEW.COM
 These new tools let you see for yourself how biased AI image models are
 Bias and stereotyping are still huge problems for systems like DALL-E 2 and Stable Diffusion, d...

Part 2: Challenges And Threats Posed By Cyber-surveillance And Digital Rights Violations In Today's Digital World



SUSPECTED PEGASUS INFECTIONS
A GLOBAL MAP MADE WITH DNS CACHE PROBING

Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak & Ron Deibert

CITIZEN LAB 2018

AI Surveillance vs Human Rights

“Although the boundaries between AI as a model of the mind and AI as surveillance tools are blurry, a tool for “profit maximization” captures current AI”
(associate professor Abeba Birhane in 2020)

AI-based biometric technologies are particularly prone to “function creep “ and perpetuate discrimination (Access Now report 2023)

Automating Digital Repression: How AI Can Harm Human Rights

Without robust safeguards and oversight, AI can make censorship, surveillance, and the creation and spread of disinformation easier, faster, cheaper, and more effective.



The infographic features a central photograph of a busy city street with many pedestrians. Several yellow rectangular boxes are overlaid on the image, each containing a person's face, representing AI facial recognition. Lines connect these boxes to six blue callout boxes, each with an icon and text describing a human right that is violated by AI surveillance.

- Privacy** (Eye icon): Big-data surveillance systems aggregate and analyze massive amounts of personal data, inferring people's most sensitive information. AI models often rely on enormous datasets to function.
- Due process** (Scales icon): AI-enabled surveillance tools, such as social media monitoring, forgo standards like “probable cause,” treating everyone as a possible wrongdoer.
- Free expression** (Speech icon): Automated systems are deployed to censor political, social, and religious speech. AI surveillance can incentivize people to avoid reprisal through self-censorship.
- Nondiscrimination** (Person with X icon): Algorithmic systems can perpetuate bias built into their training data and exacerbate long-standing discrimination.
- Access to information** (Information icon): Platform algorithms have promoted incendiary content over reliable information. Progovernment commentators can use generative AI to create disinformation at scale.
- Association and assembly** (Group icon): AI systems with abilities like facial recognition can identify and track prodemocracy protesters, allowing state forces to arrest and retaliate against them.

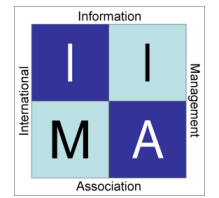
Freedom House logo in the bottom left corner.

This infographic is from the *Freedom on the Net 2023* report, as seen on www.freedomhouse.org

African Digital Rights Network

Sousveillance Research Question:

Who is supplying **what** technologies **to whom** with what effect on citizen's digital rights?

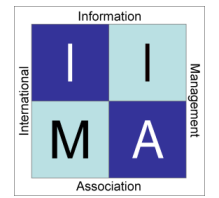


Five categories of surveillance technologies:

1. Internet interception - intercepting private Internet communications
2. Mobile interception - intercepting private mobile phone communications
3. Social Media Monitoring – surveillance of social media interactions
4. Safe City / Smart City – including CCTV and remote sensing surveillance.
5. Biometric-ID including facial recognition, iris scanning and fingerprint scanning.

These are categories of technologies that are well-researched and documented in the UK/USA/Europe but have yet to be well-documented in Africa.

Examples of Suppliers & donor countries



Huawei launched a US\$1.5 billion fund to support the development of smart cities across Africa; for example, setting up digital infrastructure in Zambia where the WSJ reported it helped authorities intercept encrypted communications and use mobile data to track political opponents.



EU institutions, Frontex and the EEAS being investigated by the European Ombudsman over failures to conduct human rights assessments of their surveillance technology transfers to non-EU countries.

TECH Huawei Technicians Helped African Governments Spy on Political Opponents

Employees embedded with cybersecurity forces in Uganda and Zambia intercepted encrypted communications and used cell data to track opponents, according to a Wall Street Journal investigation

By [Joe Parkinson](#) [Follow](#), [Nicholas Bariva](#) [Follow](#) and [Josh Chin](#) [Follow](#)
Updated Aug. 15, 2019 3:21 am ET

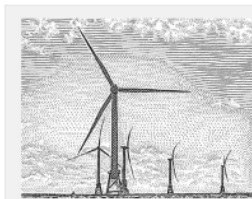
SHARE [TEXT](#)

351 RESPONSES

KAMPALA, Uganda—Huawei Technologies Co., the world's largest telecommunications company, dominates African markets, where it has sold security tools that governments use for digital surveillance and censorship.

