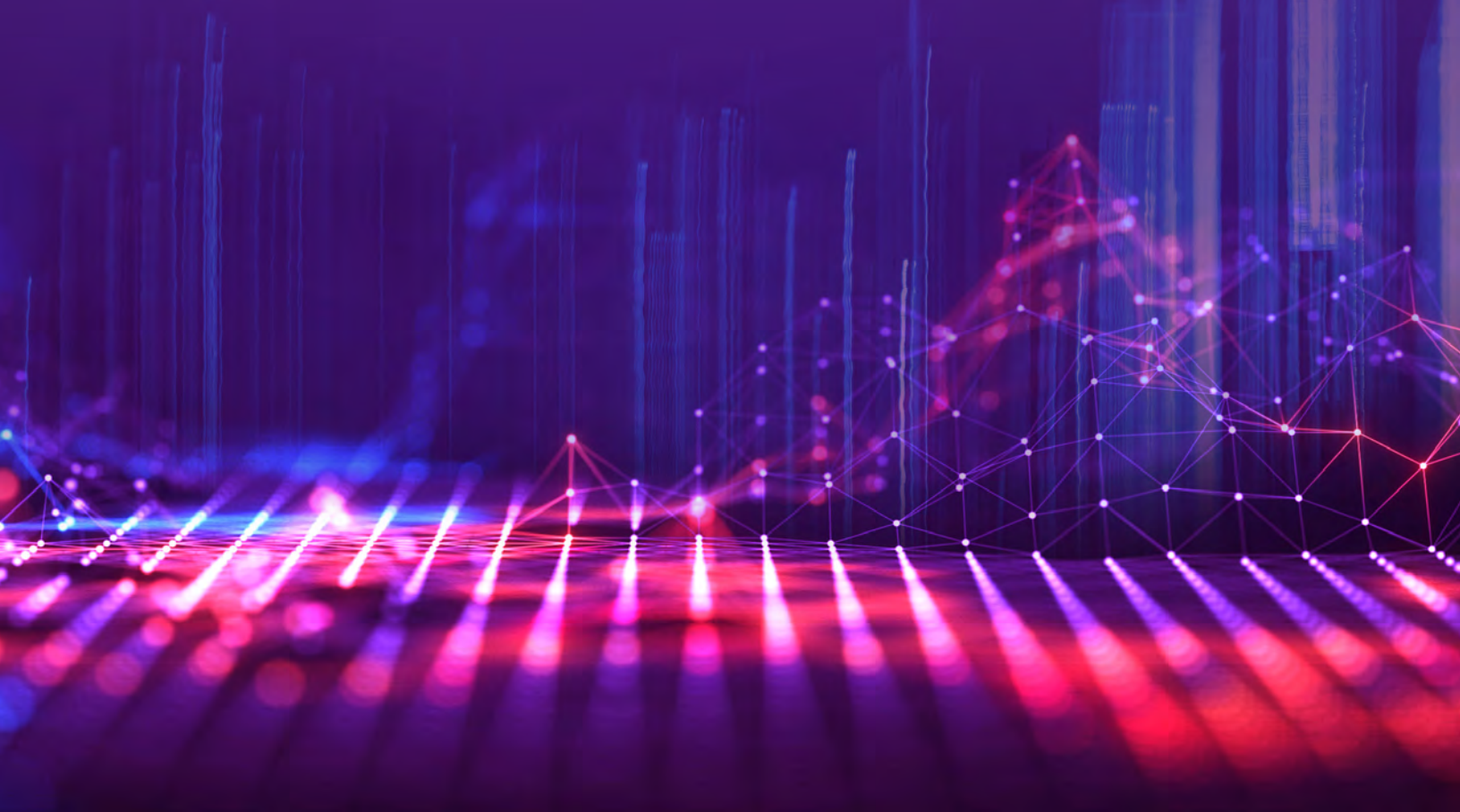
NYU

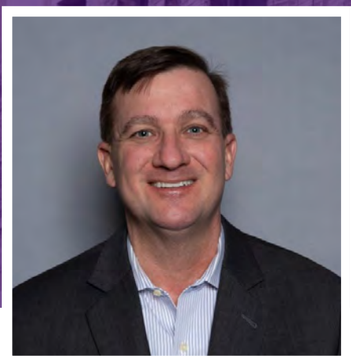
NYU Langone Health

Technology Opportunities & Ventures

2025 Annual Report



Welcome Message



Technology Opportunities & Ventures (TOV), NYU's technology commercialization unit, reported another record-breaking year for innovation and research translation across NYU and NYU Langone Health.

