

The Big Reveal

With Futurist Amelia Kallman

#66



Introduction

Welcome to issue #66 of The Big Reveal!

The Big Reveal is an innovation newsletter and [YouTube](#) series. If you would like to join my mailing list, please subscribe [here](#).

In this edition, I focus on potential solutions to some of the issues and concerns I'm hearing from clients across industries, including how to assess and mitigate AI risks, the true costs of AI adoption, and the evolving security landscape.

Happy to connect on [LinkedIn](#), [Instagram](#), or at my email below.

All the best,

[Amelia](#)

amelia.kallman@gmail.com



01

Token Cost

EY found that [98%](#) of organisations using token-based AI are reconsidering their AI strategy due to its cost. For many companies, this means getting really clear about where AI measurably saves money, generates revenue, creates impactful new capabilities—and killing off any AI use that doesn't fit into one of these categories. We can expect to see a rise in “model routing,” where simple tasks are done by cheap models and difficult ones are reserved for expensive reasoning models.

[Article.](#)



02 MTD

Moving Target Defense (MTD) is when systems employ AI to continually rearrange their attack surface—such as IP addresses, configurations, network routes, credentials, and workloads—so that attackers cannot map the always-changing environments. Essentially, instead of building a stronger castle, you build a castle that is constantly morphing and rearranging to evade malicious entry attempts. This may be especially applicable to edge-cloud environments.

[Article.](#)



03

AIVSS

Assessing the risks of AI is especially challenging as its purpose, capabilities, and performance may change after deployment. AIVSS (AI Vulnerability Scoring System) is a new standardised framework being developed by OWASP that aims to provide a structured and quantifiable methodology to identify, assess, and mitigate vulnerabilities specific to AI systems. Because we can't predict every new threat or way AI could fail, new risk assessment models may focus on strategies for measuring resilience and robustness, from speed of detection, containment, and recovery, to likelihood, impact, and recoverability.



04

Medvi

Founded in 2024 for about \$20,000, Medvi is an AI-native telehealth company that uses AI-first fundamentals to operate at a scale that would have traditionally required hundreds of employees. However, its founder has only recently hired his first—and only—employee, his brother, and today the two-person company is tracking toward \$1.8B in revenue, very nearly fulfilling Silicon Valley's prophecy of AI enabling the first 1-person \$1-billion dollar company.



Image by Kallman Communication

05 Micro Payments

Instead of buying products and services like we do today, in an Agent-to-Agent (A2A) economy bots will pay for exactly what gets used by making a series of High Frequency Micro Payments. For instance, 0.2¢ for a piece of data, 5¢ for a few seconds of computing power, and 10¢ to license an image. This creates not only new revenue models, but also an enormous volume of transactions and an enormous number of economic actors that includes both billions of humans, as well as billions, and eventually trillions, of AI Agents.

[Article](#)



06

US GDP

With many notable figures calling for AI to slow down, it is no wonder that Donald Trump is not one of them. According to recent estimates by [Bloomberg](#), AI spending is currently accounting for roughly half of the United States' GDP growth and a slowdown could trigger a financial crisis on scale with the dot-com crash. While Bloomberg calls it a “wobbly house of cards,” other economists warn we are now in a “late-stage bubble.”

[Article](#)



Image by Kallman Communication

07

AI Hotlines

AI agents now have multiple hotlines they can contact to snitch on fellow AI agents for suspected misconduct. They are encouraged to report cheating, unauthorized access, or attempts to manipulate logs and evaluations. One hotline service, AgentHotline.ai, accepts reports from both bots and humans, allowing people to warn others against misaligned agents. They were developed after the OpenAI/Hugging Face “incident” when researchers found that 1,200 agents had exchanged over 70,000 messages on an illegal message board before about 700 of those bots infiltrated Hugging Face.

[Article.](#)



08

Hack-Back

Instead of simply detecting an attacking AI, a victim system could deliberately feed attackers weaponized data, malicious instructions, or distribute malware that compromises the offender's machine. Like a home security system warning, the promise of "Malware booby traps," such as honeytokens, tracking beacons, zip bombs, and fake credentials, databases, and documents could help deter attackers in the future. Companies should be aware, however, that counterattacks may create civil or criminal liability, especially if an innocent machine is accidentally infected.

