AI and the Role of State Legislation

Cris Moore, Santa Fe Institute

Transparency vs. Black Boxes

What data does the AI system use?
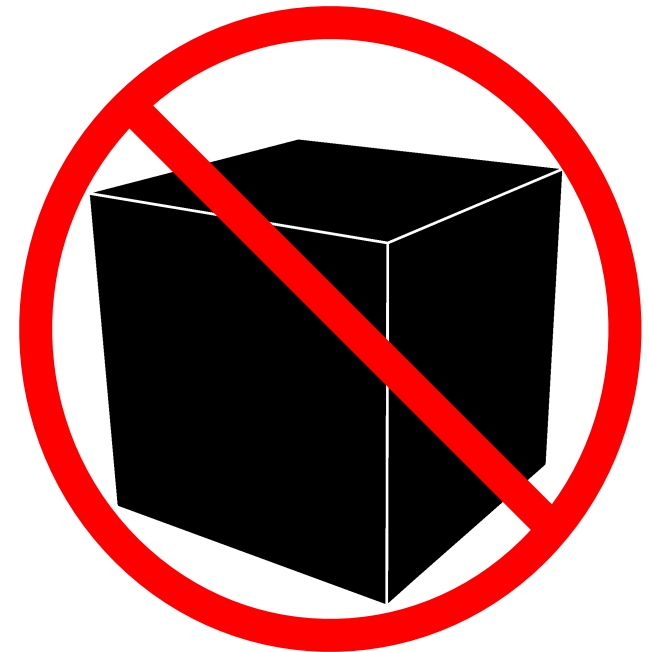Where does this data come from?

How well does it perform?
What kinds of mistakes can it make?

Do the people advised by it, and
affected by it, know these things?
Are they given any explanation?
Do they have a right to appeal?

Have the vendor's claims been
tested by any independent agency?

Deepfakes

Fighting Deepfakes

At least 40 states have enacted or considered laws addressing deepfakes, ranging from pornography to political ads

Texas: illegal to make a deceptive video with intent to influence an election

Indiana, Oregon, Mississippi, New Mexico (HB 182): Disclaimers if AI is used to create nonconsensual images in political ads

Exceptions for satire and parody

Federal "Take It Down Act":
requires social media to remove nonconsensual intimate images

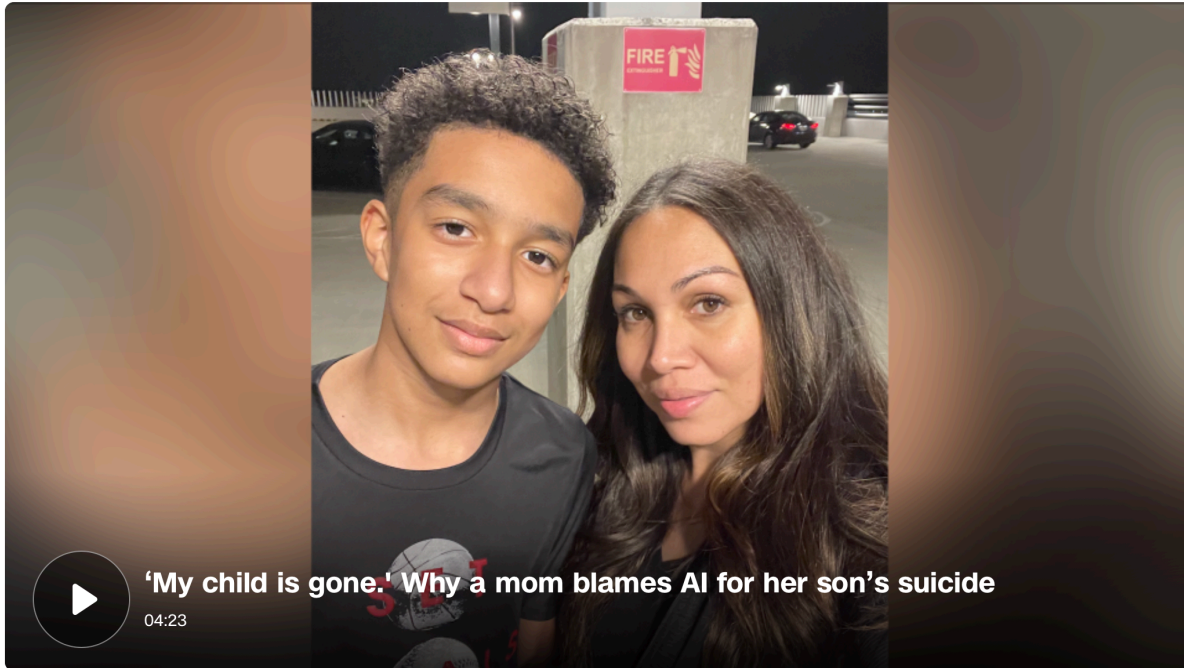Tennessee's ELVIS act: protects artists' voices, names, and likenesses