Serving all University campuses, colleges, and schools, TOV works to translate discoveries from NYU's $1.5 billion research enterprise into commercial solutions that maximize social and economic impact. In FY 2025, TOV received a record number of innovation disclosures, launched a record number of startups based on NYU technologies, and executed a record number of licensing agreements with organizations commercializing NYU research.

Innovation Disclosures
Filing an innovation disclosure with TOV is the first step in the commercialization process. It enables researchers to describe their discoveries, supports intellectual property protection, and helps identify potential industry partnerships.

In FY 2025, TOV received a record 431 innovation disclosures—an increase of 16% from the 373 disclosures submitted in FY 2024. The growth reflects NYU's commitment to fostering a culture of innovation and commercialization and advancing University discoveries toward real-world applications.

Startups Launched
Over the past 40 years, NYU researchers have participated in the formation of more than 250 startups. In FY 2025, TOV launched a record 20 new companies based on NYU innovations.

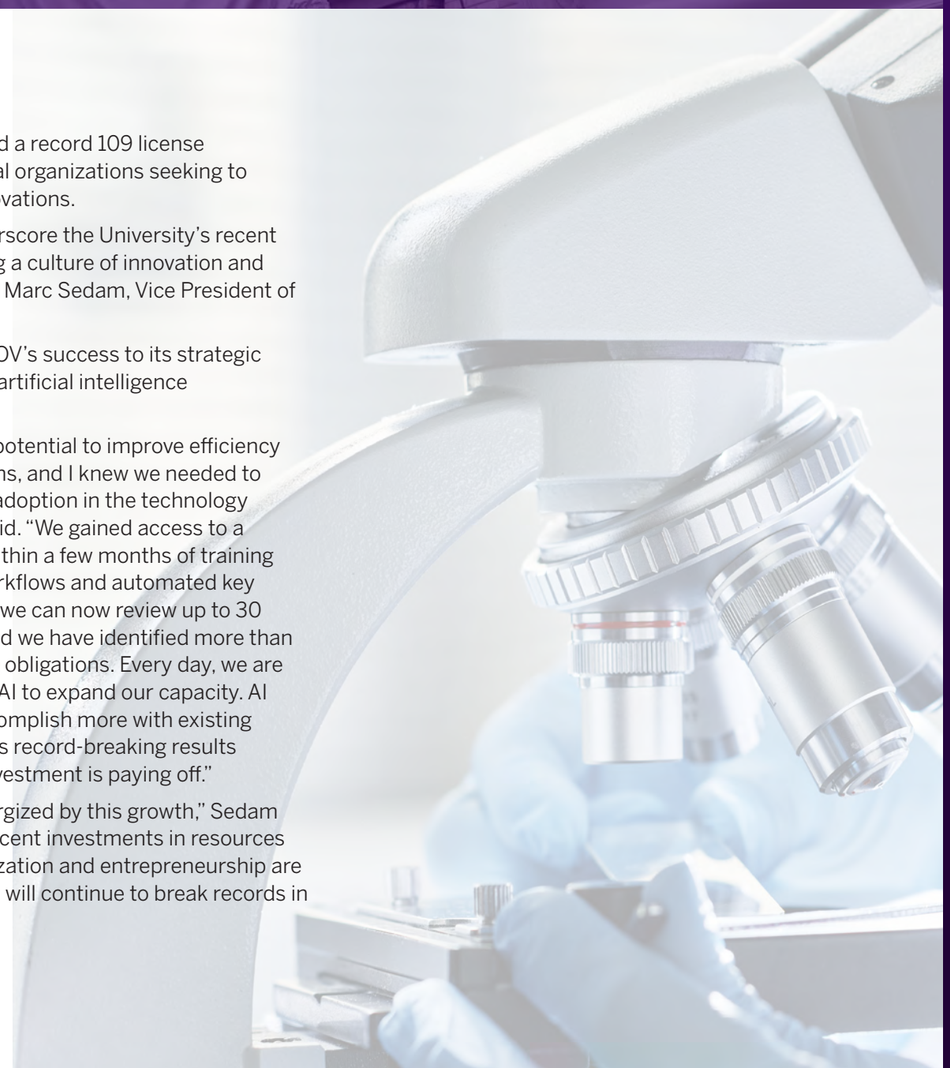
License Agreements
In FY 2025, TOV executed a record 109 license agreements with external organizations seeking to commercialize NYU innovations.

