Socitm

Artificial Intelligence (and Cyber Security)

Samantha Smith – Director of Socitm Institute (Inspire)

UK Authority 18th Oct 2023

@Socitm | www.socitm.net

PURPOSE AND SCOPE
OF THIS SESSION

AI vs Cyber Security

- Socitm influencing policy, collaborating, undertaking research, providing guidance and tools
- Practical help available now
- Opportunities, challenges and risks
- AI and cyber security

Samantha Smith

Director of Socitm Institute (Inspire)

27 years in Local Government

- Started work for Cambridgeshire County Council specifically supporting **social workers using IT,** in particular a Social Care database.
- Worked in various technical and then managerial roles for CCC before moving to first of 3 different shared services across 9 different local authorities,
- Within LGSS I was responsible for creating the IT Strategies for LGSS and our customers (5 local authorities and a Health trust)

Including 9 years working with Socitm

- Regional Chair & Vice President (2016 – 2018)
- President (2020 – 2022)

Current

- Now in a new full time role as Director of Socitm's 'Inspire' Institute

Socitm institute – what is it?

The institute,
known as **Socitm Inspire**
is the home for…

Policy and research functions

Data services

Learning and development activities

Support for communities of interest*

* (social care, digital, data technology)

Introduction

We will answer…

Why is everyone talking about AI?

Introduction

We will answer…

What are Large Language models?

Introduction

We will answer…

How is AI being used in local government?

Introduction

We will answer…

How can we help ensure we get the benefits and safeguard against the harms?

Introduction

We will answer…

Is AI a threat to Cyber Security, or part of the solution?

Practical help: guidelines

Use of Gen AI

- Governance
- Vendors
- Copyright
- Accuracy
- Confidentiality
- Ethical Use
- Disclosure
- Integration with other tools

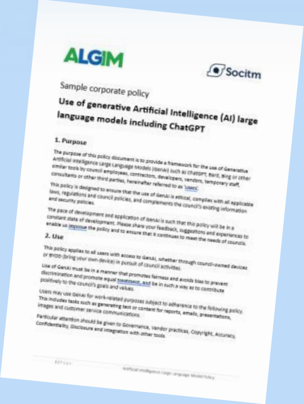
Risks

- Legal compliance
- Bias and discrimination
- Security
- Data sovereignty and protection

Compliance

Sample corporate policy document.

Produced with ALGIM - Association of Local Government Information Management, New Zealand



ALGIM Socitm

Sample corporate policy

Use of generative Artificial Intelligence (AI) large language models including ChatGPT

1. Purpose

The purpose of this policy document is to provide a framework for the use of Generative Artificial Intelligence Large Language Models (GenAI) such as ChatGPT, Bard, Bing or other similar tools by council employees, contractors, developers, vendors, temporary staff, consultants or other third parties, hereinafter referred to as 'Users'.

This policy is designed to ensure that the use of GenAI is ethical, complies with all applicable laws, regulations and council policies, and complements the council's existing information and security policies.

The pace of development and application of GenAI is such that this policy will be in a constant state of development. Please share your feedback, suggestions and experiences to enable us improve the policy and to ensure that it continues to meet the needs of councils.

2. Use

This policy applies to all users with access to GenAI, whether through council-owned devices or BYOD (bring your own device) in pursuit of council activities.

Use of GenAI must be in a manner that promotes fairness and avoids bias to prevent discrimination and promote equal treatment, and be in such a way as to contribute positively to the council's goals and values.

Users may use GenAI for work-related purposes subject to adherence to the following policy. This includes tasks such as generating text or content for reports, emails, presentations, images and customer service communications.

Particular attention should be given to Governance, Vendor practices, Copyright, Accuracy, Confidentiality, Disclosure and integration with other tools.

