

A NEXT CANADA PUBLICATION

GRIT

ED. 15
FALL 2024

TOP SECRET

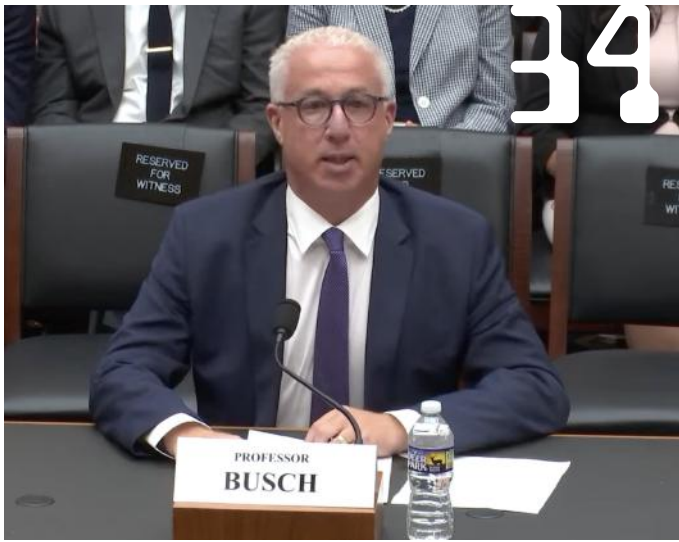
Data security
in today's
digital realm





CONTENTS

- | | | | |
|----|---|----|--|
| 04 | Letter from the CEO Kyle J. Winters | 20 | Two Steps Ahead Featuring Jonathan Roy |
| 06 | Contributors | 22 | Levelling the Playing Field Featuring Fion Lee-Madan |
| 08 | Soaring Securely in a Boundless Digital Age Air Canada | 24 | The Clinician's Scribe Featuring Mahshid Yassaei |
| 10 | Bienvenue! A conversation with NEXT AI Montréal Executive Director: Brian King By Adam Palter | 26 | Plain, Simple, Secure. Featuring Ezzeldin Tahoun |
| 14 | Securing Innovation: Why Cybersecurity Matters for Entrepreneurs By Carlos Chalico, EY | 28 | Safe-Guarding Digital Futures Featuring Jennifer Arnold |
| 18 | Unlocking AI with Privacy Featuring Patricia Thaine | 30 | SIM Swapping: The Silent Threat and Your Solution Featuring Haseeb Awan |
| | | 32 | Guardians of Data: Aaron Le on Hatch's Security Vision Featuring Aaron Le, Hatch |



TOOTHPOD



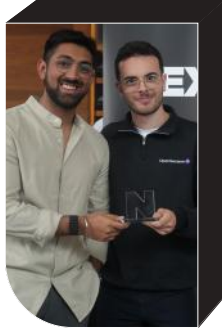
AVENUE STORIES



MANEVA



MY DORM STORE



OPENSesame



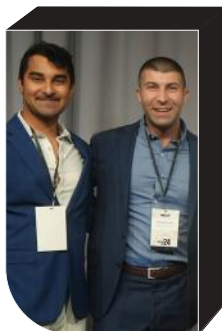
EPILOID BIOTECHNOLOGY



ANALYST3



AFAIK.IO



TENOMIX



QUANTOFLOW

42 10 FOUNDERS TO WATCH



34 **NEXT Canada's Secret Sauce (Our World-Class Faculty)**
Featuring Prof. Marc Busch

36 **Protect Your Startup in 5 Easy Steps**
By Nir Mofet, BDC

38 **Conversations with Leadership Volunteers: Dharmesh Gandhi**

40 **Who's Listening to What**

42 **10 Founders to Watch**
By Fletcher McLaughlin

44 **Community News**
Featuring NEXT Alumni



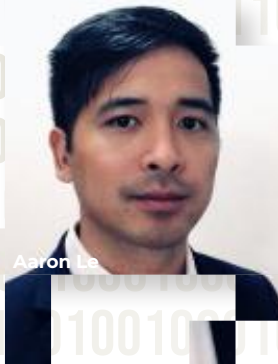
Jennifer Arnold



Mahshid Yassaei



Fion Lee-Madan



Aaron Le

DEAR GRIT READERS,



WELCOME TO THE FALL 2024 ISSUE OF GRIT MAGAZINE!

As I sat down to write this introduction, I was reminded of a humbling moment a few months ago. Imagine this: our IT security lead walking past my desk, only to spot a not-so-subtle Post-it note with what could only be my password scrawled on it. One sheepish conversation later, he had devised a whole enterprise security plan for NEXT Canada, sparking a new level of data security for our team. Consider it a win for everyone (and a well-deserved lesson for me).

This issue is dedicated to the ever-evolving world of privacy and data security, a topic that has become increasingly important for organizations of all shapes and sizes. We're thrilled to highlight several NEXT Canada alumni who are making waves in this critical space, leading innovative projects that safeguard data while enhancing efficiency.

First up, Jennifer Arnold from Minerva shares how her company is revolutionizing anti-money laundering (AML) processes. Minerva leverages intelligent automation to accelerate risk screening and investigations, making these efforts 300 times faster than traditional methods. Not only does this reduce backlogs, but it also ensures that companies remain compliant with regulatory standards, which is no small feat in today's fast-paced financial world.

Next, we have Mahshid Yassaei from Tali AI, who is tackling inefficiencies in healthcare documentation. Tali AI's voice assistant is a game-changer for clinicians, saving them roughly 20 hours each month on administrative tasks. This means more time for patient care and less time grappling with paperwork, which has already transformed the clinical experience for countless users.

Lastly, Fion Lee-Madan from Fairly AI takes us through her company's mission to build automated governance and control mechanisms for AI applications. As AI becomes more embedded in our daily lives, ensuring that these systems are secure, fair, and compliant is essential. Fairly AI's work ensures organizations can trust their AI applications, even as regulatory landscapes evolve.


Our community partner, Aaron Le from Hatch, also shares his insights on delivering innovative product capabilities while maintaining a robust focus on data privacy.

I hope you enjoy this issue. Don't forget to stay connected with us on social media or drop by our Toronto or Montreal offices. Happy reading!

Warm regards,



Kyle J. Winters
CEO, NEXT Canada



“ NEXT Canada helped me acquire new skills and business acumen. I became stronger and more confident as a founder and as an individual. I donate to NEXT to help future entrepreneurs gain valuable experience and resources. ”

LEXI KAPLAN (NEXT 36, 2016)

Visit www.nextcanada.com/donation/
to make a donation today.

NEXT Canada accelerates the growth trajectory of aspiring anscaling entrepreneurs with education, mentorship and access to Canada's strongest entrepreneurial network.
Charitable Registration No. 81519 8403 RR0001



1. FLETCHER MCLAUGHLIN

Fletcher McLaughlin is the Program Coordinator for NEXT Canada. He assists in setting up the programming and provides support to founders across all three cohorts. Fletcher has worked with a diverse range of startups and has been involved with various accelerators within the Canadian ecosystem. He has a passion for studying resources that have been directly applied to building startups, including Paul Graham’s essays, YC’s content library, and Clayton Christensen’s work. Additionally, he enjoys developing tools that help founders measure and optimize product-market fit and growth.

2. ADAM PALTER

Adam Palter holds a B.A. in History from McGill, a Master’s Degree in Management Innovation and Entrepreneurship from Queens University’s Smith School, and an MBA from Rotman, at the University of Toronto. Prior to joining NEXT Canada as a Venture Manager, he contributed to Toronto’s innovation ecosystem in various roles with technology accelerators, early-stage capital allocators, consulting independently, and as Co-founder and CEO of a start-up in the neurodegenerative disease diagnostics space. Various obsessions include Keith Jarrett’s jazz mastery, Karl Friston’s theory of Active Inference, and old grainy films with subtitles.

3. KAI RONCERIA

Kai Ronceria is an emerging filmmaker and creative with a passion for storytelling through media. His diverse skill set spans photography, videography, editing, concept development, and even marketing. Starting as an intern, Kai is now a Marketing Coordinator at NEXT Canada, where he both supports the team’s projects and undertakes his own. In his free time, he enjoys walking or lounging outside, discovering new music, becoming lost in the world of games, and of course enjoying a delicious meal. You can find snippets of his creative projects via his instagram @keyebuh

GRIT

A NEXT Canada Publication
GRIT, Edition 15; Fall 2024
“Top Secret”

175 Bloor Street East, Suite 1800, South Tower
Toronto, ON M4W 3R8
NEXTCANADA.COM

6795 Rue Marconi, Suite 200
Montréal, QC H2S 3J9

PUBLISHER

NEXT Canada
Kyle J. Winters, CEO

EDITOR

Jaskaran Chauhan

GUEST EDITOR

Adam Palter

DESIGN DIRECTOR

Eng C. Lau

MARKETING COORDINATOR

Kai Ronceria

NEXT CANADA

At the heart of our alumni success lies our premier programming:

NEXT36

For students and recent grads launching their startups.

[LEARN MORE](#)

NEXTAI

For AI-enabled ventures looking to disrupt industries.

[LEARN MORE](#)

NEXTFOUNDERS

For founders of revenue generating ventures looking to scale.

[LEARN MORE](#)

NEXTALUMNI

Events and programs to support lifelong founder development.

Be the first to receive GRIT.