"These milestones underscore the University's recent commitment to fostering a culture of innovation and commercialization," said Marc Sedam, Vice President of TOV.

Sedam also attributes TOV's success to its strategic investment in emerging artificial intelligence technologies.

"I immediately saw AI's potential to improve efficiency and streamline operations, and I knew we needed to be at the forefront of AI adoption in the technology transfer field," Sedam said. "We gained access to a secure AI system, and within a few months of training it, it transformed our workflows and automated key processes. For example, we can now review up to 30 agreements per hour, and we have identified more than $1 million in outstanding obligations. Every day, we are finding new ways to use AI to expand our capacity. AI enables our team to accomplish more with existing resources, and this year's record-breaking results demonstrate that the investment is paying off."

"We are excited and energized by this growth," Sedam added. "It is clear that recent investments in resources supporting commercialization and entrepreneurship are working, and I expect we will continue to break records in the years ahead."



Another Record Year

431
Innovation Disclosures

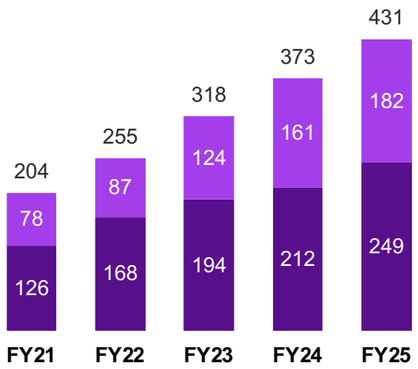
20
Startups Launched

109
License Agreements

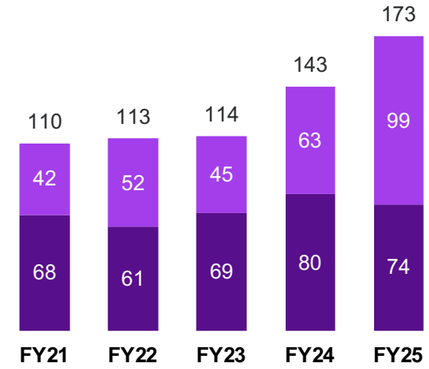
During fiscal year 2025, TOV received a record number of new innovation disclosures, launched a record number of startups based on NYU innovations, and signed a record number of licensing agreements with companies looking to commercialize NYU research outputs.