[illegible] Artificial Intelligence Large Language Model Policy

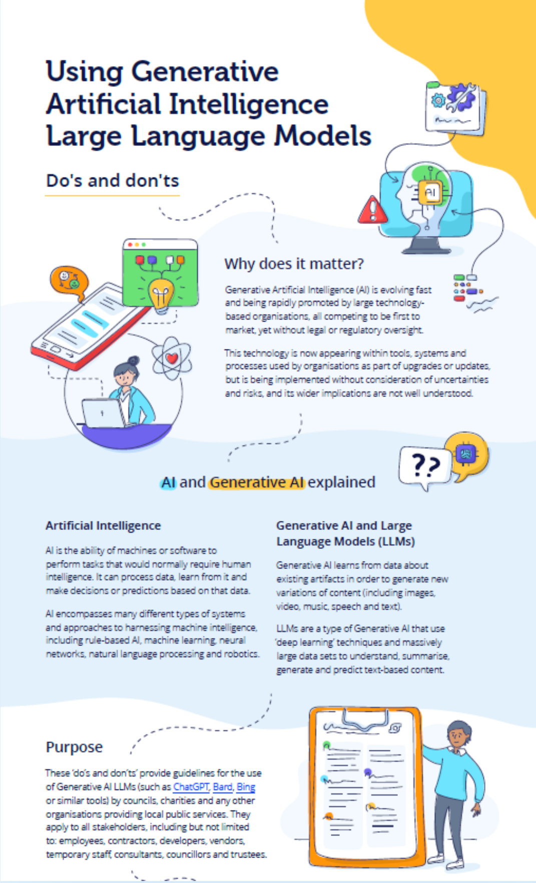
Review

Practical help **infographic**

Do’s & Don’ts

Guidelines for the use of Generative AI LLMs by councils, charities and other organisations providing local public services

Find it on Socitm’s resource hub



Using Generative Artificial Intelligence Large Language Models

Do's and don'ts

Why does it matter?

Generative Artificial Intelligence (AI) is evolving fast and being rapidly promoted by large technology-based organisations, all competing to be first to market, yet without legal or regulatory oversight.

This technology is now appearing within tools, systems and processes used by organisations as part of upgrades or updates, but is being implemented without consideration of uncertainties and risks, and its wider implications are not well understood.

AI and Generative AI explained

Artificial Intelligence

AI is the ability of machines or software to perform tasks that would normally require human intelligence. It can process data, learn from it and make decisions or predictions based on that data.

AI encompasses many different types of systems and approaches to harnessing machine intelligence, including rule-based AI, machine learning, neural networks, natural language processing and robotics.

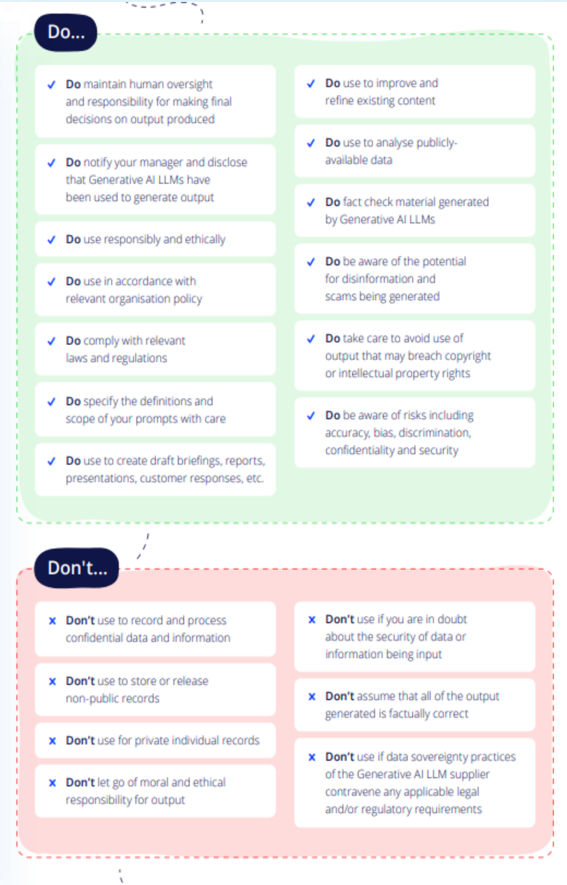
Generative AI and Large Language Models (LLMs)

Generative AI learns from data about existing artifacts in order to generate new variations of content (including images, video, music, speech and text).

LLMs are a type of Generative AI that use ‘deep learning’ techniques and massively large data sets to understand, summarise, generate and predict text-based content.

Purpose

These ‘do’s and don’ts’ provide guidelines for the use of Generative AI LLMs (such as ChatGPT, Bard, Bing or similar tools) by councils, charities and any other organisations providing local public services. They apply to all stakeholders, including but not limited to: employees, contractors, developers, vendors, temporary staff, consultants, councillors and trustees.



Do...

