AI and the Impact on Individual Privacy

Raymond Patterson, PhD, MBA, CPA (CGA)
Professor & Area Chair, Business Technology Management
Raymond.Patterson@UCalgary.ca

haskayne
School of Business

UNIVERSITY OF
CALGARY

Key aspects of AI's impact on privacy

1. **Data Collection and Surveillance:**
   - AI systems, particularly those used in surveillance and monitoring, can collect extensive data about individuals, often without their explicit consent. This raises concerns about the potential for mass surveillance and the erosion of privacy.
2. **Biometric Data:**
   - The use of AI in facial recognition and other biometric technologies can pose significant privacy risks. If mishandled, biometric data could be misused or lead to the tracking of individuals without their knowledge.
3. **Predictive Analytics:**
   - AI algorithms are increasingly used for predictive analytics, which can make inferences about individuals based on their behavior, preferences, or historical data. This may lead to the profiling of individuals and potential privacy intrusions.

Source: Chat GPT-3

Key aspects of AI's impact on privacy

4. **Invasive Profiling:**
   - AI systems that analyze personal data may create detailed profiles of individuals, potentially revealing sensitive information about their habits, preferences, and lifestyles. This information can be used for targeted advertising or other purposes.
5. **Security Risks:**
   - The use of AI in cybersecurity can be both beneficial and risky. While AI can enhance security measures, it may also be exploited by malicious actors for sophisticated cyber attacks, leading to privacy breaches.
6. **Ethical Considerations:**
   - AI systems may inadvertently perpetuate or exacerbate biases present in training data, potentially leading to discriminatory outcomes. This raises ethical concerns, as biased decisions may impact individuals unfairly.

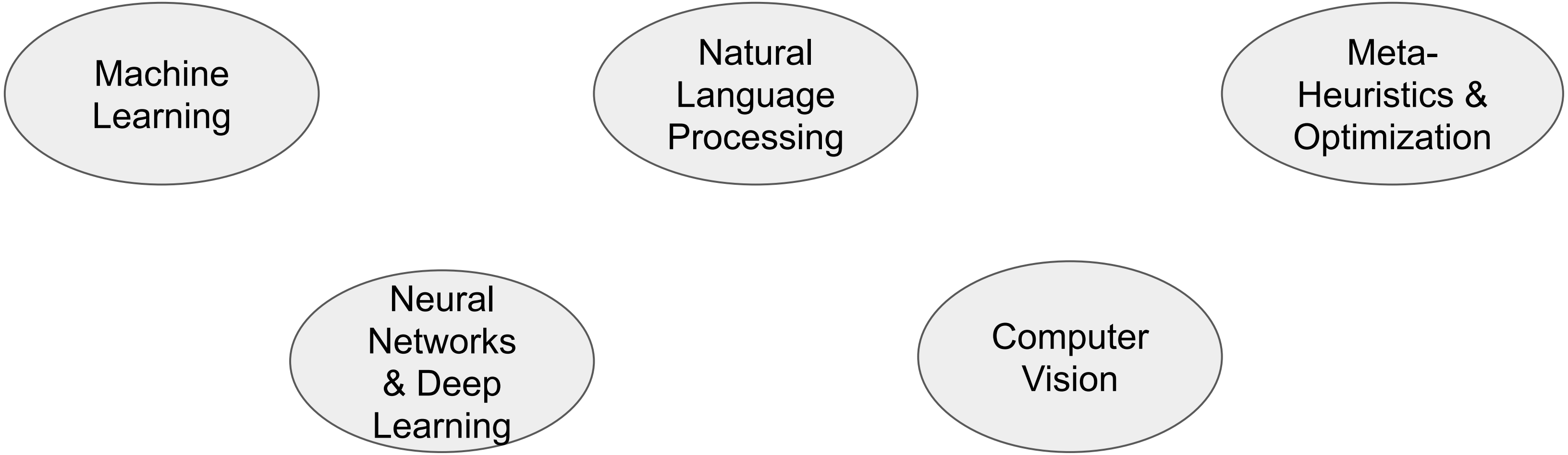
Source: Chat GPT-3

Key aspects of AI's impact on privacy

7. **Lack of Transparency:**
   - Some AI models, especially complex ones like deep neural networks, can be difficult to interpret. Lack of transparency in how AI systems reach decisions may leave individuals in the dark about how their data is being used and processed.
8. **Legislation and Regulation:**
   - Privacy laws and regulations vary across jurisdictions, and there is an ongoing effort to adapt these frameworks to the challenges posed by AI. Establishing clear rules and standards for AI usage is crucial to protecting individual privacy.
9. **Consent and Control:**
   - Individuals may not always be fully aware of how their data is being used or have control over its usage. Ensuring transparent communication and obtaining informed consent are essential for respecting individual privacy.