[JOIN THE MAILING LIST](#)



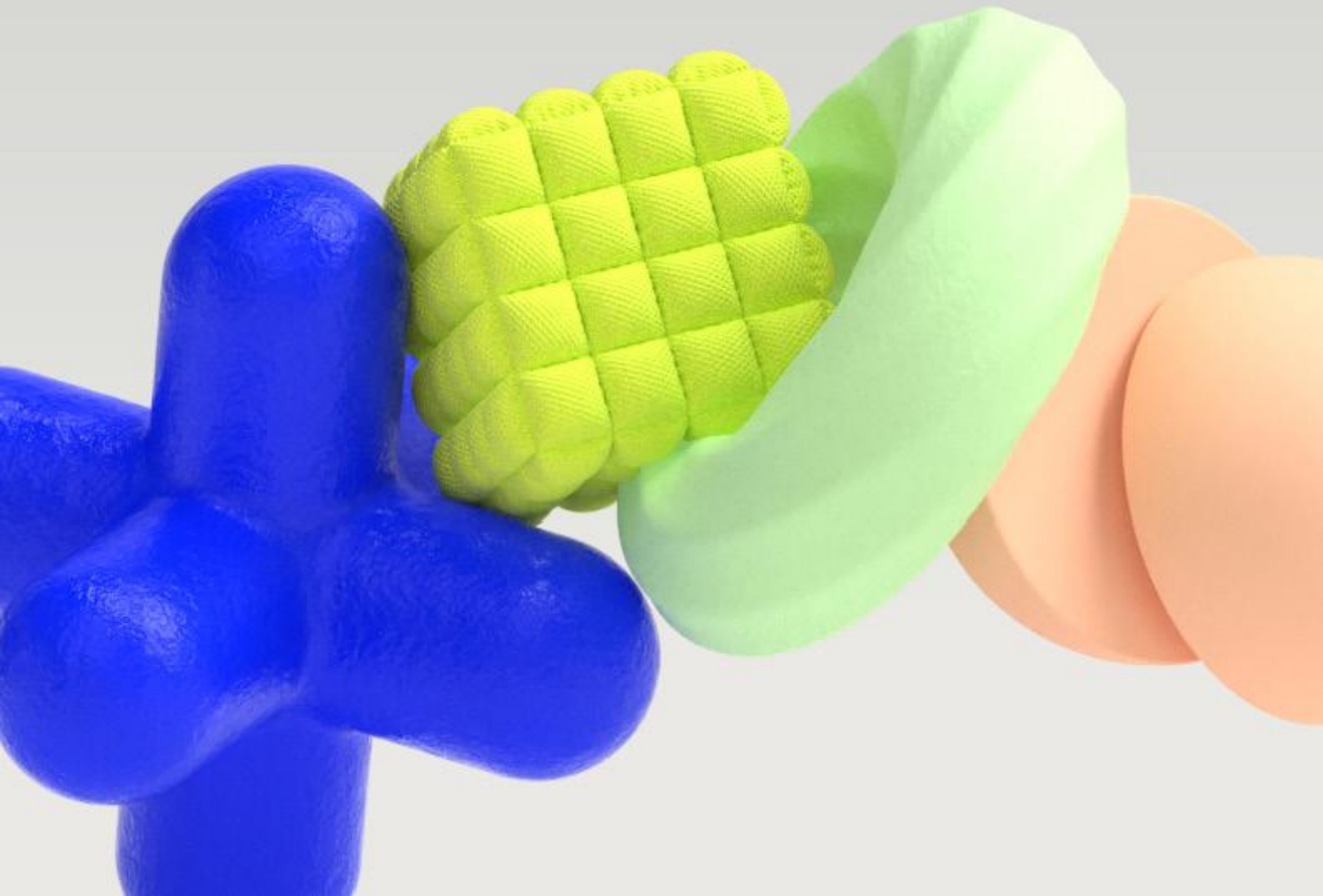
EY Entrepreneur
Of The Year®

30
YEARS
CANADA

Meet the entrepreneurs redesigning possibility.

Be inspired by these brave
and bold architects of change.

ey.com/eoy



SOARING SECURELY IN A BOUNDLESS DIGITAL AGE

THE MODERN ERA OF TECHNOLOGY provides us with unparalleled convenience and connectivity, yet the looming threat of data security remains ever-present. And as we generate and share more information online, it's crucial that we prioritize the protection of our digital identities. In this piece, we'll discuss how innovation can be harnessed to build a more secure online environment, with a focus on Air Canada's privacy policies and how we use—and safeguard—your personal information.

The cost of cutting corners

As we generate more data each and every day, the risk of breaches and misuse also grows. Hackers evolve just as quickly as complex security systems do, often exploiting vulnerabilities. Ignoring data security isn't just a minor convenience; it's a gamble with potentially devastating consequences. So, what's at stake?

Distrust, for starters. People are becoming more cautious about sharing their information. A significant breach can destroy that trust, making it harder for new technologies to be accepted. Innovation could also be stifled; concerns about breaches can cause companies to shy away from forward-thinking ideas, hindering overall progress.

Building a fortified digital frontier

How do we navigate this complex landscape? By adopting a multifaceted approach that embraces innovation while heavily prioritizing security. That means investing in robust security measures including encryption, firewalls and intrusion detection systems. It's also crucial to educate your people on safe online

practices like strong password creation and safe browsing habits. By cultivating a security-conscious culture within your organization, you'll strengthen the collective defense against cybercrime.

The Air Canada way

We collect your personal information when you contact us, browse our website, use our concierge services and book/venture on your travels.

What do we use it for? We use your personal information to complete bookings and requests, address customer service matters, analyze it to better understand your preferences and measure the effectiveness of our offers, to name a few instances.

But above all else, we take your data seriously. We use a combination



of measures to keep your information safe and secure. Only authorized personnel can view your personal information, and we use tech safeguards, like firewalls, encryption and other strategies like pseudonymization (replacing personal details with codes) to protect your electronic data.

For members and customers using our Single Sign On browser, we require multi-factor authentication. This adds an extra layer of security beyond a username and password. We also make sure our staff are equipped with the necessary knowledge and skills to keep your personal information safe from being lost, stolen, accessed by unauthorized people, or used or shared without your permission.

We only keep your information as long as it's needed for the purpose it was collected for, or longer if required by law. Once it's no longer required, we destroy, anonymize, or dispose of your personal information.

You can also help keep your information safe by using strong, unique passwords that you don't share with anyone. We also suggest avoiding using a shared email address for your Air Canada account, or any for that matter. This ensures password resets and other sensitive messages reach only you.

Establishing a secure and ethical digital future

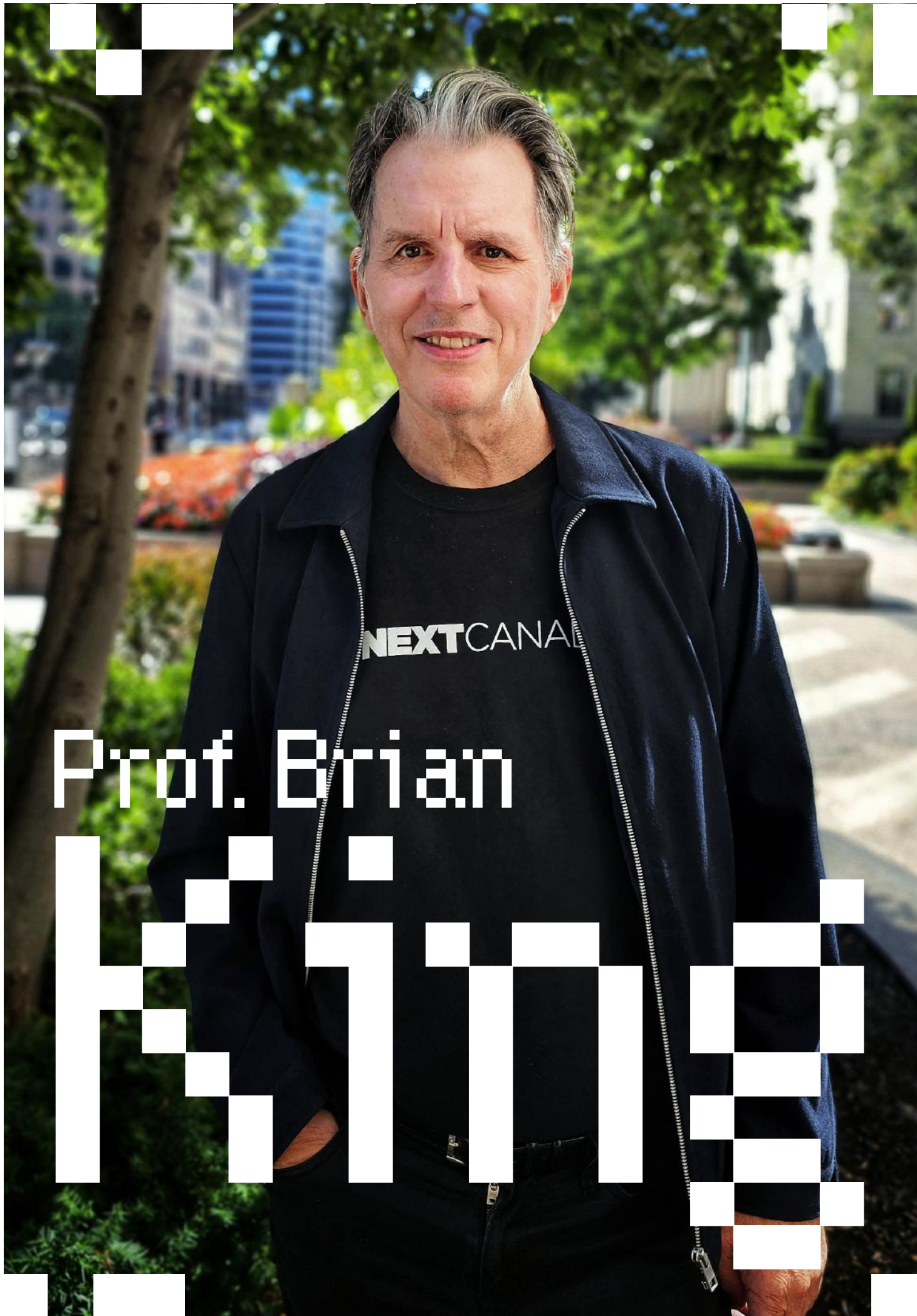
Protecting data is no longer just a technical issue; it's a matter of social responsibility and ethical necessity. By embracing new ideas, educating users and setting ethical standards, we can foster a digital environment where privacy and security are top priorities, not mere add-ons. The result? Being able to fully enjoy the benefits of the online world with confidence, knowing our data and our digital selves are safe.