- ✓ **Do** maintain human oversight and responsibility for making final decisions on output produced
- ✓ **Do** notify your manager and disclose that Generative AI LLMs have been used to generate output
- ✓ **Do** use responsibly and ethically
- ✓ **Do** use in accordance with relevant organisation policy
- ✓ **Do** comply with relevant laws and regulations
- ✓ **Do** specify the definitions and scope of your prompts with care
- ✓ **Do** use to create draft briefings, reports, presentations, customer responses, etc.
- ✓ **Do** use to improve and refine existing content
- ✓ **Do** use to analyse publicly-available data
- ✓ **Do** fact check material generated by Generative AI LLMs
- ✓ **Do** be aware of the potential for disinformation and scams being generated
- ✓ **Do** take care to avoid use of output that may breach copyright or intellectual property rights
- ✓ **Do** be aware of risks including accuracy, bias, discrimination, confidentiality and security

Don't...

- × **Don’t** use to record and process confidential data and information
- × **Don’t** use to store or release non-public records
- × **Don’t** use for private individual records
- × **Don’t** let go of moral and ethical responsibility for output
- × **Don’t** use if you are in doubt about the security of data or information being input
- × **Don’t** assume that all of the output generated is factually correct
- × **Don’t** use if data sovereignty practices of the Generative AI LLM supplier contravene any applicable legal and/or regulatory requirements

Future plans

Socitm Institute:

- Collection of use cases and their transferability
- Place-based leadership training
- Policy position for use in local public services, ethics, security, impact on people, communities and places

St George’s House AI – Threats & Opportunities consultation

- Misinformation
- Social Disruption
- Dangerous Activities
- Lawmaking and Regulatory Functions

ST GEORGE’S HOUSE

Artificial Intelligence
- why it matters

The rate at which organisations are making use of AI is already:

- transforming ways of working
- changing consumer expectations

“

Amara’s law - “we tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run”

In the case of AI, it may be the other way round; we’re **talking too much** about artificial general intelligence in the decades to come**, not enough about AI at work now**.

GenAI Definition

Generative artificial intelligence (GenAI) can create new, realistic, human-like generated content using patterns and relationships learned from massive amounts of (usually public) data on which it has been trained.

CAN CREATE...

TEXT

IMAGES

AUDIO

CODE

VIDEO

ART

GenAI Application

Wider application across **local governments** and other **public service organisations**, because it can…

☑ Produce a range of useful outputs, like text, audio, images and code

☑ Respond to natural language prompts, so any officer, politician or resident can use it

☑ Understand different types of data
- useful given that local public services hold large amounts of unstructured data in a variety of formats

Other types of AI used by local government

Those tend to have very specific uses.

- Predictive analytics
- Machine learning
- Robotic process automation
- Chatbots

Artificial Intelligence Opportunit

For the public sector

However....

AI can find patterns where humans can't

n process data

ledicine

Healthcare

Education

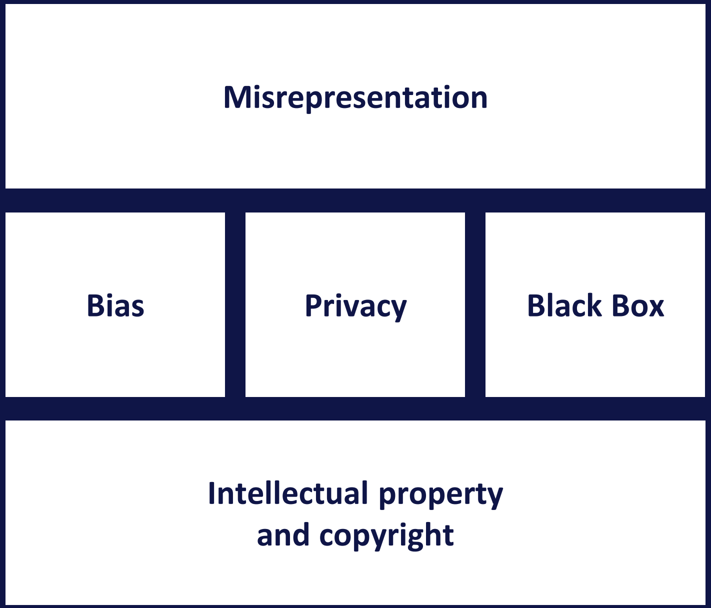
House of Commons

The Twelve challenges of AI governance

- Bias
- Privacy
- Misrepresentation
- Access to data
- Access to compute
- Black Box
- Open-source
- Intellectual property and copyright
- Employment
- International coordination
- Liability
- Existential