Source: Chat GPT-3

Types of AI algorithms



Machine Learning

Natural Language Processing

Meta-Heuristics & Optimization

Neural Networks & Deep Learning

Computer Vision

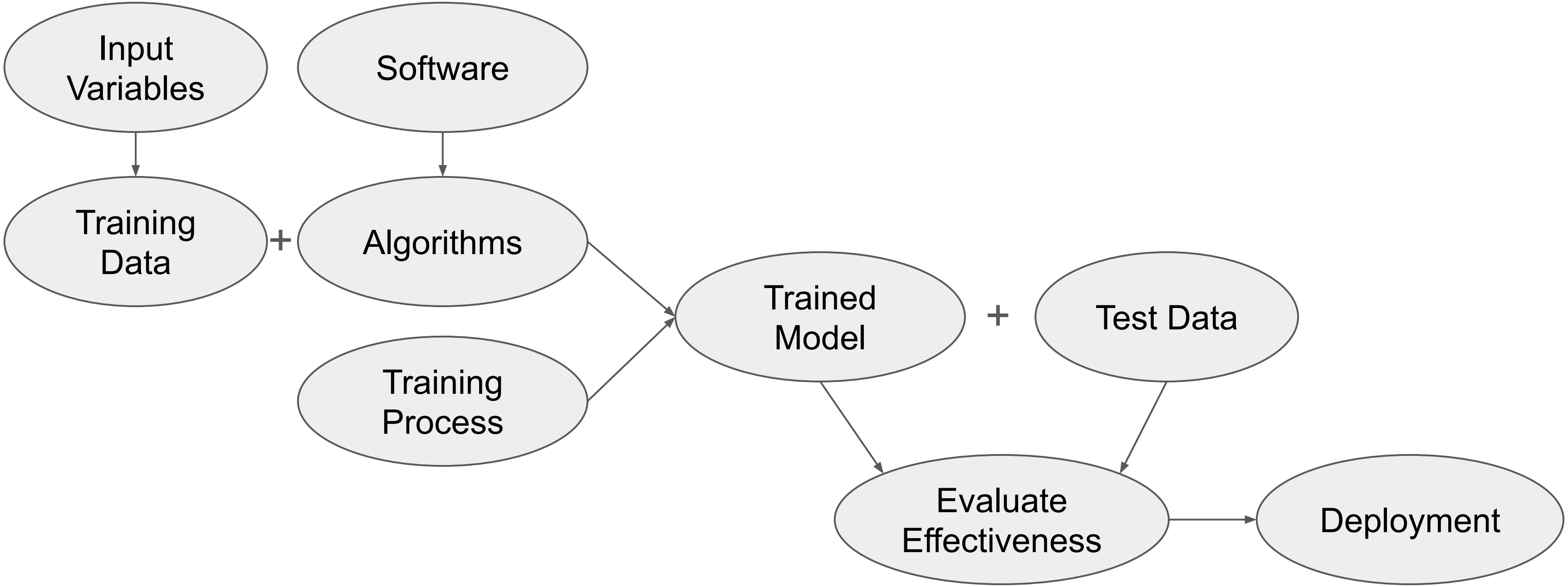
Source: Chat GPT-3

What are the most common “public” uses of AI today?

1. **Virtual Assistants:** Siri, Google Assistant, and Amazon Alexa.
2. **Recommendation Systems:** Netflix, Amazon, and Spotify.
3. **Smart Home Devices**
4. **Online Customer Support:** AI-powered chatbots.
5. **Autonomous Vehicles**
6. **Language Translation:** Improve translation accuracy.
7. **Image and Speech Recognition:** Facial recognition on smartphones and voice-activated assistants.
8. **Fraud Detection:** Financial institutions and online payment systems.
9. **Healthcare Diagnostics:** Medical imaging for diagnostics, helping to detect and analyze diseases from medical scans.
10. **Social Media Algorithms:** Personalize content feeds.

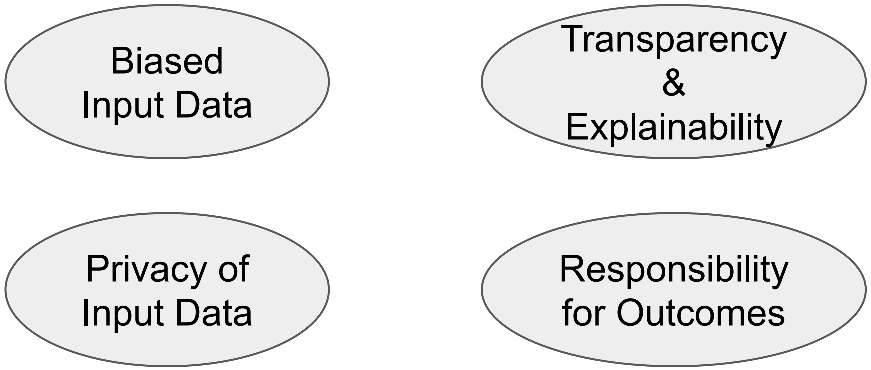
Source: Chat GPT-3

How does AI work?