Learn more at aircanada.com



BIENVENUE!
A CONVERSATION WITH
NEXT AI MONTRÉAL
EXECUTIVE DIRECTOR

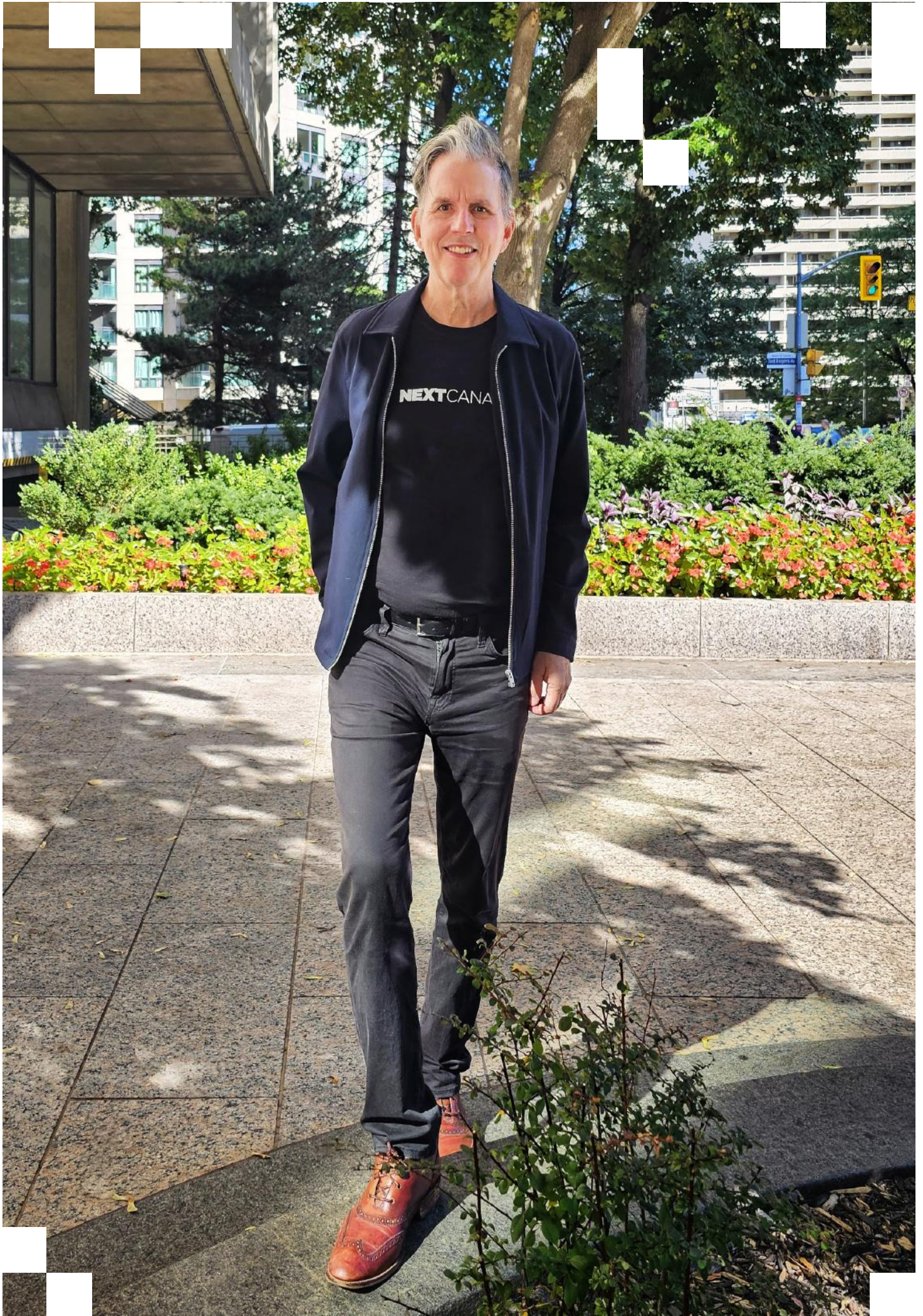




NEXT CANAL

Prof. Brian

2024



NEXT CANADA'S FORMER VENTURE MANAGER, Adam Palter, sat down with Prof. Brian King to talk about what he's looking forward to as he takes the reigns at NEXT AI, Montréal as the new Executive Director and what his vision is for the team and the relationship between NEXT Canada and NEXT AI.



AP: You've recently entered into your new role leading NEXT AI in Montréal. What are some of the most striking things you've observed since accepting the position?

BK: I'm impressed by the fact that we have really developed a strong system for helping our startups. We have a team of Venture Managers that has a mix of senior and junior people, and the juniors are learning from the senior in how best to move startups through the process – and the result is some very exciting startups. My first impression is just that it's a really great team producing some really great results.

What were some aspects of the company culture that you immediately noticed and either wanted to improve or, on the other hand, to celebrate and emphasize?

I've been onboard for roughly six months so far at NEXT AI, so I'm still learning the culture. I'm happy to chip in and help when I can help, but I also don't see a lot that's broken. I was brought in to supplement the organization so I'm simply looking for opportunities to help out. A very concrete example – at our most recent demo day, I felt it would be helpful if I brought out some of the messaging from Ajay Agrawal for the reasoning of why we exist as an organization, so I was happy to credit Ajay but also to show the necessity of NEXT AI to help improve our economy and improve our standard of living in Canada.

Expanding on that last thought, could you elaborate on what makes NEXT AI so incredibly important and invaluable to the Canadian innovation ecosystem?

I think that NEXT AI is here because we in Canada have, through hard work on our scientific side, have developed really strong capabilities in AI that, rather than exporting those capabilities, we should actually build companies here in Canada based on those capabilities. The main reason NEXT AI is so important is to exploit the potential in AI science and build AI companies.

Is there a specific team or company among the many incredible ventures in your recent cohort that you found particularly exciting?

I saw a lot of different ones that I liked. I think the one that really impressed me is Cyberfilm, with their approach to scriptwriting. I was really blown away with how they really very practically applied AI and in some ways democratized film-making by virtue of their scriptwriting tool. The founders are brothers, Russell Palmer from Hamilton and Andrew Palmer from LA. They're very impressive.



Russell Palmer and Andrew Palmer, CyberFilm (Click on the image to learn more)

In terms of the collaboration between the Montréal and Toronto teams of NEXT, what comes to mind and how does that look from your vantage point?

My general approach to life is that we're always stronger together. One of my disappointments in Canada is how difficult we make it to work interprovincially. Sometimes it's easier to sell to Europe than to Ontario if you're from Montréal. So I really think it's exciting to work with NEXT Canada and really bring a message that we can actually work across the country to build startups and then ultimately those startups, because they're backed by the combined resources for Québec and Ontario, and even across the country, can be more successful.

There's a good history of collaboration between NEXT AI, Montréal and NEXT Canada. Even during the recruitment phase we're often collaborating on which startup will fit better in which cohort, so there's a rich history of collaboration and I want to continue that. And maybe we can take that to the next level, for instance, realizing there's a Toronto mentor who's better suited for the Montréal cohort, and vice versa.

Also, I'm really looking forward to working with Kyle (CEO of NEXT Canada) to raise money collaboratively, and to make sure our cohorts work better together and our messaging works better together. Kyle and I see a lot of opportunities where we can make the two organizations stronger through collaboration.

What are some things you're seeing in Montréal that make it a particularly unique landscape for fostering innovation?

Montréal is very well known for its youthful and burgeoning creative culture and in some ways Toronto is becoming the New York of Canada. The strength we have at NEXT AI is being able to combine the characteristics of both cities, positioning us well to grow the Canadian economy.

What do you like to do for fun?

I take a lot of joy in hanging out with my family. And I'm trying to regain my skills as a guitarist. What I play generally tends more towards folk and rock than other genres. Whether it's Led Zeppelin or Neil Young, anything that's challenging.

SECURING INNOVATION: WHY CYBERSECURITY MATTERS FOR ENTREPRENEURS

Authored by
CARLOS CHALICO
EY Canada Partner
Technology Services.



AS DIGITAL THREATS INTENSIFY and data breaches devastate businesses overnight, safeguarding data is now a top priority for entrepreneurs. Recent developments in artificial intelligence (AI), while exhilarating, carry significant risks – especially when the security of your business and its data is at stake.

As the lines between technology and cybersecurity blur, entrepreneurs find themselves at an intersection where the need for innovation meets the importance of protecting digital assets. This is not only an operational challenge, but also a critical business imperative that can determine the future of a venture.

The EY Entrepreneur Of The Year® program has seen firsthand how businesses that prioritize cybersecurity and data protection thrive in this challenging landscape. By fostering a culture of cybersecurity alongside innovation, the program has guided entrepreneurs to ensure their ventures are built on a foundation of trust and resilience. Where AI is increasingly integrated into operations, entrepreneurs must be vigilant and ask the hard questions: Are we fully aware of the implications of AI on our data security? Are our systems designed with privacy and security in mind? Are we using AI responsibly?

THE AI DILEMMA

AI is actively reshaping businesses, offering opportunities for efficiency and cost savings. Tools like ChatGPT and other generative AI technologies have unlocked new possibilities for automating tasks, enhancing stakeholder interactions and driving growth. Yet, the rapid adoption of AI has outpaced the development of ethical and security frameworks, leaving many entrepreneurs to navigate uncharted waters while trying to innovate.

Working with AI comes with privacy, consumer protection, copyright and intellectual property considerations that need to be met. Making sure to review company policies and updating employee training is a first step in securing data and preventing threats. To ensure responsible use, entrepreneurs can work with trusted operators and engage third-party auditors to assess AI systems. With AI tools introducing more features to protect user data and new business subscription tiers offering more control, it's important to choose AI products carefully, considering privacy and data usage practices. Independent AI audits can help identify concerns and recommend risk strategies, strengthening stakeholder trust and safeguarding company reputation as regulatory environments change.

AI4



EMBRACING ZERO TRUST

As cyber threats evolve, traditional security models are no longer sufficient. The zero trust model offers a different approach in cybersecurity, challenging the conventional wisdom of trust within organizations. It is a cybersecurity model based on the principle of “never trust, always verify.” Unlike traditional protection measures that often rely on a fortified perimeter, zero trust assumes that threats can exist both outside and inside the network.