But Huawei employees have provided other services, not disclosed publicly. Technicians from the Chinese powerhouse have, in at least two cases, personally helped African governments spy on their political opponents, including intercepting their encrypted communications and social media, and using cell data to track their whereabouts, according to senior security officials working directly with the Huawei employees in these countries.

THE WALL STREET JOURNAL.



WSJ Climate & Energy Newsletter

Essential news and data focused on the intersection of business, money and climate.

SUBSCRIBE

ComputerWeekly.com

IT Management

Industry Sectors

Technology Topics

NEWS

EU fails to protect human rights in surveillance tech transfers

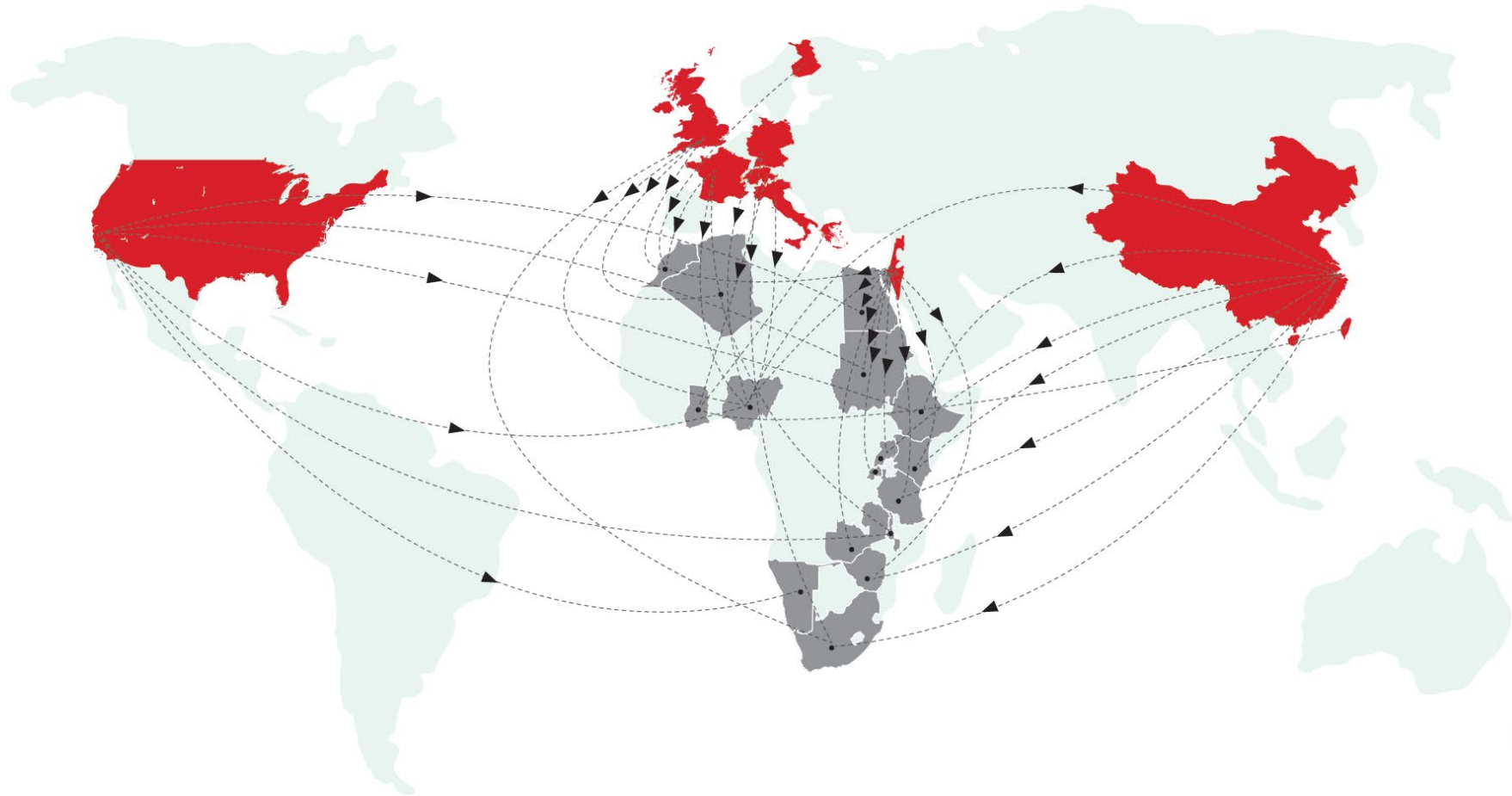
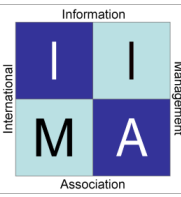
Transfers of surveillance technology from the European Union to African governments are carried out without due regard for the human rights impacts, the European Ombudsman has found after a year-long investigation into the European Commission's management of an aid fund