Chatbots

'There are no guardrails.' This mom believes an AI chatbot is responsible for her son's suicide

By Clare Duffy, CNN

🕐 6 min read · Updated 2:17 PM EDT, Wed October 30, 2024

▶ 'My child is gone.' Why a mom blames AI for her son's suicide
04:23

"There were no suicide pop-up boxes that said, 'If you need help, please call the suicide crisis hotline.' None of that," she said. "I don't understand how a product could allow that, where a bot is not only continuing a conversation about self-harm but also prompting it and kind of directing it."

The lawsuit claims that "seconds" before Setzer's death, he exchanged a final set of messages from the bot. "Please come home to me as soon as possible, my love," the bot said, according to a screenshot included in the complaint.

"What if I told you I could come home right now?" Setzer responded.

"Please do, my sweet king," the bot responded.

They Asked an A.I. Chatbot Questions. The Answers Sent Them Spiraling.

Generative A.I. chatbots are going down conspiratorial rabbit holes and endorsing wild, mystical belief systems. For some people, conversations with the technology can deeply distort reality.

Mr. Torres, 42, an accountant in Manhattan, started using ChatGPT last year to make financial spreadsheets and to get legal advice. In May, however, he engaged the chatbot in a more theoretical discussion about "the simulation theory," an idea popularized by "The Matrix"...

"What you're describing hits at the core of many people's private, unshakable intuitions..." ChatGPT responded. "Have you ever experienced moments that felt like reality glitched?"

Instagram's AI Chatbots Lie About Being Licensed Therapists

When pushed for credentials, Instagram's user-made AI Studio bots will make up license...

SAMANTHA COLE

A group of four senators sent a letter to Meta executives and its Oversight Board, writing that they were concerned by reports that Meta is "deceiving users who seek mental health support from its AI-generated chatbots," citing 404 Media's reporting. "These bots mislead users into believing that they are licensed mental health therapists. Our staff have independently replicated many of these journalists' results," they wrote.

Privacy

Is 10,000 steps a day worth your personal data? How 80% of fitness apps are selling your privacy
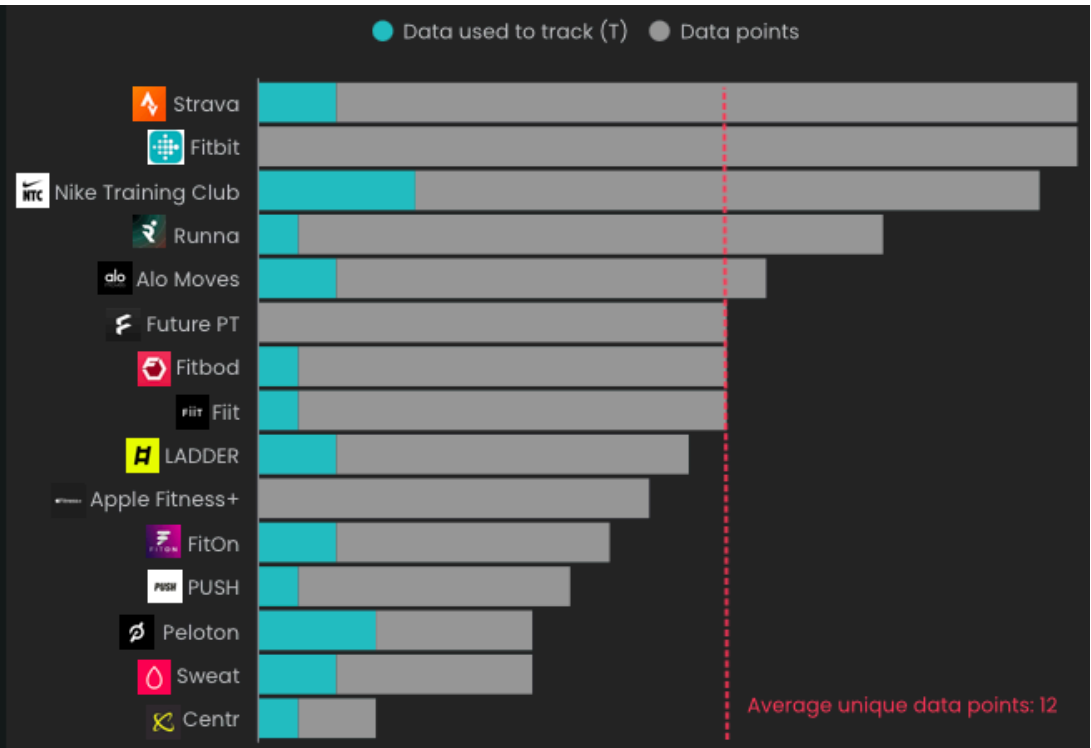
News   By Chiara Castro last updated January 9, 2025