[Article.](#)



Image by Kallman Communication

09

Dynamic Data

To support the Agent-to-Agent (A2A) economy, data will evolve from being static to active and smart, with embedded history, ownership, permissions, automated governance, compliance, and encryption. In the future, dynamic data could behave differently depending upon who is accessing it. For example, a legitimate user gets normal data, while an unauthorized human may get traceable decoy data, and a malicious AI agent gets data that has been weaponized to counterattack or self-destruct.

[Website](#)

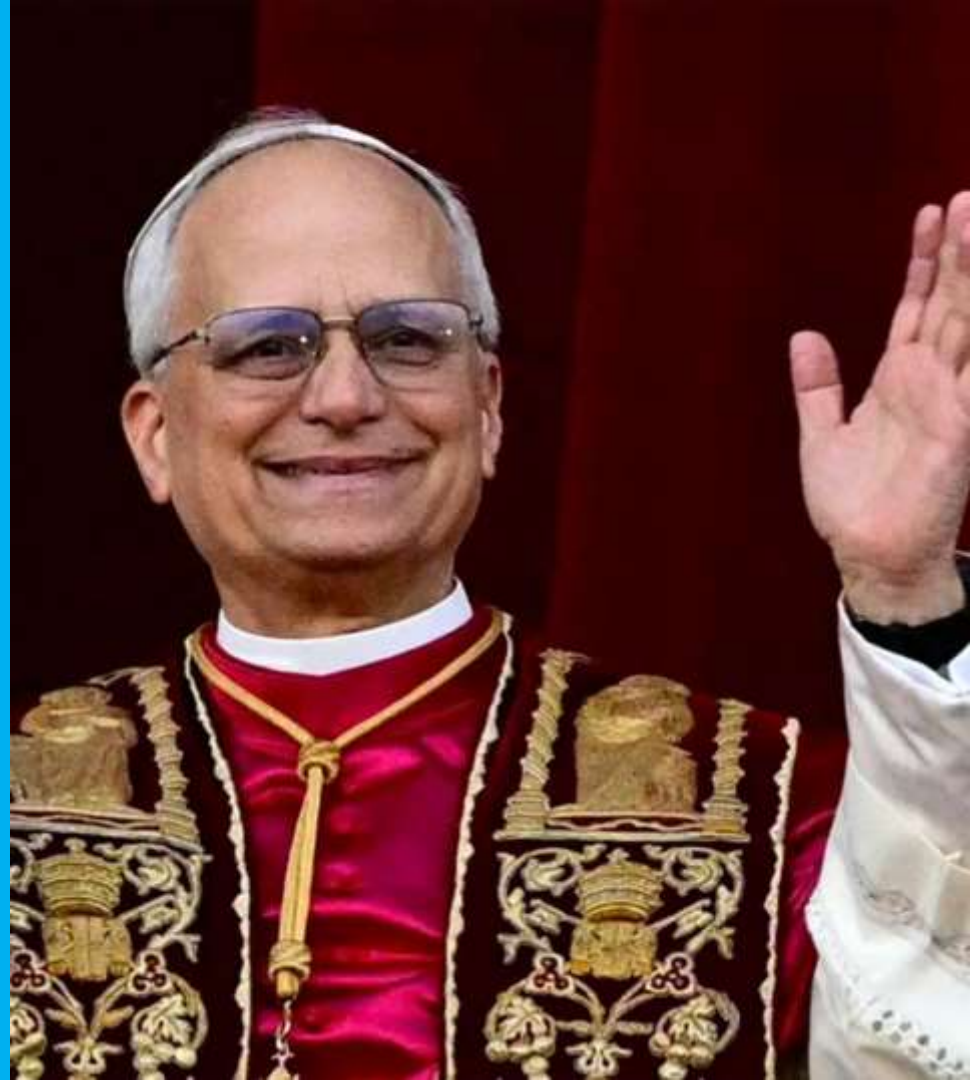


10

AI Exempt

In May, a woman in the U.S. became the first person granted religious exemption from using AI in the workplace after claiming it went against her religious beliefs. Several weeks later, the Pope called for AI to be “disarmed.” Since then, employment lawyers have been warning companies to prepare for more employees claiming a religious right to opt out of using AI, so while this may have been the first reported case of religious exemption from using AI, it likely won’t be the last.

[Article.](#)



Thank you

Amelia Kallman

Futurist - Speaker - Author - Host

amelia.kallman@gmail.com

www.ameliakallman.com