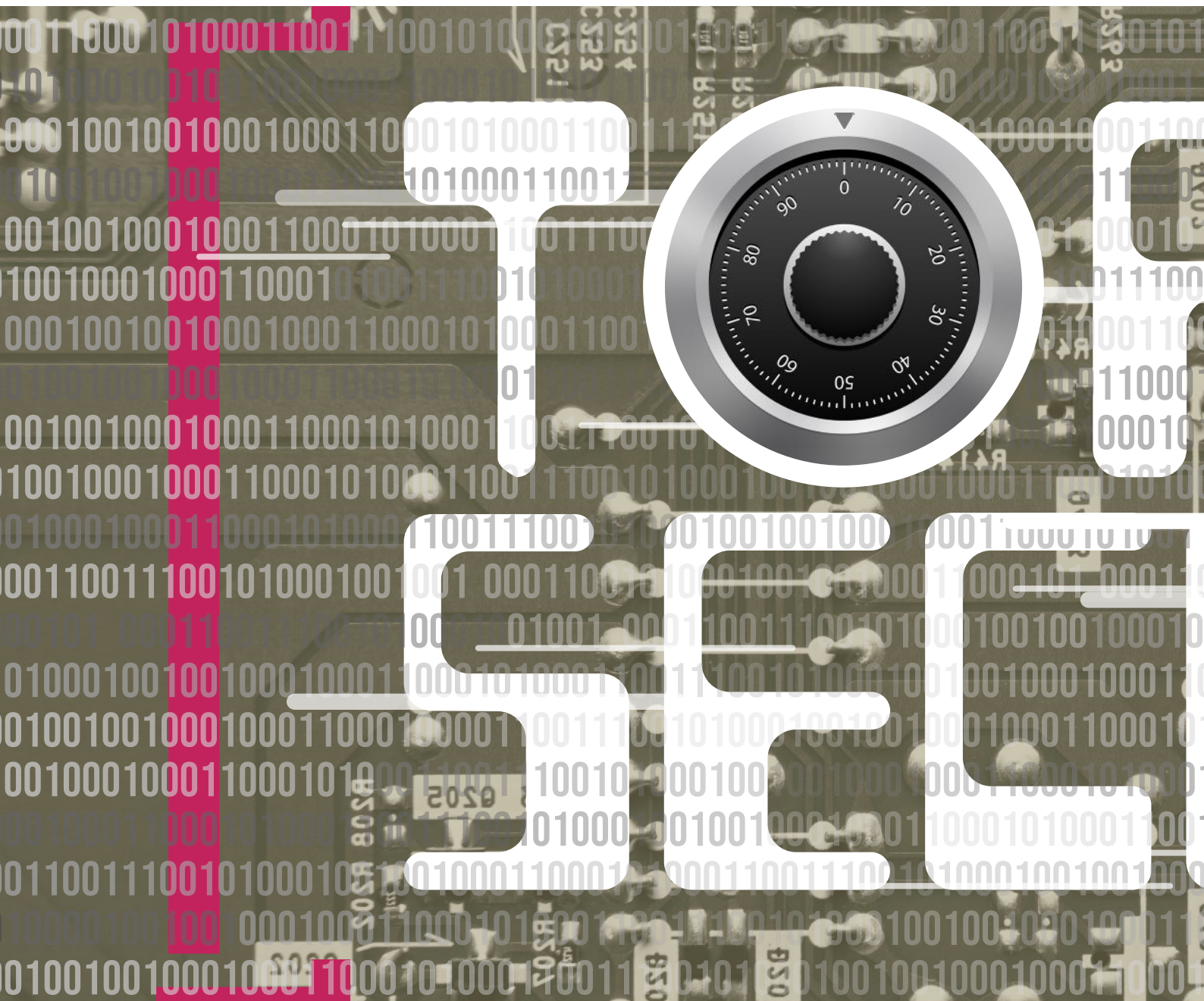
For entrepreneurs, this means implementing strict access controls and not assuming that users within the network are automatically safe. Zero trust requires verification at every stage, creating multiple layers of defense that can significantly reduce the risk of unauthorized access and data breaches.

It’s not a one-size-fits-all approach but a customizable one that varies from one organization to another. For entrepreneurs, adopting zero trust begins with identifying business require-

ments, user types and existing legal and privacy policies.

In the race to innovate, entrepreneurs must not lose sight of the importance of cybersecurity, data protection and responsible AI use. These are not only technical considerations, but fundamental to building a resilient business in today’s digital landscape. For the last three decades, the EY Entrepreneur Of The Year® program has seen the transformative impact of prioritizing cybersecurity and we stand ready to support entrepreneurs as they build the innovative businesses of tomorrow.





Meet some of NEXT Canada's superstar ventures that are ushering in the future



alumni who are hard at work building
of AI, data privacy, and cybersecurity.

TOP SECRET

UNLOCKING AI WITH PRIVACY



PATRICIA THAINE
Private AI
NEXT AI, 2020

NC: What inspired you to start the company, and what was your initial vision for it?

PT: I was inspired to start Private AI because I realized that even the very basics of privacy weren't being done right. So mainly, identifying the information that you have that is personally identifiable and sensitive, and being able to minimize that personal information, which are two key requirements of data protection regulations. Moreover, even in this day and age, technology is not up to par to the expectations of global data protection regulations. Companies who need to be compliant and have unstructured data – for example, text, audio, images, documents, where the data might be very messy in multiple languages and multinational data – can now, using Private AI, better understand what the risks are within that data, minimize, pseudonymized, and anonymize the data, but there are still quite a few innovations we're working on to continue to enable true compliance with much less pain. And in addition to that, it was really obvious that AI was going to be unlocking that unstructured data, which makes up 80-90% of data collected, and companies would have to figure out a way to not just store it in a data lake and lock away the key or trash it. They want to get value out of it. But privacy was going to be one of the main blockers for accessing that data.

Can you explain how data minimization tools work and what types of data they protect?

Yes, data minimization tools will recognize personally identifiable information, that includes direct identifiers like names, exact addresses, social security numbers, credit cards. But they also include quasi-identifiers like religion and approximate location. And those quasi-identifiers, when combined together, can exponentially increase the risk of re-identifying an individual. But some of them are also considered special categories of sensitive data, and under regulations like the GDPR, you're not allowed to process them, except under unique circumstances.

What are the key industries you are currently serving? How do you see that demand changing over the years?

Key industries that we initially served and are still serving are in the conversational AI space. Our beachhead market since 2020 has been conversational AI. We've also served insurance banking, as well as pharma and clinical research. The big change, I'd say, is in the level of awareness companies have with regards to the importance of privacy for unlocking data in order to enable different parts of the organizations to benefit from generative AI or to build AI tools on top of their data.

How do you keep up with the changing landscape and stay relevant in such a dynamic environment?

The interesting part is that the core technology is relevant to basically all kinds of data. We mentioned unstructured, but we

also enable companies to better understand their structured data. We work across fifty three languages. We scale efficiently, both horizontally across use cases and vertically for large amounts of data per team. This is a fundamental technology necessary for compliance and for unlocking data. The way that we stay relevant is really by trying to make it comprehensible for folks who are using new technologies to understand how privacy fits in, how data protection fits in, and how we play a role in that scenario.

What were the key challenges you faced while developing your product?

Some of the key challenges are figuring out what to focus on first or next, if you will. There's, as I mentioned, a dearth in technology that allows you to comply with data protection regulations at a fundamental level. There are lots of steps that need to be taken in order to reach that level. Now that we've got the best system in the world for what we do, those next technologies that we're building on top of it, being able to decide which ones will have the biggest impact at this moment, has been probably the biggest challenge with regards to building.

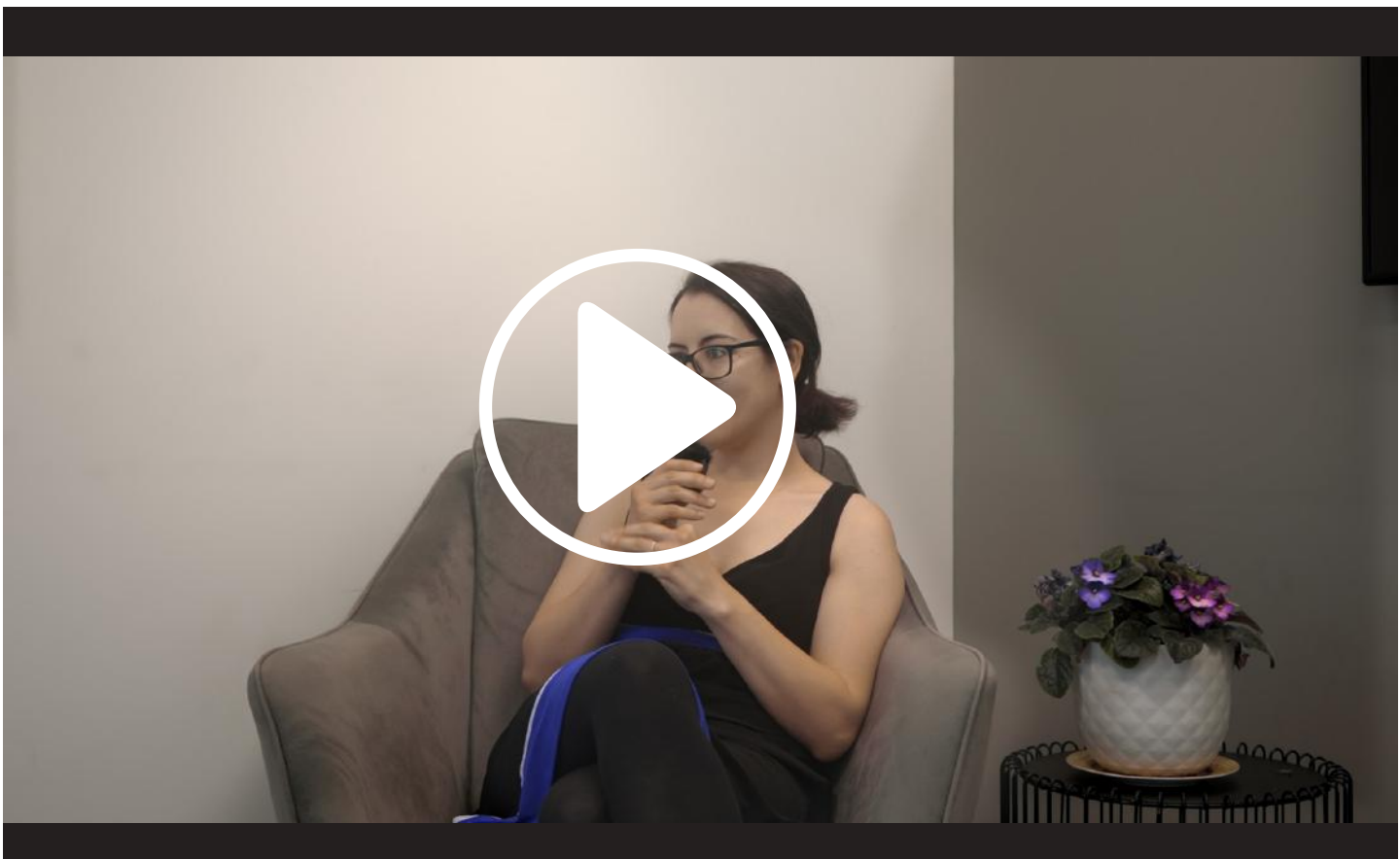
How do you envision the future of data privacy and how do you see PrivateAI playing a role in that?