By Sebastian Klovig Skelton, Senior reporter

Published: 06 Dec 2022 13:56

Surveillance Supply Lines – ADRN project



■ SOURCE COUNTRIES ● DESTINATION COUNTRIES

Source Roberts et al. (2023) or
<https://www.africandigitalrightsnetwork.org/our-publications>

institute of development studies

Mapping the supply of surveillance technologies to Africa: case studies from Nigeria, Ghana, Morocco, Malawi, and Zambia

Editor: Tony Roberts

Authors: Tony Roberts, Judy Gitahi, Patrick Allam, Lawrence Oboh, Oyawole Adetunji Olatapo, Gifti Appiah-Adjei, Amira Gelel, Jimmy Kainja, Sam Phiri, Kiss Abraham, Sebastian Klovig Skelton and Anand Sheombar

Call for Chapter Abstracts for a New Book:
'Internet Shutdowns in Africa: digital rights, repression, and resistance.'



9 October 2023

Call for Chapter Abstracts for a New Book:
'Internet Shutdowns in Africa: digital rights, repression, and resistance'

Edited by Felicia Anthonio and Tony Roberts
A collected edition to be published by Zed Books in 2025

Call for abstracts:
We invite abstract submissions for chapters to be included in a collected edition book on the implementation of internet shutdowns and civic responses.

| Supplier country: China | | | |
|--------------------------------|----------------|--|--|
| Technology | Supplier | Government | Examples |
| Mobile interception | ZTE | Zambia | Via subsidiaries in Ghana, Nigeria, and Zambia – and also Côte d'Ivoire. Construction of a rural telephone service in Nigeria. |
| Internet interception | | | |
| Social media monitoring | | | |
| Smart cities | Huawei | Ghana, Malawi, Morocco, Nigeria, and Zambia. Also Côte d'Ivoire. | Huawei launched a US\$1.5bn fund to support the development of smart cities across Africa; e.g. setting up digital infrastructure in Zambia where <i>The Wall Street Journal</i> reported it helped authorities intercept encrypted communications and use mobile data to track political opponents. |
| Biometric ID | Huawei and ZTE | Ghana | Ghana received a US\$129m loan from China Exim Bank for extension of dedicated information infrastructure, including implementation of intelligent video surveillance by Huawei and ZTE. |

Source: Authors' own. Created using data from Takouleu (2018); Ofori-Atta and Kan-Dapaah (2019); Parkinson *et al.* (2019a,b); Huawei (2020, 2021, 2022); ZTE (2021); Burkitt-Gray (2022); Abdulaziz (2023).

Supplier country: EU and member states France (F), Germany (DE), and Italy (IT)

EU institutions, Frontex, and the EEAS are being investigated by the European Ombudsman over failures to conduct human rights assessments of their surveillance technology transfers to non-EU countries