House of Commons

The Twelve challenges of AI governance



Misrepresentation

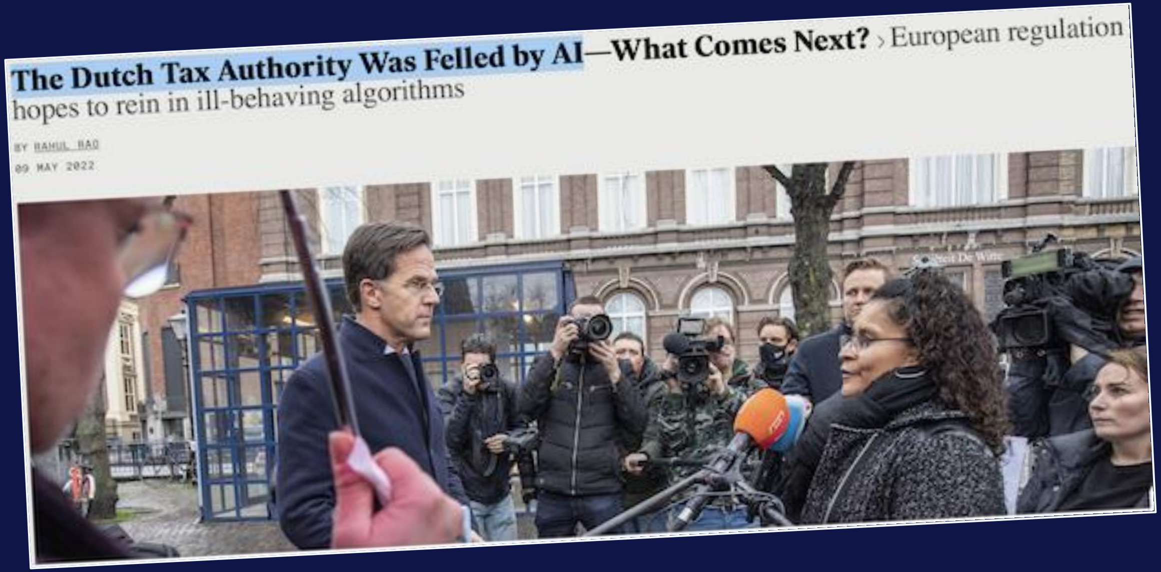
Bias

Privacy

Black Box

Intellectual property and copyright

Artificial Intelligence Risks



The Dutch Tax Authority Was Felled by AI—What Comes Next? › European regulation hopes to rein in ill-behaving algorithms

BY RAHUL RAO

09 MAY 2022

Human rights

Fairness

Privacy & agency

Safety

Societal wellbeing

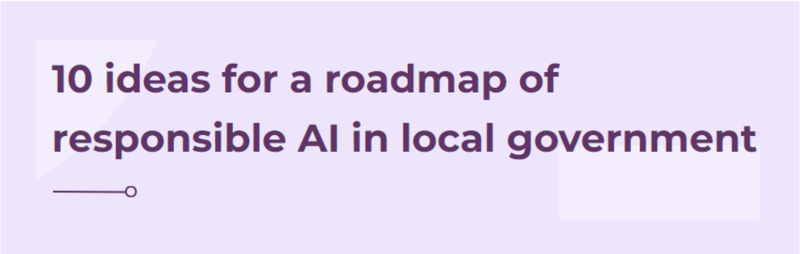
Security

Artificial Intelligence & cyber security

- AI already used in Cyber Security monitoring
- Safe and secure use of AI – what needs to be in place to assure this?
- Information Governance - Data Protection Impact Assessments (DPIA)s
- How prepared are you to respond to a data breach generated by AI?
- Election Security – is AI playing a role?

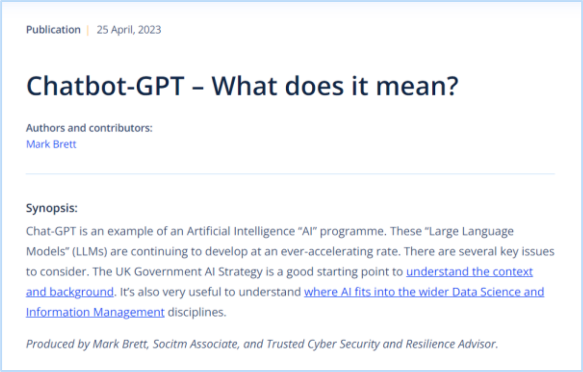
Artificial Intelligence & cyber security

