



—
Centre for
Artificial Intelligence
and Digital Ethics

CAIDE Internship 2023 Discussion Paper Presentation

Discussion Paper for Consultation With Stakeholders

Allegra Triakash, Bri Hines, Khadijah Majid

25 May 2023

Agenda

Item 1: How Do Businesses Navigate the Use Of No-Code And Low-Code Platforms? Are The Potential Security Risks Worth the Gains?

Allegra Triakash

Item 2: Mental Health Chatbots and User Wellbeing

Bri Hines

Item 3: Deploying AI to Improve Safety Measures in Manufacturing Industries in Developing Countries

Khadijah Majid

Agenda item 1: HOW DO BUSINESSES NAVIGATE THE USE OF NO-CODE AND LOW-CODE PLATFORMS? ARE THE POTENTIAL SECURITY RISKS WORTH THE GAINS?

Introduction

No-code and low-code platforms are AI tools that compute input from a user to produce a code constructed completely or partially by an AI algorithm. These platforms are software building tools, that can aid businesses to create mobile apps, webpages, digital infrastructure and the automation of systems. No-code platforms can be used by anyone, regardless of coding knowledge, making this form of software building platform, completely functional through artificial intelligence. Low-code platforms, require minimal coding experience from the end user, however it is still heavily powered from artificial intelligence input. When implementing this technology, questions of liability can arise as these platforms could create codes that are unchecked if the proper safeguards and regulations are not set.

Technical description

Using drag-drop and building block systems, no-code and low-code platforms enable the user to create a code based on pre-sets within the platform. No-code and low-code platforms use visual interfaces for its user to engage with which then enables the platform to generate a code based on the input of the end-user. The drag-drop element of the platforms, allow the user to create the application it desires, such as a webpage or mobile app, by connecting components available within the platform. From a strictly coding perspective, the platforms offer more visual aid, stimulation and support rather than traditional coding infrastructure. Popular low-code platforms across the industry in 2023 include OutSystems, Appian, Zoho and Power Apps by Microsoft. Whilst popular no-code platforms include Glide, Google AppSheet and Bubble.

Benefits

The use of no-code and low-code platforms offer smaller businesses access to technology that was previously reserved for bigger companies that could afford expensive AI tools. Additionally, no-code and low-code platforms aid in the labour shortage that currently permeates the workforce, in particular the deficit of technological skills across the economy. No-code and low-code platforms additionally provide low-cost and efficient solutions for business' infrastructures, reducing the time spent creating software, the amount of people needed to code such software and the money usually spent on large software coding teams.

Risks

Although the implementation of no-code and low-code platforms are beneficial to a business, Forbes Technology Council cited that "these platforms are designed for rapid development, there may be a lack of quality control or security measures." When using these software development platforms, there may be a lack of oversight and supervision by the businesses implementing the tool, leaving the creation of codes by the artificial intelligence unchecked and unregulated.

This begs the question of liability:

- who is responsible when a faulty code is produced by a low-code or no-code platform that exposes a business and its consumers to security risks such as data leaks of personal information. Is the no-code platform at fault or the business?
- When implementing artificial intelligence to create technological infrastructure for a business such as webpages, apps and automation - how much can a business trust the integrity and quality of artificially produced codes?

Working assumption

No-code and low-code platforms have the potential to create significant security risks within the businesses such technology is implemented. These codes can be unstable and unchecked and thus the integrity of the code may be compromised. Nonetheless, no-code and low-code platforms can provide a wide variety of benefits to businesses and their impact can remain positive if the correct regulations and legislations are enforced to provide a check on the platforms' quality of coding output. No-code and low-code platforms will continue to remain relevant within the corporate world, though the question will remain how we regulate such artificial intelligence and do the benefits outweigh the potential harms that can arise as a result of extensive use of no-code and low-code platforms.

Discussion questions

- How trustworthy are no-code and low-code platforms, when creating vital technology to businesses?
- How wary should businesses and customers be of no-code and low-code platforms?
- No-code and Low-code platforms provide opportunity to businesses, but are the benefits of implementing this technology worth it when considering the security risks accompanied with their use?

Agenda item 2: MENTAL HEALTH CHATBOTS AND USER WELLBEING

“Tech that listens, learns, and delivers...A reliable ally you can trust.”

- <https://woebothealth.com/what-powers-woebot/>

Introduction

App based mental health interventions have surged in popularity, particularly as a response to the COVID-19 pandemic and shortage of mental health workers more broadly. These programs propose to offer a range of strategies that are more accessible than conventional therapies.

Chatbots are one example of a pre-existing technology being applied in this context. These programs aim to fill the role of a therapist or psychologist, which may be otherwise inaccessible to users due to cost, availability, etc. Woebot seeks to help users manage their mental health through mood tracking, curated videos, games, and conversations. Going forward, the company behind Woebot is seeking clearance from the F.D.A. to develop its algorithm to help treat two psychiatric diagnoses; postpartum depression and adolescent depression, to then sell the program to health systems.

Technical description

Woebot is a machine learning based chatbot that users communicate with through a chatroom functionality, either through its own individual app or Facebook Messenger. It uses natural language processing (NLP) algorithms to discern the meaning behind user messages and traces a decision tree to inform and offer appropriate responses. Cognitive behavioural therapy (CBT), Interpersonal Psychotherapy (IPT), and Dialectical Behavioural Therapy (DBT) based strategies form the basis of the advice that Woebot communicates to users.

Benefits

The current inaccessibility of conventional forms of therapy means that chatbots such as Woebot may be of benefit to users who would otherwise go without treatment. AI-powered apps have a much broader potential for scale, and they do not require additional therapists to be hired, paid, or given breaks.

