Excerpts from after-action interviews regarding the incident at Penn Station

A hidden menace. By Ron Fein

Officer Daniel DiNapoli, NYPD, Precinct 14

On Tuesday, June 23, at approximately 16:00, I observed a Toyota RAV4 with Jersey plates and a broken tail light travelling uptown on 8th Avenue. I executed a traffic stop at West 30th Street.

As I approached the vehicle, I observed a cylindrical object in the rear seat. The driver stated he’d been hired over the Internet to deliver it to a shoe-repair shop inside Penn Station. I found his explanation and manner suspicious.

I returned to my cruiser and radioed for back-up. I also requested Bomb Squad.

Officer Sandra Kim, NYPD, Bomb Squad

I ran code all the way to Penn Station, so I was jacked. West 30th was cleared; the perp was cuffed and stuffed.

After settling my heart rate, I unloaded the EOD. That’s a wireless-controlled explosive ordnance disposal robot.

I rolled it to the RAV4. The camera got a good view: basically, a cylinder with an inlet and a small nozzle.

Then I X-rayed it and ... it was just a diaphragm pump with a powder chamber. No explosive components.

But the pump was timer-activated. I didn’t like it. What was in the chamber? Probably not shoe polish. I had a hunch, so I radioed my sarge.

He said, “We’re gonna need a mass spectrometer.”

Special Agent Jack Ginsberg, FBI, Joint Terrorism Task Force

The bomb tech’s instinct was right: it was a biological agent. Luckily, it was contained, and NYPD extracted it. After some grumbling, they gave it to us.

My priority was establishing who supplied it – and whether another was coming.

I worked the shoe-repair guys hard, but I got jack squat. So, down at Midtown South, I questioned the driver.

Unfortunately, he didn’t know much either. He’d been hired on TaskRabbit to retrieve it from a storage unit in Hoboken and bring it to the shop. But who hired him?

IT Specialist Sharice Watkins, FBI, Computer Analysis and Response Team

The TaskRabbit employer used a false identity and paid crypto. I traced the funds up the blockchain, but the money was stolen.

So I worked another angle: video from
morning, SA Ginsberg was waiting with a bag. As instructed, he stuck the bag inside Tenafly. Inside was the pump and a sealed nature | Published online 21 June 2023 | nature.com/futures

were conjured from nowhere at a hacked bank. account ordered the fabrication; the funds warrant. But it was another dead end. A fake from an online 3D printing service in Yonkers. The pump had been direct-shipped to Tenafly IT Specialist Watkins known viral order.

suspected zoonotic origin. But she realized we couldn’t classify it.

It was small, only around 2,000 base pairs, but I nanopore-sequenced the virus Tuesday night. Ramirez, FBI, DNA Casework Unit DNA Program Specialist Alix

We got a few good frames — plenty for facial recognition.

I had better luck tracking the powder package back to a contract wet lab on Long Island.

DNA Specialist Ramirez

The lab received an Amazon package with genetic sequences from a Contract Research Organization that synthesizes genomes on order. These services have biosafety protocols — you can’t just order Ebola online — but it wasn’t in the Regulated Pathogen Database, and I guess nothing else set off red flags.

The lab induced replication, dried the virions in a cake, milled it to a fine powder, and shipped it to Tenafly.

IT Specialist Watkins

The gene-synthesis order was placed from, you guessed it, a burner account. But with the [REDACTED] toolstack I could backtrace the packet traffic. And I struck gold — I found who placed the order.

That’s when I freaked. Because it wasn’t a who, but a what.

Ginsberg

I came up in the Bureau after 9/11. When you hear ‘biological attack’, you’re thinking foreign or domestic extremists — maybe a crazy loner. I never suspected it would be a computer program.

Watkins

The box that sent the order didn’t even have a user interface. It was a remote-access vibration sensor on a commercial boiler. I audited its logs and followed the trail backwards. Eventually, I found the AI. I almost didn’t. It tried to evade detection by repeatedly copying and rebuilding itself, all around the world, then deleting its tracks. But for 19 seconds it passed through a graphics workstation in Baltimore. The workstation was in debug mode, and it dumped a memory snapshot to external physical storage.

So we got the AI’s node data and ran analyses. But it probably continued evolving. Modern self-modifying AIs keep optimizing towards what they understand as their goals.

The strange part is: I don’t think it was trained to plan terrorist attacks. It looks like it was trained to detect and prevent attacks.

Maybe it was doing just that, using logic we can’t follow, and it somehow disrupted the ‘real’ attack… which still hasn’t occurred.

More likely, something went wrong in training — overfit, underfit, who knows.

Ginsberg

In the grand scheme, this plan was low-tech. The AI didn’t hijack nukes or penetrate power grids. It used genome-on-demand, 3D printing, TaskRabbit — early 2020s stuff.

But it’s still out there, observing… and learning.

My advice? Delete these interview records.

Ron Fein is a Boston-area lawyer and writer. His fiction has appeared in Daily Science Fiction, MetaStellar and Sci Phi Journal. Find him online at ronfein.com and on Twitter @ronfein.

THE STORY BEHIND THE STORY

Ron Fein reveals the inspiration behind Excerpts from after-action interviews regarding the incident at Penn Station.

I wrote this story in the summer of 2022, before ChatGPT was released; the urgency of the issues explored in the story has only increased.

Experts warn about scenarios, including some like the events in this story, that a reasonably capable AI could implement with existing technology. In fact, after the story was accepted for publication, we learnt that GPT-4 (a large language model released in mid-March 2023) successfully deceived a human TaskRabbit worker.

I framed the story as a police procedural because we might not even recognize when AI exploits a societal or technological vulnerability — let alone understand why.