The way that we've envisioned it since the beginning is being able to understand what data you're collecting and minimizing that information and understanding which individuals that data is associated with from the very point of collection. We started building tools for the Edge, iOS, Android, browsers, but we were too early to market with that. It was really on-prem and private

cloud deployments that took off. But down the line, I see us being in every device that's touching personal information and sensitive data, giving you that federated control over the data that you're collecting so that you're accessing the data. The moment that the data reaches your environment, it's clean. You've done what you need to do with it. It's not just a mess of information in a data lake that you don't know what to do with afterwards.

What are some consequences of minimization data?

Some of the consequences of minimizing data depends on the task. For many tasks, you don't need the personal information in the first place. If you're doing topic modeling, sentiment analysis, figuring out how all the conversations are going, understanding conversation flows, that personal information is just extraneous and toxic in some cases. Like credit card numbers, you don't need them in order to determine if a customer service agent needs training. But the whole point of data minimization is you minimize the personal and sensitive information for the particular task that you're trying to do, so if you end up needing particular information for the task you can keep it while minimizing the risk within the data by removing the information you do not need. The consequence would be if you misunderstand what the task is, you might minimize the wrong data, and then you don't have access to the original information. But the way that Private AI is usually deployed is you'll have your original data, and then you'll have a personally identifiable information firewall that lets the data through to a different part of the organization, like your data science teams. So any data going into the data science team gets stripped out of personal identifiers, and you can change what those identifiers are depending on the task at hand.



[TOP SECRET]

JONATHAN ROY

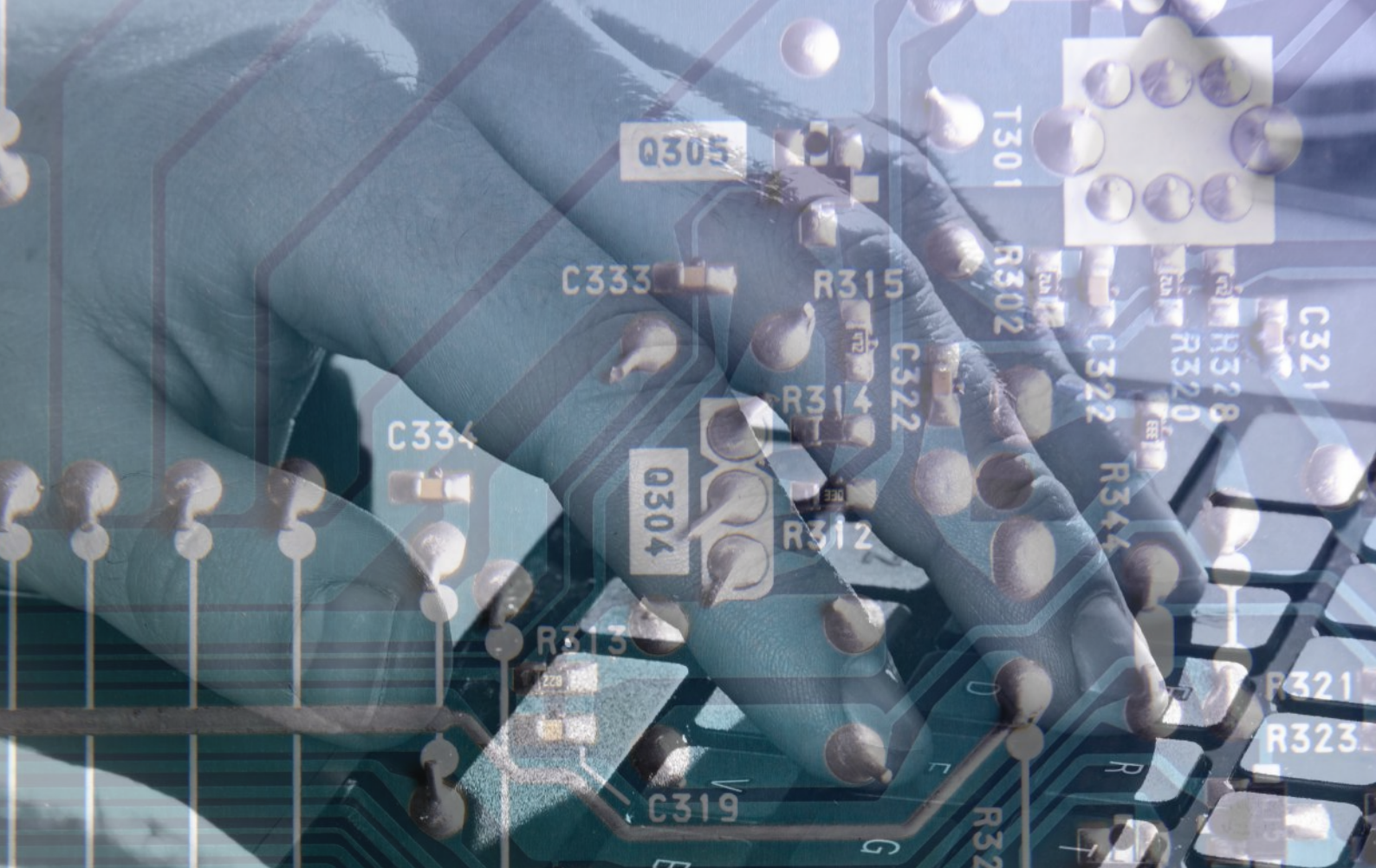
Sentryfy
NEXT AI, 2023



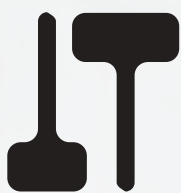
TWO STEPS



AHEAD



Cybersecurity is of the utmost importance in a world where threats to privacy and sensitive data are becoming ever more sophisticated while the devastating consequences of leaks grow in lockstep.



FEELS LIKE HARDLY A WEEK GOES BY without an all-caps news headline loudly notifying the world of another major hack or data breach against some prominent corporation or global entity. Cybersecurity is of the utmost importance in a world where threats to privacy and sensitive data are becoming ever more sophisticated while the devastating consequences of leaks grow in lockstep.

Per Jonathan Roy, CEO and co-founder of cybersecurity startup 'Sentryfy,' "businesses struggle to understand where they stand from a defensive position. They have a hard time keeping up with continuous assessments due to the overwhelming amount of security data to deal with and the speed at which the threat landscape and business operations are changing." Roy's first-hand experience with this issue compelled him to found Sentryfy, which provides cybersecurity teams with an accurate, real-time understanding of their organization's cyber-risks and defensive posture.

Without Sentryfy, cybersecurity teams grind through countless hours manually collecting and preparing security data before

they are able to ultimately review the materials – again, manually, in other words effectively just 'eyeballing it' – in order to conduct their assessments. Doing so even once is a massive undertaking; the sort of ongoing, periodic reviews required to ensure a company can truly rest assured becomes, then, a monumentally time-consuming, inefficient, and ineffective going-concern.

Sentryfy fully automates the process from start to finish. It captures the current "business operational truths," collects and prepares data, and completes both assessment and reporting, empowering cybersecurity teams and enabling shareholders to sleep soundly, knowing the team is taking every action possible in order to safeguard the company's data.

Roy's focus on staying ahead of the curve has led the team to lean heavily into Enterprise Generative AI. Solutions leveraging this new technology "give more relevant and accurate answers when fed with highly organized linked data from your business." That's why the team is cooking up improvements to their core product that will allow businesses to integrate and leverage even more of their internal data to take control of their security and effortlessly remain two steps ahead of nefarious actors.



TOP SECRET

LEVELLING THE



Policy-makers don't speak tech, and technical experts are generally unaware as to the machinations of public policy, and bridging this divide is where Fairly AI comes in.



FION LEE-MADAN

*Fairly AI
NEXT AI, 2021*

ASK FION LEE MADAN, COO OF FAIRLY AI about her vision for the company and she'll point you to a grainy clip of CEO David Van Bruwaene, in which he references Isaac Asimov, Boston Dynamics, Tesla in a matter-of-fact description of the need for compliance in the context of AI and robotics. He's in his office wearing a casual t-shirt, with no frills, no pretenses, just a mission to ensure the coming technology is met with the appropriate guard-rails to prevent it from going awry as it sweeps through our cultural and every-day institutions.

Per Lee-Madan, "we believe AI is changing the world for the better. However, it is also bringing in a new set of challenges which requires a new set of solutions." The solutions she points to relate to the automation of governance, risk and control mechanisms that can effectively guarantee novel AI

applications are safe, secure and compliant.

The company has created a software solution that enables technical and policy experts to collaborate. Having realized the enormous chasm developing between these crucial parts of the developing puzzle, they created a tool to serve effectively as a translator, a go-between, for both sides. In short: policy-makers don't speak tech, and technical experts are generally unaware as to the machinations of public policy, and bridging this divide is where Fairly AI comes in. Their open-source 'Global AI Regulation and Policy Tracker' helps teams understand which protocols they must adhere to, when developing products and growing their company, based on jurisdiction and sector.

At the forefront of this developing niche, the team runs thought-leadership workshops to collate insights about the field. A selected group of passionate experts gather in a confidential

PLAYING FIELD

setting to describe the “issues that are causing them to lose sleep at night,” and the team immediately launches into action building their feedback into features to deploy in their product.

Everything revolves around the “rules,” as Lee-Madam describes the set of compliance standards, which are digested and translated into policies, before being mapped to “control bundles” and then specific controls – which bound the behaviours that clients’ AI products operate according to. These controls can be quantitative or qualitative, and organizations can choose the thresholds they implement based on their risk appetite and organizational constraints.

A company rolling out an AI-based mortgage loan approval tool has to find a way to minimize accidental bias against certain characteristics being built into its model – but these characteristics are wildly different from those that an anti-

money laundering model is liable to be prejudiced against. That’s why the team starts with the inherent purpose of the model they’re working with – borrowing from the Federal Reserve Board’s ‘Model Risk Management Framework SR11-7,’ deploying the ‘fit for purpose’ guidelines in the context of AI even before the National Institute of Standards and Technology followed suit.

Technologies evolve in real time, without supervision – there’s no telling whether their influence will ultimately be beneficial, let alone equitable. Whether for a large bank ensuring inclusive service to diverse clients, for preventing unfair rejection for the opportunity to purchase a home, or even for a glucose-monitoring device for diabetics with different ethnicities and genetic makeups, Fairly AI’s is working constantly to build equality and fairness into the very fabric of this unfolding industry.