Another prospective benefit of these chatbots apps is the claim that they can form relationships (or the perception of) with users, which in turn provides a comfortable space for users to discuss their problems. Research has found that in some cases, users are more comfortable sharing sensitive information with chatbots and perceive them as less judgmental than when communicating with real people. Woebot boasts that it can form [‘a trusted bond with users’ in 3 to 5 days.](#)

Risks

These platforms present the opportunity for a wide array of harms. Woebot has struggled to identify and appropriately handle cases of child sexual abuse, eating disorders, and drug use. While some limited

research does show that users benefit from the use of these programs, most of these studies have been funded or conducted by the companies that create them. Therefore, their efficacy is ambiguous at best.

Additionally, Woebot and similar applications are not bound by the same rules or oversight as therapists and psychologists, meaning that they are also not directly accountable in the same way a person might be. While its continued operation has seen improvements to the program, vulnerable users remain at the mercy of the finetuning process.

The interactions users have with Woebot further aid its development and allow the program to respond to concerns more effectively, however, the safety of this sensitive data is a topic of much concern. Woebot's privacy policy states that user data is never sold, however, it also enables them to share the information they collect with third parties, including "external advisors". They also do not accept liability for unintentional disclosure of personal information.

Working assumption

Mental health chatbots raise ethical and quality concerns for patients and therefore should be subject to similar regulatory regimes as other forms of treatment.

Discussion questions

- Is regulatory intervention sufficient to ensure Woebot develops in the direction of public interest?
- How do corporate interests and mental health concerns clash?
- Is the personification of chatbots helpful or harmful?
- Are mental health apps a reasonable response to the mental health crisis?
- Is it ethical to be testing such emergent technology on Woebot's target demographic?

Agenda Item 3: DISCUSSION ON THE DEPLOYMENT OF AI TO IMPROVE SAFETY MEASURES IN MANUFACTURING INDUSTRIES IN DEVELOPING COUNTRIES

Introduction

Providing safer working environments in the manufacturing industry has become an important area of focus in recent years, particularly after events like the Rana Plaza factory collapse (2013) have drawn attention to the risks of working in unsafe factory conditions. Due to this, work-related accidents and injuries in the manufacturing industry has been highlighted as a significant issue in developing countries. Artificial Intelligence (AI) can be used to address safety concerns in manufacturing and has the capacity to save lives by improving safety measures in some settings and eliminating the need for human contact entirely in others (for example, removing the need for humans to work with harmful chemicals).

We will consider whether there is a need for AI to be used in this field to:

- a) improve safety standards
- b) ensure these standards are met
- c) observe the practices of employees (with regards to safety in the workplace)?

Technical description

Examples of some the technologies that are being applied in the workplace to improve safety include:

- Predictive maintenance (using AI to monitor production lines and ensure machinery is running smoothly)
- Robotic maintenance (to improve efficiency with maintenance and repair works)
- Machine learning (to analyse hazards and risks and to anticipate potential accidents before they occur)
- Sensors and cameras/surveillance (to ensure appropriate safety measures are taken and safety regulations adhered to)

Benefits

Using AI in the manufacturing industry can improve safety standards because these systems analyse data at a speed that is impossible for humans to emulate. Not only can predictive maintenance be used to increase efficiency in manufacturing, machine learning and AI can be used to detect risks and predict safety hazards with more accuracy. This data can then be assessed by humans who can determine how to proceed.

Some examples of deploying AI in manufacturing include using sensors that are attached to the garments of employees during work hours in order to track their contact with potential safety hazards and other risks. Other programs include increased surveillance to detect noncompliance with safety regulations, as well as AI that focuses on 'part attention regions' of the body to compliment the regular use of PPE (hardhats and safety vests etc) in the workplace.

Risks

When considering the challenges faced when increasing the use of AI in manufacturing, we must acknowledge that using AI to heighten surveillance also runs the risk of compromising the privacy of employees. Particular concerns arise with using technology like sensors which are in close contact with workers and are thus able to monitor them more closely. This raises an ethical dilemma; should workers be under constant surveillance in the workplace?

Cost is also a significant factor to consider when contemplating the possibility of using AI in the manufacturing industry. We can see that the effects of Covid-19 have accelerated the use of AI in industries like manufacturing; the pandemic saw a rise in the need to run operations safely but with fewer human beings present at worksites. This was particularly advantageous for developing countries like India, who have seen many businesses shift their factories to the subcontinent in recent years.

Therefore, though AI has the potential to save lives with increased efficiency, the technology also comes at a high price; the costs of hardware and computer equipment must be considered, as well as the efforts and expenses incurred in training and programming these systems. Manufacturing companies could consider whether this technology is a worthwhile investment by evaluating the loss of labour they have previously suffered due to injuries in the workplace as well as considering compensation costs. Utilising intelligent maintenance systems (a combination of AI and IoT) also maximises efficiency and ultimately reduces costs over time.

Working assumption

To ensure that AI is used ethically and safely in the manufacturing industry to implement better safety measures in the workplace, sufficient precautions are necessary such as considering the privacy and autonomy of employees. Companies should also set aside a budget for investing in AI technology to reduce the number of accidents in the workplace.

Discussion questions

- One of the key reasons for accidents in factory settings is noncompliance when wearing PPE or employees not adhering to safety measures. Would AI be the best tool to fix noncompliance in the workplace? Are there other ways we might combat noncompliance?
- How much closer does the use of AI get us to reaching the 100 percent zero accidents goal? Is this realistic to achieve at some point with the help of AI?
- “You can’t put a price on human life.” How can we convince companies to invest in predictive AI for safety purposes? What is the trade off? Are the potential privacy issues worth the benefits?