Source: Chat GPT-3

Key AI ethical considerations



Input Data

Biased Input Data

Privacy of Input Data

Output

Transparency & Explainability

Responsibility for Outcomes

Constraints

Security

Inclusivity & Accessibility

Human Oversight

Environmental Impact (Energy Efficiency)

Data Governance: Data Ownership and Control

Ethical Use Cases: Applications in Sensitive Areas

Community Engagement: Stakeholder Involvement

Regulatory Compliance: Adherence to Laws and Regulations

Source: Chat GPT-3

Will AI make something up if facts are unavailable?

- Generative AI, particularly language models like Chat GPT, does not "make up" information in the same way humans might.

- Instead, it generates responses based on patterns it learned during training on a large dataset.

- If it encounters a scenario or question for which it doesn't have specific information, it may attempt to provide a response based on general knowledge and context from its training data.

Source: Chat GPT-3

How to defend against AI-enabled scams

1. Stay informed & Be aware
2. Verify Information & Be skeptical
3. Avoid sharing sensitive personal information
4. Use Strong Passwords
5. Install Security Software
6. Be Cautious with Emails: Avoid clicking on links or downloading attachments
7. Verify Callers
8. Keep Software Updated
9. Regularly review bank and credit card statements for any unauthorized transactions
10. Limit Social Media Exposure: Targeted scams
11. Consult Trusted Family or Friends
12. Report Suspicious Activity
13. Ask for Help: family member or friend

Source: Chat GPT-3

Is there anyway to look at data/text to see if it is AI generated?

Not with the naked eye. There are a few potential methods and considerations that researchers and analysts might use to examine text and infer if it's likely to be AI-generated:

1. **Pattern Recognition:** AI-generated text may exhibit certain patterns, repetition, or structures that differ from human writing styles. This could involve analyzing sentence structures, word choices, or the use of uncommon phrases.
2. **Context and Coherence:** AI models, particularly large language models like GPT-3, may struggle with maintaining context and producing coherent, contextually relevant text. Human-generated content often exhibits a deeper understanding of context and more nuanced language use.
3. **Lack of Personalization:** AI-generated content might lack a personal touch, individual experiences, or emotions. It may not provide personal anecdotes or insights that a human author might include.
4. **Knowledge Verification:** If the content makes specific claims or references recent events, fact-checking against reliable sources can help determine if the information is accurate and up-to-date. AI models may not have real-time information.
5. **Prompt-Response Inconsistencies:** Some AI models generate responses based on the provided prompts. If you notice inconsistencies or illogical responses to similar prompts, it could be an indicator of AI generation.

Source: Chat GPT-3

Is there any talk to “watermark” AI generated material so you can see the source?

Yes.

In July, OpenAI, Microsoft, Google, Meta, Amazon, Anthropic, and Inflection promised to clearly watermark AI-generated content.

It is not clear exactly how watermarking will be accomplished.

Source: https://arstechnica.com/ai/2023/07/openai-google-will-watermark-ai-generated-content-to-hinder-deepfakes-misinfo/

AI is becoming as common as using Google. Will anyone will care if material is AI generated once it is that common?

Several factors can influence how individuals perceive and respond to AI-generated content:

1. **Quality and Accuracy:** If AI-generated content consistently demonstrates high quality and accuracy, users may be more likely to accept and trust it. Conversely, inaccuracies or low-quality outputs may lead to skepticism.
2. **Transparency:** Clear communication about the use of AI is essential. If users are aware that content is generated by AI and understand its limitations, they may be more accepting. Transparency builds trust and helps manage expectations.
3. **Context and Purpose:** The context in which AI-generated content is presented matters. If it's used for creative purposes, entertainment, or certain types of information retrieval, users might be more forgiving. However, in critical or sensitive contexts, users may prefer content created by humans.
4. **Legal and Ethical Considerations:** As AI-generated content becomes more widespread, there may be legal and ethical considerations, such as intellectual property rights, accountability, and potential misuse. These factors could influence public perception.
5. **Cultural and Societal Attitudes:** Cultural and societal attitudes toward AI can vary. Some individuals may embrace AI as a useful tool, while others may have concerns about job displacement, ethical implications, or privacy issues.

Source: Chat GPT-3

Thank You!