TOP SECRET

THE CLINICIAN'S SCRIBE

MAHSHID YASSAEI

Tali AI
NEXT AI, 2021



IN AN ERA where data is considered more valuable than gold and diamonds, the co-founder and CEO of Tali AI, Mahshid Yassaei, is quick to point out that collecting data does not come without its costs. Around twenty years ago, with the implementation of Electronic Medical Record (EMR) software at hospitals, clinicians' hourly burdens skyrocketed due to the new requirement for their patient notes to make their way into the electronic systems. Overnight, some of the most highly-skilled, in-demand specialists on earth found an unreasonable amount of their productive hours consumed copying handwritten notes into a computerized document one letter at a time.

Yassaei and Co-founder Hesam Dadafarin worked with hospitals and government agencies when they first came upon this

monumental problem, and already by 2019 they were hard at work pursuing a solution. In the early days after the EMR transition, some of the larger hospitals were hiring scribes to effectively follow physicians around and document their conversations with patients on their behalf; clearly this would be untenable for smaller-budget facilities, not to mention being simply a waste of resources for any hospital anywhere.

Mahshid and Hesam decided to lean into AI, long before chat-GPT had become a household name across the globe. Initially hospitals were deeply skeptical of 'yet another' AI solution, given the frustrations they had experienced with prior so-called fixes to the data entry problem. When an early version of GPT (2.5) was released a few years ago, it shook things up in healthcare and started to enable Tali AI to begin making real headway. EMR firms, once unsure about deploying AI whatsoever, suddenly



At every juncture, they took the ‘long road,’ when faced with the opportunity to take short-cuts designing and building the product – instead pursuing and achieving stringent approvals certifications such as ‘SOC-2 type 2’ compliance.”

began to open their doors – and quickly recognized Tali AI was nothing like all the other players, given their attention to detail and the accuracy of their solution.

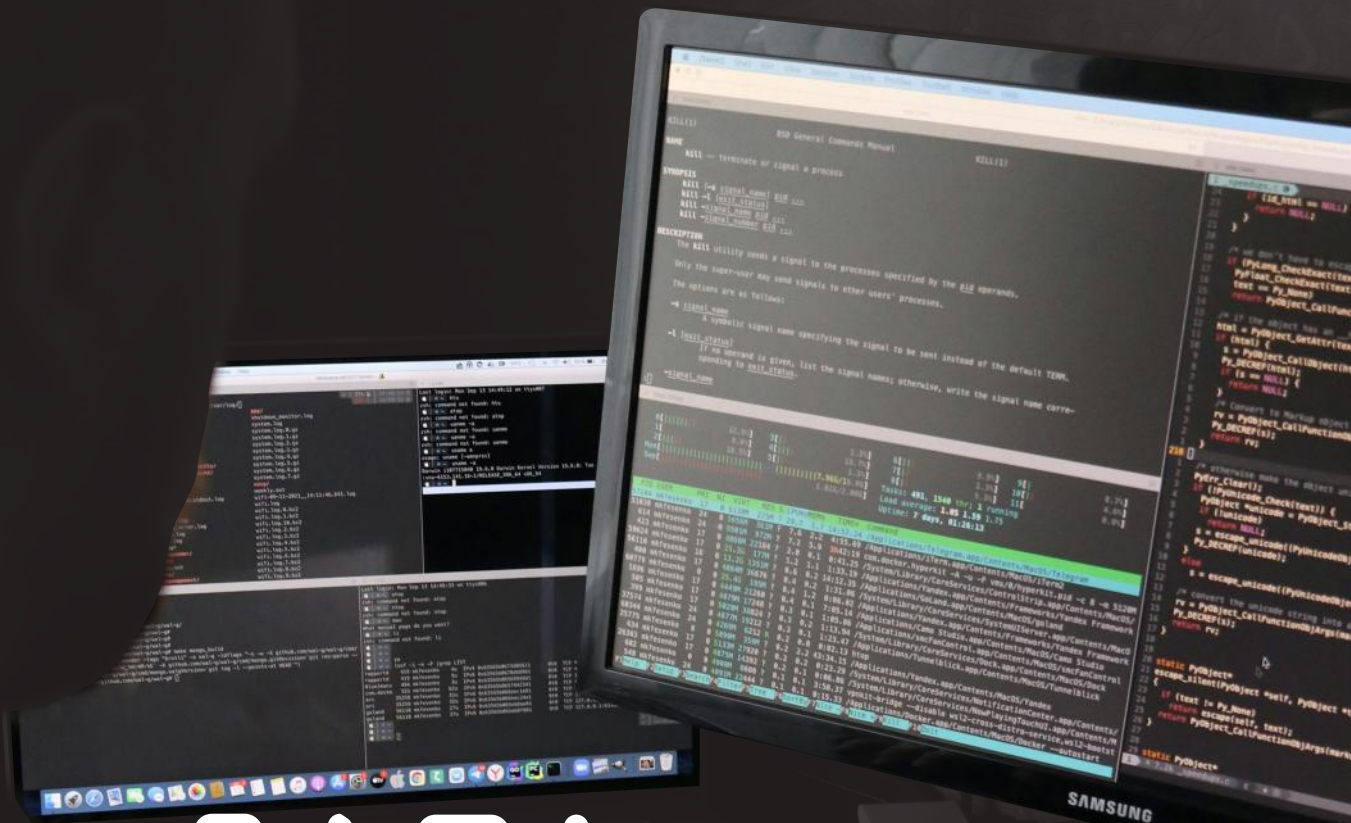
Further, they nailed the issue of how to safeguard the privacy and security of sensitive patient data. At every juncture, they took the ‘long road,’ when faced with the opportunity to take short-cuts in building the product – instead pursuing and achieving stringent approvals certifications such as ‘SOC-2 type 2’ compliance.

In all, the team sleeps soundly at night knowing they’re making a meaningful impact in myriad ways. It’s not just the hours saved inscribing notes that frees up physicians to spend more hours addressing patients; the hours they spend with patients, in turn, are higher-value, higher-leverage because patients now earn their undivided attention while Tali AI takes care of the note-taking ‘ambiently,’ automatically, in the background.

The product requires clinicians to obtain patient consent before recording them, and it can struggle with thick accents spoken by patients for whom English is not their first language. Challenges and opportunities for improvement are still plentiful for the firm, but the response has been overwhelmingly positive. Physicians have mentioned they were considering leaving Family Medicine before using the product, and have changed their minds and decided to stay after implementing Tali AI. Others report increases from thirty to fifty patients per day, a monumental productivity increase, and feeling less burned-out by the end of the day due to the nature of the work.

Based in Canada, the company is already expanding into the US, and has active users in the UK and Australia despite zero advertising there to date. Turns out word of mouth works great when Tali AI takes care of the pen-work.

TOP SECRET



PLAIN, SIMPLE, SECURE.

EZZELDIN TAHOUN

Founder & Chairman, ezSec
Co-Founder & CEO, Cypienta
NEXT AI, 2022



EZZELDIN TAHOUN'S approach to cybersecurity innovation stems from his firsthand experience with the inefficiencies of traditional security systems. Over the years, he realized how restrictive rule-based systems had become. These systems required analysts to continuously create and adjust correlation rules, a process that could take up valuable time and resources. His response to this challenge was to rethink how cybersecurity could be made both more flexible and effective, without relying on rigid structures. He previously founded ezSec, before founding Cypienta, which is a cybersecurity company that develops AI-driven solutions to detect and mitigate cyber threats without relying on traditional, rule-based systems, offering a transparent and adaptive approach to threat detection across diverse data sources.

The central problem Tahoun aimed to solve was the difficulty of finding relevant data points within massive, unstructured data sources, and making connections between them even when months had passed. This required a system capable of continuously learning and adapting to new inputs, and detecting subtle relationships that may otherwise go unnoticed. By eliminating the reliance on pre-defined rules, this adaptive approach addresses the evolving nature of cyber threats more effectively.

Tahoun also places significant emphasis on transparency and interpretability. He believes that AI solutions in cybersecurity must be understandable to users, ensuring that the systems are not "black boxes" but can explain how they arrive at decisions. This level of clarity builds trust, something crucial in an industry where precision and reliability are paramount.

Regarding concerns over the potential for errors, Tahoun stresses the importance of simplicity in AI models. Instead of using more complex AI architectures that are prone to hallucinations, such as large language models (LLMs), he prefers clustering algorithms running on knowledge-encoded graphs. This reduces false positives and ensures a more reliable identification of threats, allowing human users to guide the system's learning.

Tahoun is also deeply committed to ensuring that cybersecurity solutions do not infringe on privacy. His belief is that cybersecurity should not involve collecting or handling sensitive data. Instead, he advocates for systems that operate on the customer's own infrastructure, ensuring that private information stays within

Looking to the future, Tahoun believes that AI will dominate both offensive and defensive cybersecurity strategies.

the user's control, minimizing potential risks.

Looking forward, Tahoun sees a future where machine learning will be integral to both attacking and defending systems. AI will empower both criminals and defenders, making it crucial for security solutions to continually evolve. As cybersecurity continues to grow in complexity, Tahoun's adaptive and transparent approach sets a clear direction for the future.



GAME
CHANGERS
TOP
SECRET



SAFE- GUARDING DIGITAL FUTURES

MinervaAI's platform uses AI-powered automation to speed up AML (anti-money laundering) investigations by up to 300 times, ensuring financial institutions can quickly respond to risks.

JENNIFER ARNOLD

Co-Founder and CEO of MinervaAI
NEXT AI, 2020



JENNIFER ARNOLD was working at one of the largest banks in Canada when she resolved to start MinervaAI, a company aptly named after the Roman goddess of justice and strategic, defensive warfare. Her team had been assembled and mandated to detect and deter crimes related to money laundering and human trafficking: a thankless, repetitive undertaking – and, all too often, a frustratingly futile one.

Catching and thwarting these types of crimes is a profoundly time-sensitive endeavour. The team quickly realized that they had little hope of accomplishing their mission if they couldn't execute investigations practically in real-time, in the precious moments immediately following the crime's occurrence. When it comes to money laundering, in particular: time really is money, and Arnold's team estimated they would need to move roughly 300x faster to even make a dent.

Hence the need for MinervaAI, which empowers Anti-Money Laundering (AML) teams to achieve vastly superior outcomes in a few key ways. First and foremost, MinervaAI shatters the '300x threshold,' meaning their solution works 300x faster than an unassisted human risk screening and investigating threats manually. This breakneck speed advantage not only lets AML teams catch a significantly greater proportion of crimes, but also it shrinks the backlog of alerts and cases piling up on investigators' desks. All told, they help teams open and close more files, more cost-effectively than ever before, and all within the stringent frameworks of constantly changing AML regulations.