By the Numbers

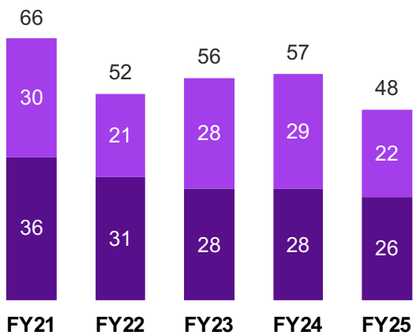
Five-Year Breakdown



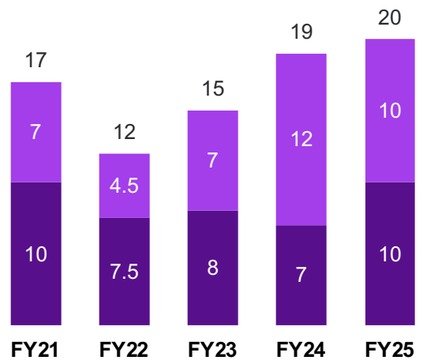
Innovation Disclosures



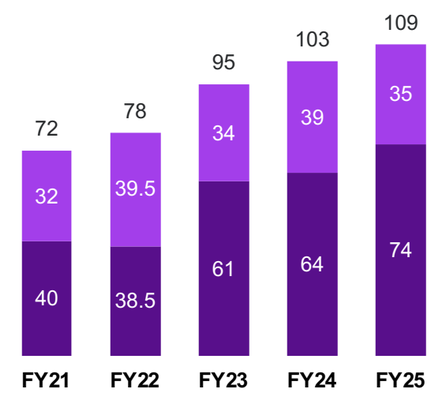
US Patents Filed



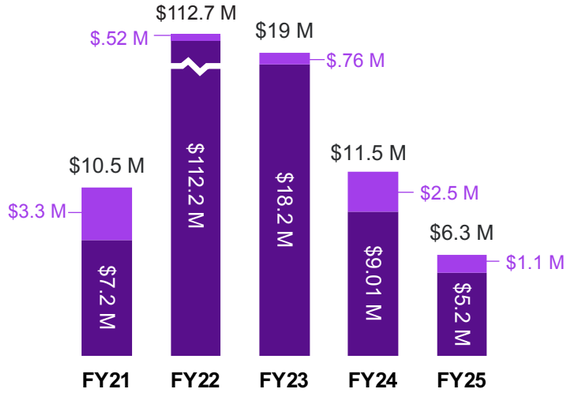
US Patents Issued



Startups Formed



Licenses & Options



Licensing Revenue

NYU Grossman School of Medicine
New York University

New Ventures

FY2025 Startups

Antilope Biosciences
Genetic biomarkers of immune checkpoint inhibition response
NYU Grossman School of Medicine

CardioSpring
Detachable cardiac pacing wire solution
NYU Grossman School of Medicine

CaroRhythm
Outpatient stroke patient monitoring device
Tandon School of Engineering

Cassette Genomics
Genetic system to selectively generate single-sex chicken
NYU Grossman School of Medicine

Glaucus
Biosensing nanotech solutions for at-home diagnostics
Tandon School of Engineering

Heartsounds Labs
AI for detecting fetal heart block
NYU Grossman School of Medicine

Innomune Biologics SAS
Biological and chemical sensing
Tandon School of Engineering

Intercept Tx
Rage Inhibitor technology for the treatment of diabetic nephropathy and other diabetic complications
NYU Grossman School of Medicine

Invenio Imaging
Fresh tissue imaging with NIO laser imaging system
NYU Grossman School of Medicine

MirnaCure Therapeutics
microRNA analog technology for hypercholesterolemia
NYU Grossman School of Medicine

Mobile Defender
Detection of hidden cellular GPS vehicle tracker
Tandon School of Engineering

MoveMend
Motion tracking immersive exercise programs
NYU Grossman School of Medicine

Neptune Biotech
A flexible method for combinatorial pooled CRISPR Cas13 RNA targeting screens and multimodal single-cell profiling
Arts & Science

Novel AI Technologies Corporation
Wearable health data and AI-driven analytics providing predictive risk insights and cost-reduction solutions for insurance companies
Tandon School of Engineering

OsseiMimetic
Implants with enhanced bone ingrowth
College of Dentistry

Regerna Therapeutics
Muscle regenerative therapies
NYU Grossman School of Medicine

Riffit
AI-assisted text-to-song platform
Courant Institute of Mathematical Sciences

The Sequel Institute
Computational neuroscience and AI
Arts & Science

Velai Health
Artificial intelligence tools for enhancing continuity of care for cardiac patients
Courant Institute of Mathematical Sciences

Ximio Health
Cardiopulmonary resuscitation device
NYU Grossman School of Medicine



Mobile Defender

Mobile Defender is a new NYU hardware and software automotive cybersecurity startup focused on GPS security, from protecting individuals against covert GPS tracking and cyberstalking to defending vehicles and fleets against GPS signal manipulation.

Founded by NYU Tandon School of Engineering PhD candidate and cybersecurity expert Moshe Satt, Mobile Defender is developing technology that addresses two distinct GPS-related threats: hidden cellular GPS trackers used in cyberstalking, and GPS signal spoofing used to manipulate vehicles and fleets. The company's tracker detection work is focused on empowering victims, particularly survivors of domestic violence, to regain control, safety, and peace of mind.