loti



10 ideas for a roadmap of responsible AI in local government

The London Office of Technology and Innovation



Publication | 25 April, 2023

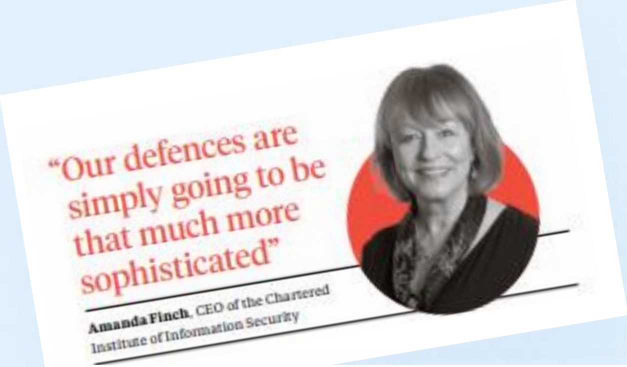
Chatbot-GPT – What does it mean?

Authors and contributors:
Mark Brett

Synopsis:

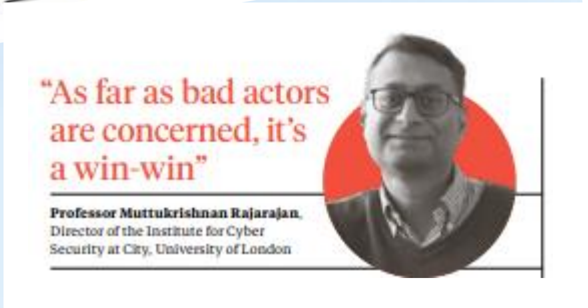
Chat-GPT is an example of an Artificial Intelligence "AI" programme. These "Large Language Models" (LLMs) are continuing to develop at an ever-accelerating rate. There are several key issues to consider. The UK Government AI Strategy is a good starting point to understand the context and background. It's also very useful to understand where AI fits into the wider Data Science and Information Management disciplines.

Produced by Mark Brett, Socitm Associate, and Trusted Cyber Security and Resilience Advisor.



"Our defences are simply going to be that much more sophisticated"

Amanda Finch, CEO of the Chartered Institute of Information Security

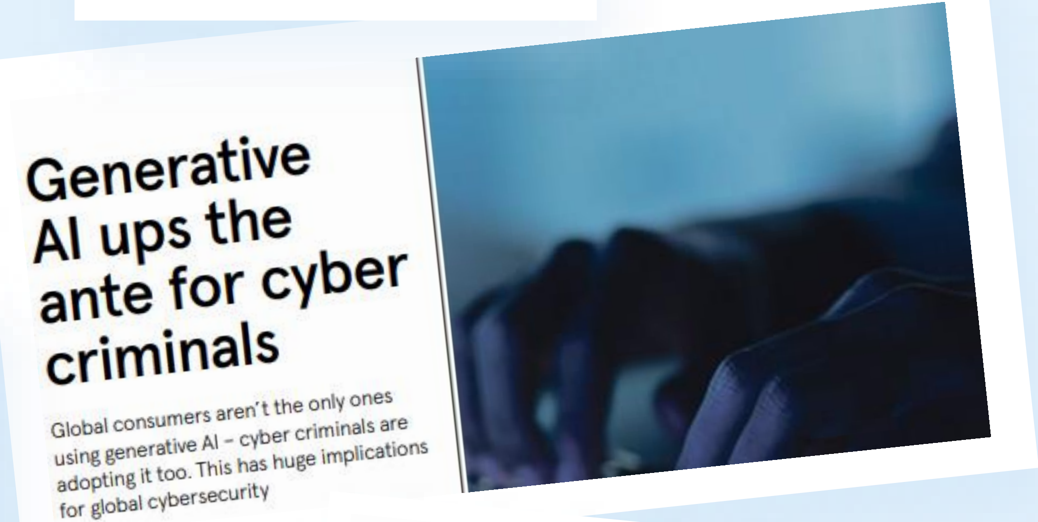


"As far as bad actors are concerned, it's a win-win"

Professor Muttukrishnan Rajarajan, Director of the Institute for Cyber Security at City, University of London

DEBATE

AI in cybersecurity: blessing or curse?



Generative AI ups the ante for cyber criminals

Global consumers aren't the only ones using generative AI – cyber criminals are adopting it too. This has huge implications for global cybersecurity

INDEPENDENT PUBLICATION BY

Raconteur

RACONTEUR.NET | #0885 | 21/09/2023

CYBERSECURITY & THE CTO

What can we do?

We can...

Share best practice

Align governance

Utilise toolkits

Invest in leadership skills

Socitm

Sam Smith

Director of institute, Socitm

Get in touch

Email:	sam.smith@socitm.net
LinkedIn:	Sam Smith
X:	@SamSmith5008