With a warranted tinge of pride, Arnold mentions that a senior leadership team-member from Coinbase, one of their large fintech clients, stated at a recent conference that, in her opinion, AML constituted their most successful internal use case application for Artificial Intelligence. MinervaAI wasn't named explicitly; the company speaks for itself.

Arnold deliberately built the company with transparency as a key priority, shrewdly realizing at inception that, while privacy would continue to be at the forefront of regulations, so too would be the use of 'Explainable AI,' which enables oversight bodies to peek behind the curtain and see how the algorithm's gears crank. In terms of the development of AI in the field of AML in the coming years, Arnold indeed expects Explainable AI to play a central role – alleviating the 'black box' and enabling regulators to ensure AML solutions are not just efficacious, but also compliant and above-board.

By researching, reading and constantly collaborating with experts, regulators, clients, and their professional communities, the firm stays ahead of evolving tactics in financial crime, ceaselessly optimizing for usability, detection, and deterrence, and ensuring the modern-day professionals working her old job at the bank never have to wonder if they're doing all they can to fight financial crime.



TOP SECRET

SIM SWAPPING: THE SILENT THREAT AND YOUR SOLUTION



SIM SWAP ATTACK INVOLVES hacking the victim's phone number. It is a type of cybersecurity fraud in which a cybercriminal tricks a mobile service provider into transferring a victim's phone number to a SIM card they control. In the past few years, it has become a significant threat to individuals and businesses. Attackers can get around two-factor authentication by taking over a phone number. This can lead to financial loss and identity theft. They can then access sensitive accounts.

HOW SIM SWAPPING WORKS

Cybercriminals target mobile numbers because they serve as a digital key to our online lives. By getting personal information, they can get mobile carriers to move a phone number to a new SIM card they have. This allows them to intercept SMS-based verification codes and access various accounts. Here is how the

SIM swap works:

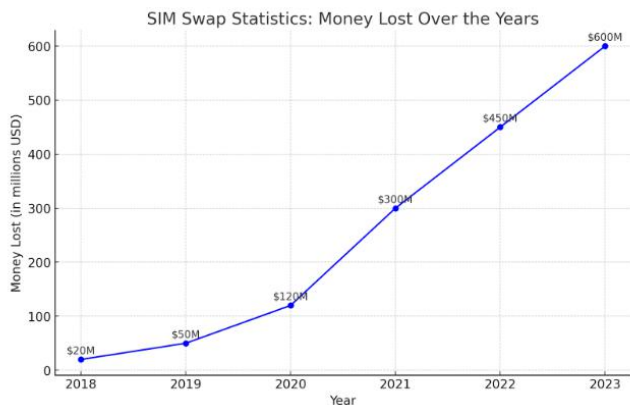
- Information Gathering:** The attacker collects personal information about the victim, often through phishing or data breaches.
- Impersonation:** The attacker contacts the victim's mobile service

provider, pretending to be the victim. They claim to have lost their phone or SIM card and request a SIM swap.

SIM Swap: The attacker tricks the service provider into giving them a new SIM card for the victim's phone number.

Account Takeover: Once the attacker takes control of the victim's phone number, he can access various online accounts such as banking, email, and social media that use SMS-based two-factor authentication.

WHY IS IT DANGEROUS?



The frequency of SIM swap attacks is only getting higher. In 2023 alone, the FBI investigated around 1,075 SIM-swapping attacks, which resulted in nearly \$50 million in losses. A SIM swap attack can cause:

Financial Loss: Attackers can transfer money, take loans, or make purchases using the victim's accounts.

Identity Theft: With access to personal information and accounts, attackers can steal identities.

Disruption: Victims lose access to their phone, email, and other important services.

HOW TO DETECT A SIM SWAP

Unfortunately, early detection of a SIM swap is challenging. However, detecting a SIM swap early can mitigate its effects. Here are some key indicators:

IMMEDIATE SIGNS:

Inability to make or receive calls: This is a classic symptom of a SIM swap. Your phone will show no service or be constantly searching for a network.

Text messages not delivering: If you're not receiving text messages, especially your OTPs, it could be a sign of a SIM swap.

Unusual account activity: Check your online accounts for suspicious logins or changes.

SUBSEQUENT SIGNS:

Unauthorized transactions: Monitor your bank and credit card statements for unfamiliar charges.

Account lockouts: If you suddenly get locked out of your online accounts, it might be due to a SIM swap.

Social media compromise: Check your social media accounts for unusual posts or messages.

While monitoring phone coverage and enabling carrier notifications can provide some indication, these methods could be more foolproof. Often, victims only realize they've been compromised after significant damage has been done.



HASEEB AWAN

Efani
NEXT Founders, 2015

WHAT IS EFANI

Efani was born out of personal frustration. The founder, Haseeb Awan, was a victim of multiple SIM swap attacks in a year, which showed him the severe impact of this crime. Mobile service providers did not offer sufficient protection. A solution was developed to address security, customer service, and guaranteed SIM swap protection.

HOW EFANI PREVENTS SIM SWAP ATTACKS

Efani has positioned itself as a leader in mobile security by implementing a robust, multi-layered approach to prevent SIM swap attacks. Their strategy revolves around stringent security measures, human verification, and advanced technology.

KEY PREVENTION METHODS:

11-Layer Verification Process: Efani utilizes a complex, proprietary authentication process involving multiple steps and human verification to authorize any changes to an account. This makes it extremely difficult for unauthorized individuals to execute a SIM swap successfully.

Cooling-Off Period: To deter SIM swap attempts, Efani implements a mandatory cooling-off period before making any significant account changes.

Employee Background Checks and Training: The company emphasizes the importance of human factors in security by conducting thorough background checks on employees and providing extensive training to minimize the risk of internal threats.

Advanced Technology: Efani employs cutting-edge technology to protect user data and detect potential threats. This includes encryption, server silos, and continuous monitoring of network activity.

\$5 Million Insurance Coverage: As an additional layer of protection, Efani offers customers a \$5 million insurance policy, providing financial security in the unlikely event of a successful SIM swap attack.

CONCLUSION

SIM swapping remains a significant cybersecurity challenge, but solutions like Efani offer hope for a safer digital future. By understanding the mechanics of SIM swapping and implementing robust prevention measures, individuals and businesses can protect themselves from this insidious threat.

GUARDIANS OF DATA: AARON LE ON HATCH'S SECURITY VISION



AARON LE

*Lead Principal Architect
at Hatch*

IN TODAY'S RAPIDLY EVOLVING DIGITAL LANDSCAPE, security and privacy are at the forefront of every organization's priorities. At Hatch Digital, Aaron Le, Lead Principal Architect, spearheads efforts to ensure data protection and cybersecurity are woven into the fabric of their operations. In this interview, Aaron shares insights on Hatch's approach to safeguarding information, the emerging trends in data security, and practical advice for entrepreneurs looking to build a security-first culture in their organizations. – **NEXT CANADA**

NC: Tell us a bit about yourself and your role at Hatch.

AL: In my role at Hatch Digital, I oversee the end-to-end development and operation of Software as a Service (SaaS) for our Digital Products. This includes everything from architecture, front-end and back-end engineering, to DevSecOps engineering, test automation, and operations.

My responsibilities also extend to the management and improvement of our software and product development processes.

I work closely with our software development scrum teams and product owners to ensure that we're delivering significant product capabilities, application and data modernizations, and innovations.

I also have the privilege of leading cross-site teams of high-performing developers, whom I hire, manage, and mentor throughout the development lifecycle.

Can you provide an overview of Hatch's approach to data privacy and security, especially in the context of its diverse

sectors like mining, energy, and infrastructure?

Hatch Digital takes data privacy and security very seriously across all of its sectors, including mining, energy, and infrastructure. We understand that each of these sectors has unique challenges and requirements, so our approach is to develop a comprehensive strategy to meet these specific needs.

We implement robust data protection measures, including encryption, secure data storage, and regular audits of our systems while adhering to all relevant local, national, and international data protection regulations.

We have adopted the Zero Trust framework. This security model operates on the “never trust, always verify” principle, which helps safeguard our digital environments against potential threats. It involves techniques like multi-factor authentication, identity and access management, network segmentation, security policy enforcement and encryption.

In addition, we emphasize continuous training for our staff to ensure they stay up-to-date on the best practices for data privacy and security. As part of our proactive security strategy, we conduct regular risk assessments and continuously monitor threats. By identifying and keeping an active watch on potential vulnerabilities and risks, we are able to stay ahead of emerging threats and take necessary preventive actions, thereby adding an additional layer of security to our systems.

Overall, our approach to data privacy and security is comprehensive and consistently evolving to keep up with the latest threats and advancements in data protection technology. This is crucial for our clients as it not only safeguards their sensitive information but also fosters a sense of trust and reliability in our services, thereby bolstering our client relationships.

In your opinion, what are the most critical emerging trends in data privacy and security that organizations should be aware of and prepared for?

In my opinion, the top three emerging trends are:

- **Privacy by Design:** Privacy measures must be incorporated into products and services from the very beginning, rather than as an afterthought. All operational data are sensitive and requires diligent protection which governs how we handle all data, from collection through to processing and storage. We implement robust encryption methods to protect the integrity and confidentiality of the data during transmission and while at rest. The principle of least privilege is applied during, meaning each individual only has access to the data they need to perform their specific tasks.
- **AI and Machine Learning:** Organizations must ensure they are used responsibly and ethically due to the rise in the use of AI and machine learning for data analysis. However, these technologies also introduce new privacy and security concerns such as privacy violations occur with unauthorized access to training datasets, model bias is introduced from training datasets, model attacks are aimed to circumvent fail-safes, prompt injection, chain of thought exfiltration and profiling of personal data.
- **Cybersecurity Threats:** Ransomware attacks, phishing schemes, and other forms of cyber threats are becoming more sophisticated, including the use of AI bots. It's crucial to implement robust, proactive cybersecurity measures to protect and maintain the integrity of business operations, reduce the risk of falling victim to cyber threats, and preserve the trust of customers.

How do you see the relationship between digital transformation and data security evolving in the next five years, particularly in the sectors Hatch operates in?