A recent report from the Bureau of Justice Statistics estimates that in the U.S. alone, roughly 400,000 people each year are stalked using inexpensive, easily concealed tracking devices. Unlike Bluetooth-based trackers such as Apple AirTags, which now trigger alerts on most smartphones, cellular GPS trackers operate silently and invisibly, often magnetically attached to vehicles and capable of tracking victims anywhere. These devices have been linked to numerous violent crimes, including intimate partner homicides. Yet until now, no consumer-accessible solution has existed to detect them.

Satt's path to entrepreneurship began after more than two decades in public service for the City of New York. A longtime Chief Information Security Officer (CISO), including serving as CISO and HIPAA Security Officer at the New York City Fire Department during the height of the COVID-19 pandemic, Satt returned to school in his forties to complete a master's in cybersecurity at NYU Tandon. He is now a part-time PhD student and an adjunct professor teaching multiple cybersecurity courses. Mobile Defender emerged from Satt's doctoral research in NYU Tandon's mLab, led by Professor Danny Huang, which focuses on building tools to address real-world security and privacy threats in healthcare and consumer technologies. While researching digital stalking and location-based threats, Satt identified a critical gap: while major technology platforms had addressed Bluetooth tracking, cellular GPS tracking remained completely unaddressed.

"The reality is chilling," Satt explains. "In many cases, tracking is the first step before violence. These devices are cheap, easy to buy online, and incredibly powerful in the wrong hands. If someone knows they're being tracked, they have a chance to get help."

Satt's research resulted in a peer-reviewed paper accepted to the USENIX Symposium on Vehicle Security and Privacy (VehicleSec), where it drew immediate attention from domestic violence advocacy organizations and industry stakeholders. The work also caught national media attention, culminating in a CBS News investigative report highlighting the real-world consequences of GPS stalking and the promise of Mobile Defender's technology.

Mobile Defender's core innovation is protected by two patents owned by NYU and exclusively licensed through TOV's Express License program. The first covers the detection of covert cellular GPS trackers. The second addresses GPS spoofing, a growing cybersecurity threat in which attackers manipulate GPS signals to mislead vehicles, fleets, or navigation systems. GPS spoofing is increasingly being used by criminal networks to facilitate cargo theft, masking route diversions so that shipments can be stolen before a fleet even knows something is wrong. North American cargo theft losses reached an estimated $6.6 billion in 2025, with confirmed incidents rising 18 percent year over year and average theft values climbing 36 percent to nearly $274,000 per incident. GPS spoofing is also a concern for connected and autonomous vehicle safety and is now explicitly covered under UN Regulation R155, which mandates cybersecurity protections for vehicles sold across much of Europe and Asia.

Together, these technologies position Mobile Defender at the intersection of personal safety, cybersecurity, and transportation security, with applications ranging from consumer protection and survivor advocacy to fleet security and automotive systems.

At launch, the company is focused on developing a proof-of-concept mobile application, beginning with Android devices, to demonstrate the technology's effectiveness and enable pilot testing with advocacy partners. The long-term vision, however, goes beyond an app.

"A survivor shouldn't have to download something to be safe," says Satt. "Just like Bluetooth tracker detection is now built into phones, this kind of protection should ultimately be embedded into operating systems, vehicles, and connected devices."

Mobile Defender has worked closely with TOV to patent and license its technology and has leveraged multiple NYU innovation resources, including the Tech Venture Workshop at the NYU Leslie Entrepreneurial Institute. The company is currently participating in the NYU Entrepreneurs Challenge while exploring non-dilutive funding, strategic partnerships, and licensing opportunities.

As the company moves forward, its mission remains clear.

"This isn't about building technology for technology's sake," Satt says. "It's about saving lives and giving people the freedom to live without fear."



Left to right, Maitry Dave, Tandon '26, Mo Satt, Tandon '28, Sarah Krueger; Mobile Defender team for the 2026 Entrepreneurs Challenge cohort.



GPS spoofing is a growing cybersecurity threat in which attackers manipulate GPS signals to mislead vehicles, fleets, or navigation systems. GPS spoofing is increasingly being used by criminal networks to facilitate cargo theft, masking route diversions so that shipments can be stolen before a fleet even knows something is wrong.