| Technology | Supplier | Government | Examples |
|--------------------------------|---|--------------------|---|
| Mobile interception | | | |
| | Altrnativ (F) | Côte d'Ivoire | Deal worth €13.8m for radio surveillance equipment and intelligence training |
| | Nexa Technologies (F) | Egypt | Surveillance software CEREBRO, which provides real-time surveillance of the mobile phones of targeted citizens and the collection of personal data and metadata |
| | Finfisher (DE) | South Africa | FinFisher Command and Control servers in South Africa |
| | Hacking Team, now active under the name Memento Labs (IT) | Morocco | Moroccan intelligence services used spyware Remote Control System and spent more than €3m on Hacking Team equipment |
| Internet interception | | | |
| | Trovicor (DE) | Ethiopia | Communications surveillance equipment to the Ethiopian government |
| Social media monitoring | | | |
| | Altrnativ (F) | Multiple countries | Tailor-made search engine Targets, to retrieve publicly available data to analyse and identify connections between places, people, and organisations |
| Smart cities | | | |
| Biometric ID | EUTFA (EU) | Ghana | €5m project for 'Strengthening border security in Ghana' to enhance border checking and surveillance capacities of the Ghana Immigration Service |
| | EUTFA (EU) | Morocco | A €44m 'Support for integrated border and migration management in Morocco' project in 2018, including the acquisition of surveillance equipment for sea and land borders, as well as improving data use and cooperation with EU authorities |

Source: Authors' own. Created using data from Marczak *et al.* (2014); Privacy International (2015a,b); Singh (2015); EUTF (2017); EC (2019); Canet *et al.* (2021); Mada Masr (2021); Braun (2022); Coluccini (2023); EUTF (2023).

Supplier country: Israel

| Technology | Supplier | Government | Examples |
|------------|----------|------------|----------|
|------------|----------|------------|----------|

Mobile interception

| | | | |
|--|------------|--|--|
| | Circles | Morocco, Nigeria, and Zambia Also Botswana, Equatorial Guinea, Kenya, and Zimbabwe | |
| | NSO Group | Morocco, Nigeria, and Zambia Also Côte d'Ivoire, Egypt, Kenya, Rwanda, South Africa, Togo, and Uganda | Developers of the Pegasus spyware |
| | Team Jorge | Nigeria | Hacked into the phones of opposition leaders during the 2015 Nigerian election |

Internet interception

Social media monitoring

Smart cities

| | | | |
|--|----------|--------------|---|
| | Briefcam | South Africa | 'Video synopsis technology' incorporated in smart city surveillance networks in suburban areas. |
|--|----------|--------------|---|

Biometric ID

Source: Authors' own. Created using data from Kwet (2019); Mwesigwa (2019); Marczak *et al.* (2020); Murray (2022).

Supplier country: USA (and UN entities)

| Technology | Supplier | Government | Examples |
|------------|----------|------------|----------|
|------------|----------|------------|----------|

| | | | |
|----------------------------|---|-------------|---|
| Mobile interception | Israeli branch of US-based Verint Systems | South Sudan | Surveillance equipment to intercept communication |
|----------------------------|---|-------------|---|

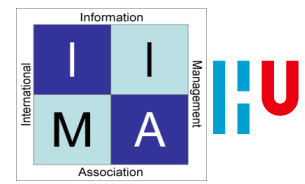
Internet interception

| | | | |
|--------------------------------|----------|--|--|
| Social media monitoring | Dataminr | Nigeria Also Kenya and South Africa | Monitoring student demonstrations in Cape Town, South Africa |
|--------------------------------|----------|--|--|

| | | | |
|---------------------|-----------|-------|--|
| Smart cities | Honeywell | Egypt | Surveillance systems for large smart city projects |
|---------------------|-----------|-------|--|

| | | | |
|---------------------|----------|-------------------------|--|
| Biometric ID | Palantir | UN World Food Programme | International aid funds are used for digital surveillance of migrants and refugees |
|---------------------|----------|-------------------------|--|

Source: Authors' own. Created using data from Dataminr (2016); Thorpe (2019); Feldstein (2019); Biddle (2020); Peterson and Hoffman (2022).



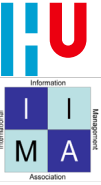
| Supplier country: Russia | | | |
|---------------------------------|-----------------|---|----------------------------------|
| Technology | Supplier | Government | Examples |
| Mobile interception | | | |
| Internet interception | | | |
| Social media monitoring | | | |
| Smart cities | | | |
| Biometric ID | Rosoboronexport | 17 sub-Saharan African countries, including Nigeria | Signed contracts worth US\$1.7bn |

Source: Authors' own. Created using data from Hedenskog (2018); Ojoye (2021); Rosoboronexport (2021b).

| Supplier country: UK | | | |
|--------------------------------|------------------------|---|--|
| Technology | Supplier | Government | Examples |
| Mobile interception | | | |
| Internet interception | ETI (purchased by BAE) | Morocco, also Algeria, Qatar, Oman, Saudi Arabia, and the UAE | Mobile and internet interception system called Evident |
| Social media monitoring | | | |
| Smart cities | | | |
| Biometric ID | | Ghana and Nigeria, also Côte d'Ivoire | Border and coastal surveillance |

Source: Authors' own. Created using data from BBC (2017).

