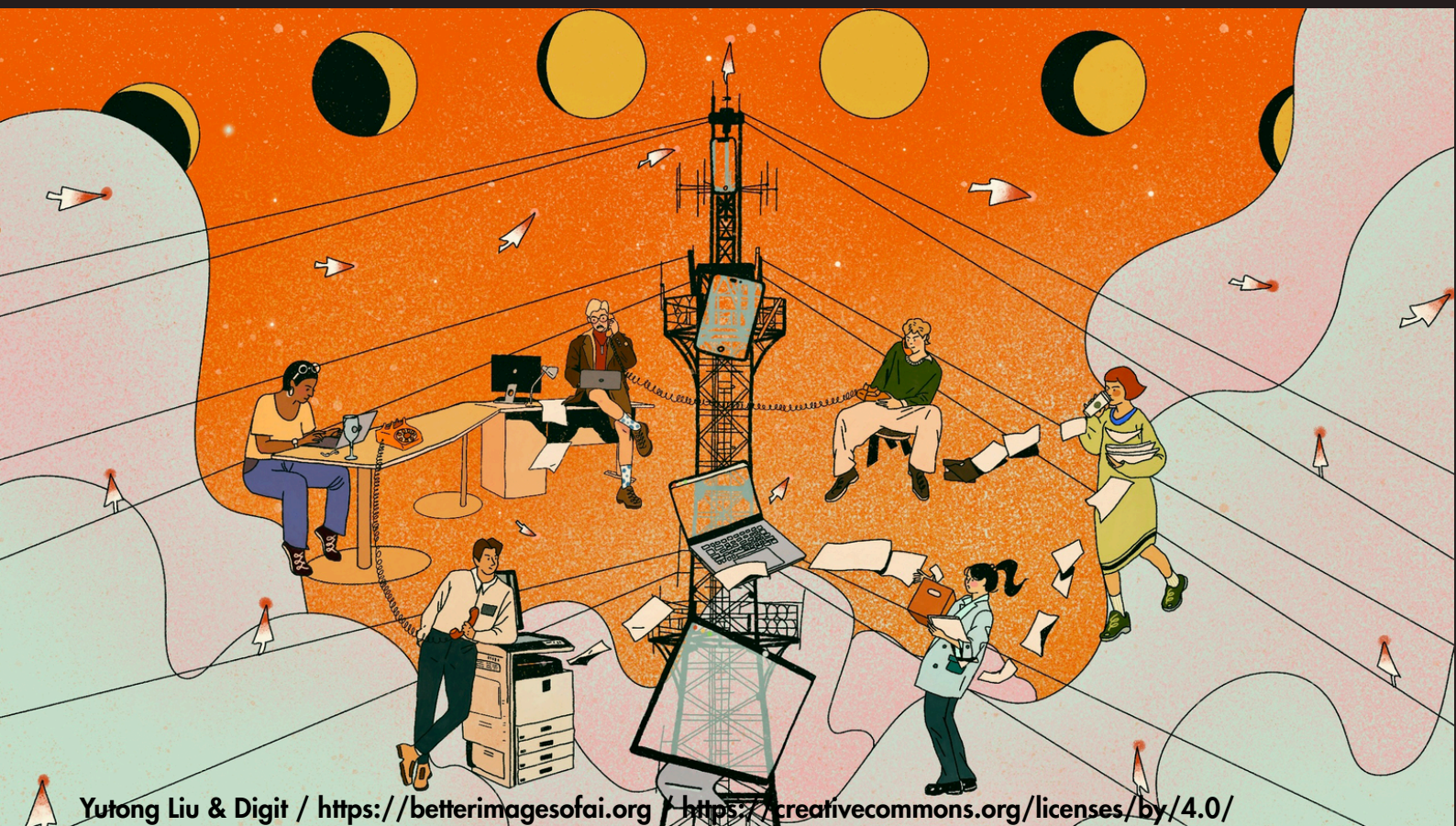
JCOTS Halloween 2026 Newsletter

This Year's *Spookiest* Science and Technology News

From a Wall Street Journal article entitled "AI's Scariest Week Yet" to comparisons between AI and nuclear safety to dozens of former developers coming out with concerns for AI innovation, the technological sphere is cloaked in an aura of apprehension. In an extra special Halloween edition of the JCOTS technology newsletter, we will dive deeper into some of the eeriest technology news from the past year.

Featuring ...

Is this the scariest AI analogy yet?
Grandma, what perfectly rendered big teeth you have!
Yes, your fridge IS conspiring against you!
The toys are listening
AI is in your head



Yutong Liu & Digit / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/



Lone Thomasky & Bits&Baume / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Is THIS the Scariest AI Analogy YET?

The AI Nuclear analogy has been tossed around for years, and yet has been gaining even more traction in the past month. This analogy argues for artificial intelligence regulatory frameworks to follow nuclear regulations. Ideas include instilling an IAEA for AI or an NPT for AI chips, granting international bodies further control of AI regulation. These models, however, are often disputed, with opponents arguing that AI and Nuclear are too dissimilar to allow for similar regulation.