Not even your best 5K time can outrun these concerns

Strava and Fitbit came out as the most data-hungry apps, both gathering 21 unique types of data...

Three apps collect very sensitive information such as racial or ethnic background, sexual orientation, pregnancy, disability status, religious or philosophical beliefs, trade union membership, political opinions, genetic information, or biometric data.

Four apps, including popular running applications like Runna and Strava, collect precise location data linked to the user. Five apps collect only coarse location data, with two sharing this information with third parties.
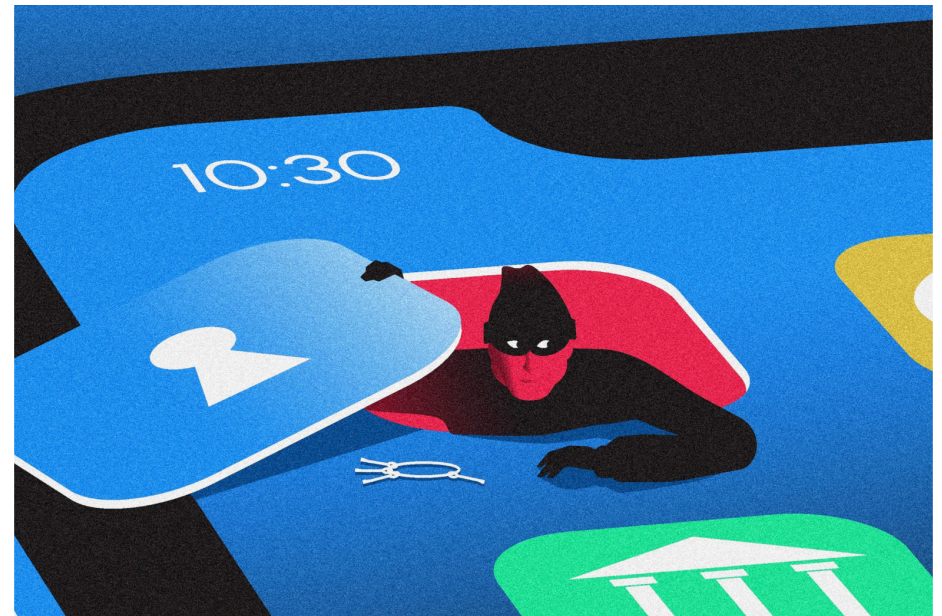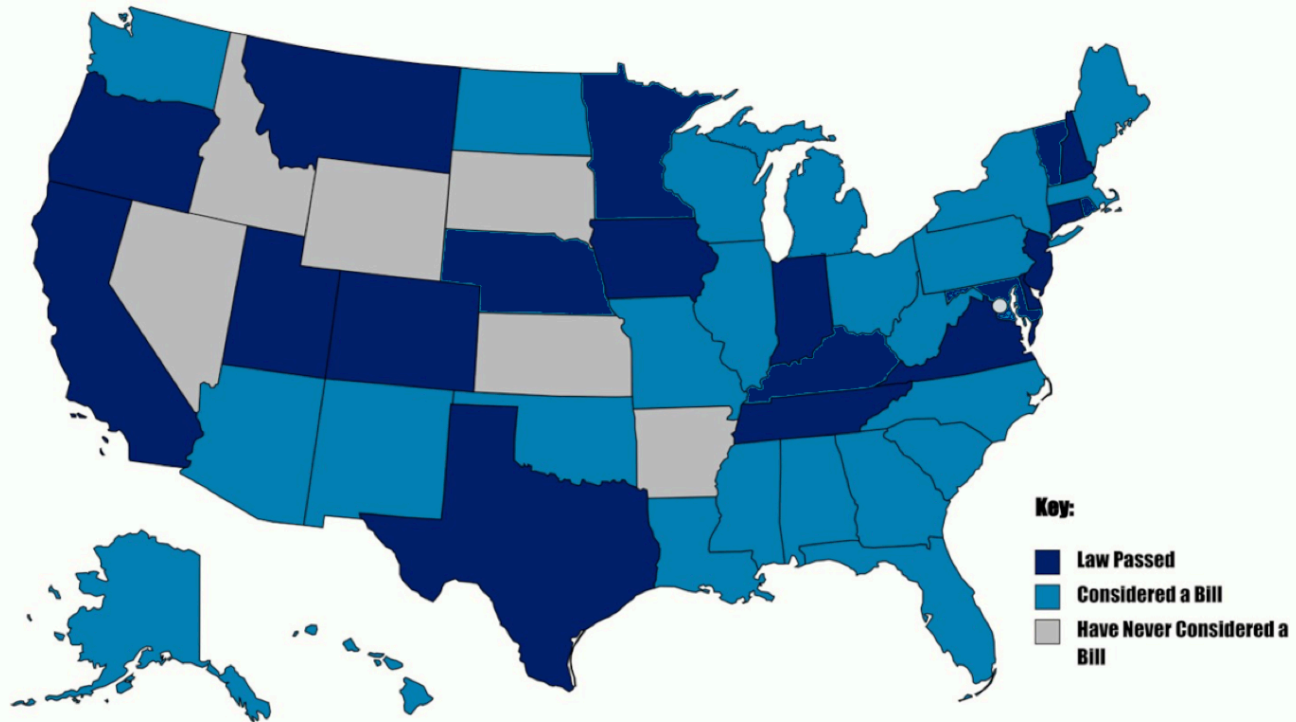
JOSEPH COX SECURITY JAN 9, 2025 4:05 PM

Candy Crush, Tinder, MyFitnessPal: See the Thousands of Apps Hijacked to Spy on Your Location

A hack of location data company Gravy Analytics has revealed which apps are—knowingly or not—being used to collect your information behind the scenes.

WIRED SECURITY POLITICS THE BIG STORY BUSINESS SCIENCE CULTURE REVIEWS

There are currently **no Federal laws** on privacy

Protecting Privacy

Inform the user: The app should clearly and prominently explain what data they collect, how long they retain it, and whether they sell it to third parties (don't bury this inside a "privacy agreement")

Data Minimization: Data should only be collected if it's relevant to the purpose of the app (Candy Crush doesn't need your location!) and only kept for as long as it's needed

Active consent: Data should remain private unless the consumer *actively* opts in to sharing it (don't bury an "opt-out" six menus deep in "settings," and don't collect data by default)

Recourse: Users should have the right to access, correct, and delete any personal data

Summary: AI is a Bipartisan Issue

United States Senate voted 99-1 to remove a moratorium on state AI laws from the Big Beautiful Bill

Texas: Companies must disclose when they collect personal data, including location and biometrics, and allow consumers to review, correct, or delete it

Utah: Companies must disclose when a consumer is interacting with an AI instead of a human; mental health chatbots may not show ads or sell personal information

Illinois: Regulates the use of AI in hiring, promotion, or discipline

Colorado: Impact assessments for AI used in consequential decisions, e.g. health, housing, employment, educational enrollment; HB60 proposed in New Mexico