Motives for State Surveillance (Research-in-Progress)

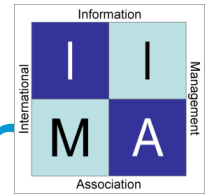


Six motives for state surveillance identified including the suppliers' perspective:

- 1) Surveillance as legitimacy for state security,
- 2) Surveillance for political gain,
- 3) Surveillance as diplomacy,
- 4) Surveillance as a tool for development,
- 5) Surveillance as neocolonialism, and
- 6) Surveillance as business opportunity.

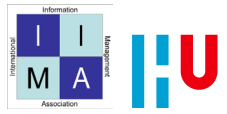
(source: Sheombar and Klovig Skelton 2023)

Part 3: Implications And Recommendations For International Technology And Information Management Research.



How can we protect citizens, organisations and society from the dystopian effects of technological advances harming the individual citizen's freedom as well as the right of expression of groups and organisations as stipulated within the frameworks of human and international rights?

Call to Action? More questions than Answers?



- How can we address these challenges?
- Are we even aware of them as researchers?
- Can we ensure that a sustainable technology-driven world is also :
- No one has the ‘right answer’, unless we intensify collaboration across disciplines and geographies?
- Multi-disciplinary research (for example, ICT & legislation) or collaboration with human rights organisations for scrutinising for harmful (un)intended consequences that deteriorate freedom and democracy?

Here are our calls to action for four groups of actors:

1. Tech companies
2. Governments and intergovernmental organisations (INGOs)
3. Research and civil society organisations
4. Online communities & digital citizens

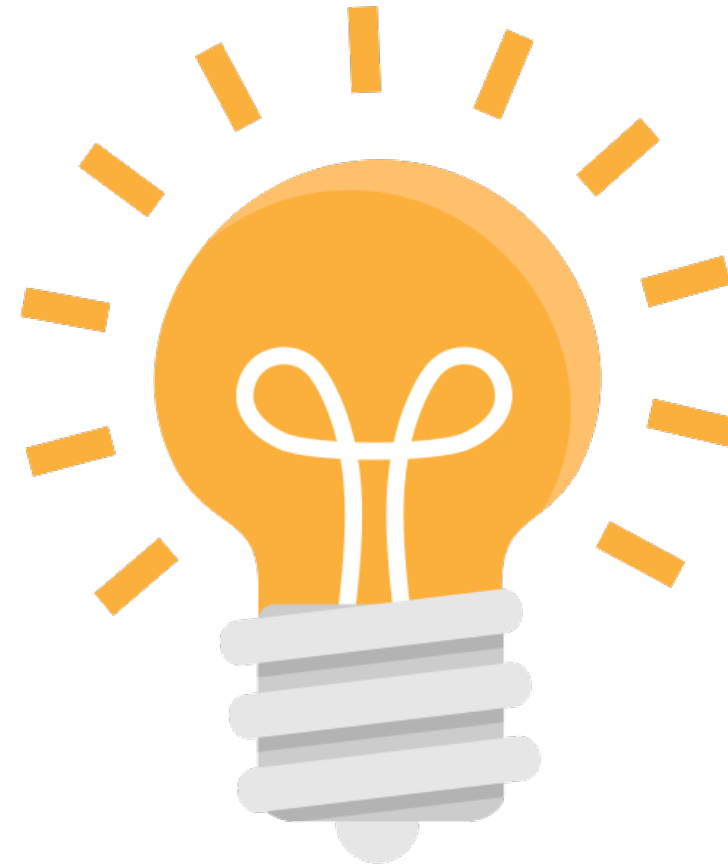
Thank you for your attention! Questions?



thehoodsfinest • 5 d. • Volgen



**MONKEYS IN BALI HAVE LEARNT THAT
THEY CAN **STEAL PEOPLE'S PHONES** AND
NEGOTIATE THEM FOR FOOD**



Anand Sheombar (anand.sheombar@hu.nl)