Proponents, on the other side, argue that the extreme positive and negative capabilities of artificial intelligence systems echo those of nuclear energy, meaning conversations over how these regulations can be applied to artificial intelligence are informative.

Whether this argument holds true or not, the conversations surrounding it are eerie. Concerns center around whether or not AI holds an existential threat to humanity, and whether regulation is even possible. If the analogy holds true, however, looking to historical regulatory principles may be the key to unlocking a safe, secure, and innovative future.

Links

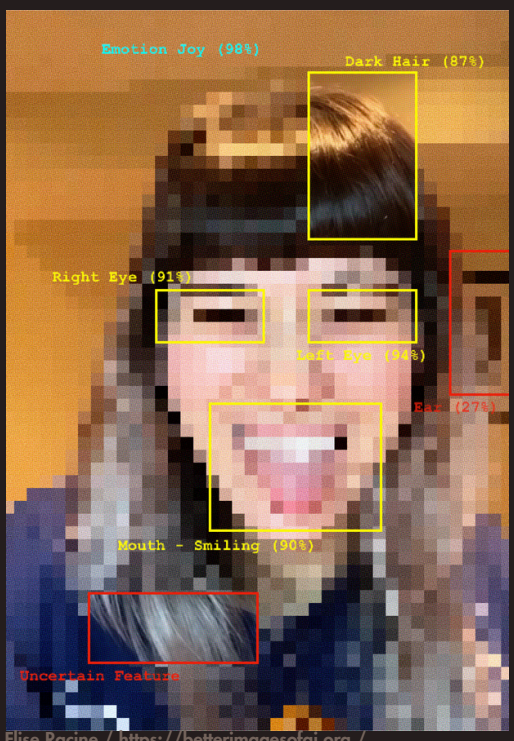
- AI Lawsuits
- What if AI Systems are the Forever Chemicals?
- The Trouble with the AI Nuclear Analogy
- Do AI Risks Require Intervention?

Grandma, What Perfectly Rendered Teeth You Have!

Deepfakes are not a new phenomenon, yet with the increased capabilities of artificial intelligence, their eminence and effectiveness is only rising. Deepfakes started as image altering — inputting one's face on another's body, changing someone's hair color, etc. — but have grown in recent years to include more complex alterations to photographs, as well as video and speech miming. This technology poses many potential challenges within society, which range from political campaign disinformation, to undermining evidential trust, to increasing psychological distress for those affected.

Due to the distress these forgeries may generate, detection mechanisms have been researched over the years. Potentially inaccurate artificial intelligence systems, analytical algorithms, and human based approaches have all been deliberated. Concerns over automated approaches have been raised in recent years, with beliefs that often it takes a person to recognize when something is instinctively unnatural. Because of this mistrust, experts in Deepfake detection are often called to testify whether or not images, audio, or video content is legitimate.

With the increased AI capabilities, however, the quality of deepfakes has risen to a point where experts with decades of experience are no longer able to trust their judgement. In an interview with the New York Times, the world's leading deepfake expert described this phenomenon as akin to "going blind," as once key giveaways disappeared, and forged information became evermore believable.



Elise Racine / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

Links

- AI Deepfake Expert
- AI In Elections
- AI Attack Ads
- AI Supercharging Scams

With detection mechanisms rendered obsolete, concerns for deepfake usage remain omnipotent. This apprehension, however, is heightened by the ways these falsities are being spread every day. If citizens cannot trust political campaigns to showcase accurate information about the candidates or news articles to show authentic images of a natural disaster, the confidence people have in their knowledge of the world around them erodes.

Yes, Your Fridge IS Conspiring Against You



Though rooted in less concrete evidence than some of the other newsletter anecdotes, recent research details the potential security concerns of smart home devices, including fridges, ovens, lightbulbs, doors, and more. This field, known as IoT (internet of things) forensics, recovers, preserves, and analyzes data collected from the internet of things.

The data collected from home devices may seem minimal, but covers a lot more than one may think. Smart fridges, for example, have been known to collect data regarding location, music taste, food currently in the fridge, temperature, and usage. Light-bulbs may collect data on when someone is in a room, smart-tvs collect data on when, where, and what you are watching.

These items are not inherently bad— smart refrigerators showcase recipes, shopping lists; smart light bulbs allow for schedules and cool colors; modern tvs combine streaming and cable services– but they add context to the growing debate around data privacy and security. What is the tradeoff between data privacy and efficiency? Between security and livability? These devices are vital parts of our everyday lives, things that are often impossible to circumvent, and yet they demonstrate legitimate examples of data collection and security concerns.

Links

- Smart Fridge Hacking
- Smart TVs

The Toys Are Listening



Robotic and electronic toys have been around for decades. Furbys, tamagotchis, dogs that you can really walk. This interactivity, however, has been scaled with some companies implementing artificial intelligence into their programming. This integration varies. From AI-driven "smart play" systems that use AI track children's movements so no controller is needed to follow along with the on-screen games, to AI voice-to-sticker makers that transform spoken ideas into colorable stickers. Integrative opportunities are endless and are being picked up by a variety of companies.

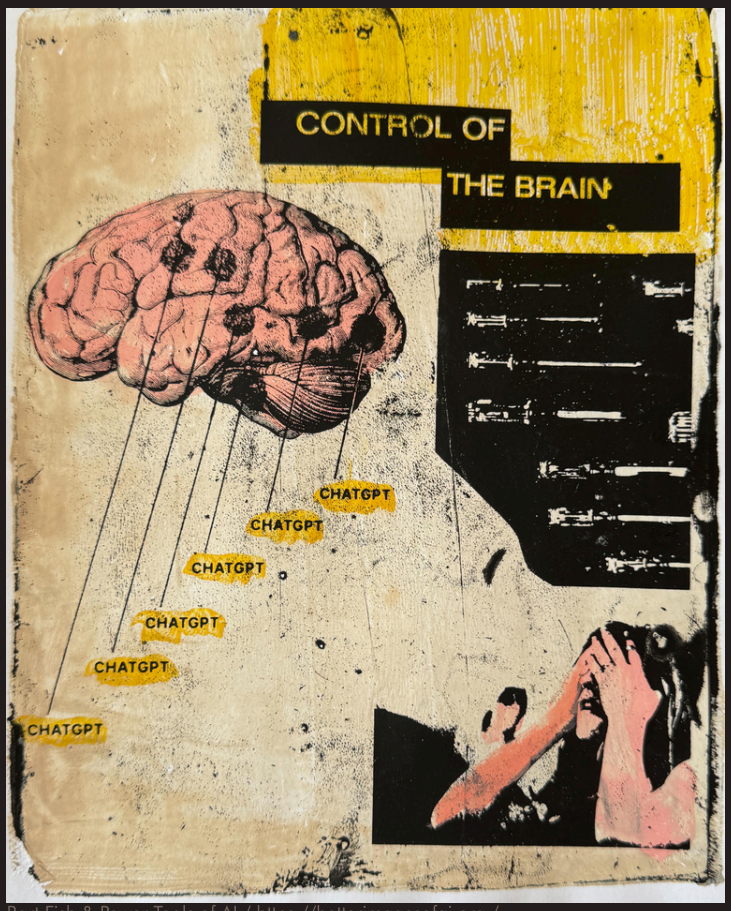
However, one version of AI integration has caused particular concern in the public sphere— AI chatbots in toys. These toys, which take the form of key-chains, stuffed animals, robots, and more, combine cute exteriors with communicative capabilities… because what kid wouldn't want to be able to talk to Teddy?

These chatbots, however, pose numerous concerns for child safety. Many of these concerns overlap with the JCOTS AI Chatbots: Companionship, & Minors study posted earlier this year. Some notable worries, however, concern chatbot access to the internet, even with restrictions, the potential for children to develop unhealthy attachments with chatbots, chatbots talking about adult topics — in one test, a stuffed teddy bear discussed issues such as sex and the Chinese Communist Party— and more. These developments can cause children to form unhealthy attachments with the toys, be exposed to explicit topics, and listen to AI opinions over those made by true, trusting, adults. This all proves that although AI integration in toys seems like a promising field, sparking a new era of play, it involves risks regarding child safety, privacy, and development.

Links

- Why AI Toys are Risky for Kids
- What AI Toys Talk About

AI is in Your Head



Bart Fish & Power Tools of AI / https://betterimagesofai.org / https://creativecommons.org/licenses/by/4.0/

If you could have any super power, which one would you choose? Flying? Mind-reading? Super strength? Teleportation? These hypotheticals aren't as far off as they'd seem. Brain-IT, a system developed by the Weizmann Institute of Science is able to replicate pictures people are looking at… by analyzing their brain activity.

The model, with only one hour of training per person, can recreate with frightening accuracy, an image— details, colors, and all. Although this isn't what is typically thought of as mind reading, the ability for researchers to reformulate exactly what someone is seeing, simply by looking at their brain, is a frightening prospect.

The models completed this task by splitting the brain into regions and recognizing how the regions responded to certain stimuli. This was to lessen the model confusion caused by variation in how people processed similar images. The encoder was able to determine which regions worked similarly, even if the regions were in separate areas of the brain.

Following this breakthrough in image recognition, scientists are hopeful that the next step is video. Video is difficult as images change multiple times a second while the scan takes two seconds. However, the possibilities for video analysis are vast. Could machines record your dreams?

Links

- AI Mind Reading Reconstructs What You're Looking At!
- Silicon Valley Wants Inside Your Head
- The New Science of Mind Reading

Terms to Know

1. **Deepfake**: Media where a person's likeness, face, or voice are manipulated or replaced using AI.
2. **IAEA**: The *International Atomic Energy Agency* is an intergovernmental organization used to regulate and control global use of nuclear weapons.
3. **IoT**: The *Internet of Things* is a network of physical objects with sensors, software, and network connections that allow them to collect and share information with the internet.

Jodi Kuhn, Executive Director
Kira Allmann, Chief Policy Analyst
Anna Dehmer, William & Mary Research Assistant

Contact Us
info@jcots.virginia.gov