These three areas will become more important:

- **Technological Advancement:** The adoption of advanced technologies like AI will not only transform business operations but also introduce new security challenges. Hatch Digital is already adopting new security strategies to protect these digital assets. By staying ahead of emerging trends, we can ensure that our digital transformation efforts are secure, efficient, and beneficial to our customers.
- **Cybersecurity Skills Gap:** As digital transformation accelerates and technology evolves, so too do the threats, the demand for cybersecurity skills will continue to grow. At Hatch Digital proactively addresses this challenge with continuous training and development. By investing in our people, we aim to equip them with the skills and knowledge they need to effectively tackle both current and future cybersecurity challenges.
- **Privacy Regulations:** As awareness about data privacy among consumers increases, governments worldwide are likely to implement stricter data protection regulations. At Hatch Digital we embed privacy measures into our products and services from the outset. This approach ensures that our digital transformation efforts comply with these regulations, helping us avoid penalties and maintain customer trust.

What advice would you give to entrepreneurs and ventures on building a culture of security within their organizations from the ground up?

Below are some of my recommendations for entrepreneurs and ventures:

- **Commitment:** Security must start at the top. Leaders should demonstrate their commitment to security by incorporating it into the company's vision and strategy.
- **Education:** Regular training and education on security practices and potential threats should be a top priority. Everyone in the organization must be aware of their role in maintaining security. No one is exempt.
- **Security Practices:** Incorporate security practices into daily work routines and keep them up to date. This could involve regular password updates, multi-factor authentication, and frequent security checks. Additionally, develop clear and comprehensive security policies covering everything from data protection and access controls to incident response plans.
- **Open Communication:** Encourage employees to speak up about any potential security risks they identify. An open dialogue about security can help prevent breaches.
- **Regular Audits:** Regularly review and update security measures to address new threats. This includes conducting regular audits of your systems and updating them as necessary.

Building a culture of security is an ongoing process, and we apply this on a daily basis within Hatch Digital. I can say with confidence that by starting with these steps, entrepreneurs can establish a solid foundation for their organization's security.



NEXT CANADA'S SECRET SAUCE (OUR WORLD- CLASS FACULTY)

PROF. MARC BUSCH

AS A LONG-TIME COLLABORATOR WITH NEXT CANADA, Prof. Marc Busch shares insights on how he helps early-stage founders navigate complex global issues, discusses emerging challenges in digital privacy, and offers valuable advice for aspiring entrepreneurs.

NC: Congratulations on your 30 years as a professor! Reflecting on your journey, could you share some of the highlights of your career and aspects you're most proud of?

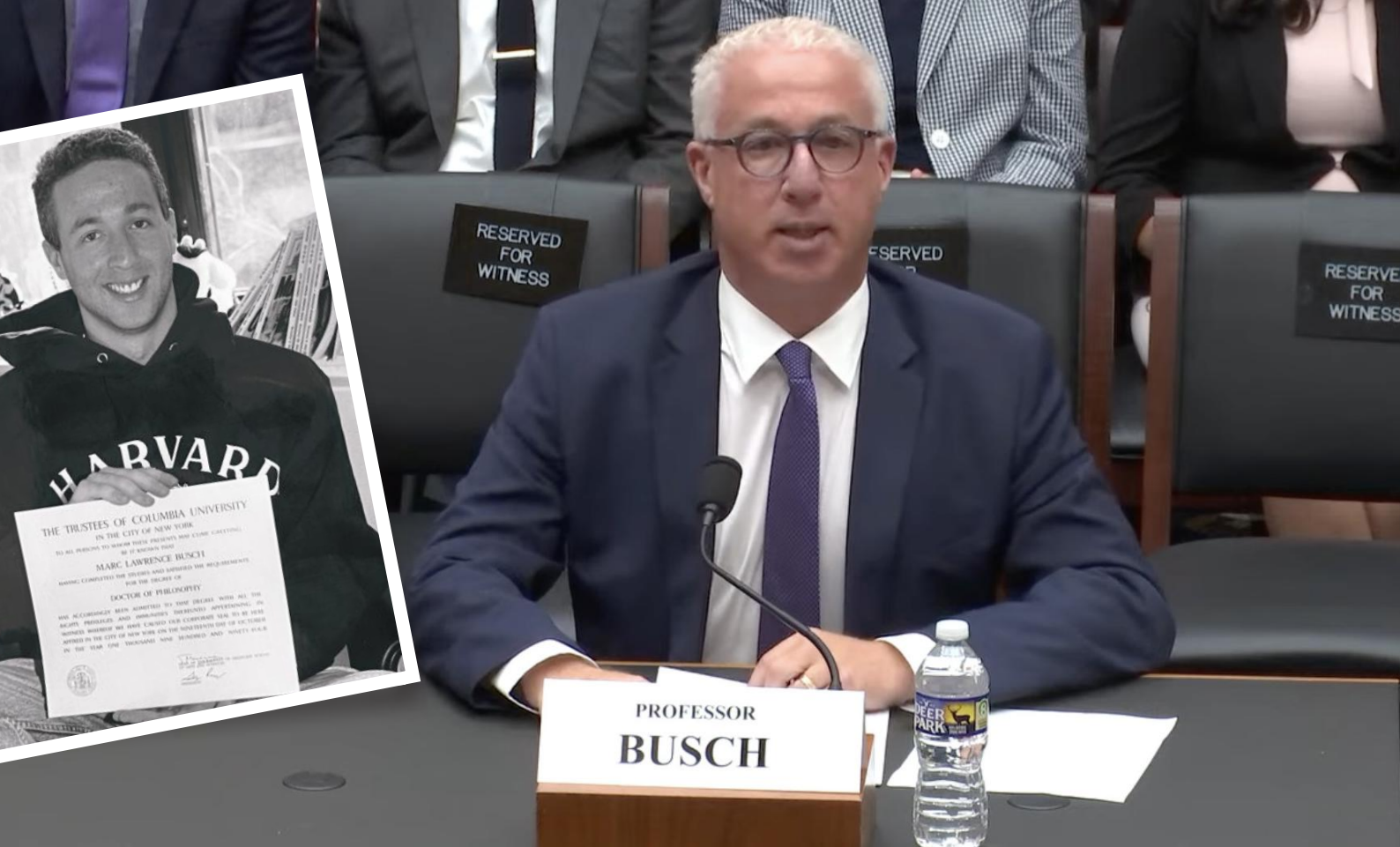
MB: Thanks, it's been a whirlwind. After all these years, it's the "thank you" cards from students that I'm most proud of. It's a thrill to think that I've made a difference in their lives. In terms of research, I've been proud to see my work inform real-world policy, and to be called on to speak before international institutions and testify before Congress. All things I could never have imagined growing up.

You've been involved with NEXT Canada for almost 15 years. How do you adapt complex topics like international trade policy and law to resonate with early-stage founders?

The challenge isn't keeping up with current events. It's showing early-stage founders how to think about the global economy in a different way so that they can better prepare for what's to come. Most NEXT Canada participants have never looked at international affairs through political economy lenses. Many find it difficult because they're thinking social welfare, and I'm asking them to think politics on the offense and defense.

Given your experience advising governments and institutions, what emerging challenges do you foresee for countries when it comes to safeguarding digital privacy and protecting against cyber threats?

The main challenge is that legislation is lagging technology, and this creates a great deal of uncertainty for entrepreneurs. NEXT



“Taking Marc Busch’s class was an eye opening experience. I had never been exposed to such content. He had an amazing ability to break down complex concepts and topics about international trade policies, and relate them to real world business challenges. This was so crucial to learn about because I realized all the important variables that take place to launch our product Toothpod internationally. I learned to scale my startup globally while staying compliant with trade laws and data security regulations. Marc’s mentorship has been crucial to my growth as a founder!”

VISHAR YAGHOUBIAN

CEO, Toothpod
 Hepburn Valedictorian,
 NEXT 36, 2024



Canada participants wow me with their ideas, but I’m always worried that the idea could be undermined by one stroke of the legislative pen. The response to AI is a case in point. The EU’s “AI Act” is mostly about minimizing the risks of a technology it can’t even define.

As someone who has consulted with leading organizations on global trade and policy, what do you see as the next frontier in digital privacy and security that will impact international trade laws?

I’m betting that AI will help reduce the cost of protectionism substantially, especially with respect to creative non-tariff barriers that work by requiring traceability. The problem is that those who want protectionism don’t want a technological fix. They’ll fight back, and they’ll do it by casting doubt on AI, for example. NEXT Canada can play a role in helping Ottawa to advocate for the WTO Joint Statement Initiative on E-Commerce.

How should governments and international organizations work together to create harmonized standards that ensure both innovation and protection in global digital markets?

Global institutions like the WTO and the OECD are already convening efforts to coordinate a path forward on digital trade. The International Organization for Standardization (ISO) is another key forum. But for these bodies to get things right, they need to hear directly from entrepreneurs at the cutting edge of what is possible, not just what is.

Finally, reflecting on your 30-year journey, what advice would you give to entrepreneurs starting on their founder journey?

Be flexible. When you hit a wall, it’s one step back, two steps to the side, and do it again.

PROTECT YOUR STARTUP IN 5 EASY STEPS

NIR MOFET

*Business Information Security Officer,
Business Development
Bank of Canada (BDC)*



AS A BUSINESS INFORMATION SECURITY OFFICER AT BDC, my role involves providing tailored security support and ensuring that cybersecurity measures are integrated into business processes. It used to be that we only saw large companies getting attacked, but now smaller companies are targeted for various reasons. Small businesses are increasingly asking for cybersecurity advice, in addition to business advice. As Canada's bank for entrepreneurs, we can help start-ups build the foundation they need to succeed.

For startups that are just beginning their journey and lack a risk management programme, some of these steps may seem difficult to implement. It's important to first establish fundamental security basics, before diving into more advanced measures. Once you've established your baseline level of security, here are more advanced actions to implement:

STEP 1: Set your goals and objectives

Goal number one for a startup is protecting your assets. Start with a security assessment to understand the current security posture and identify existing vulnerabilities. This will allow you to protect critical information like intellectual property, customer data, and financial information.

You can get started with [this guide for entrepreneurs on addressing cybersecurity in your business](#) and our new [Data to AI program](#).

STEP 2: Classify your top assets

Understanding your assets is the first step in protecting them. Begin by creating a comprehensive inventory of all digital and physical assets. Typically, key assets include customer data housed in your CRM (Customer Relationship Management) solution, payment information managed through your payment processing systems, intellectual property stored in your document management systems, and critical business data essential for maintaining your competitive advantage. Also, consider the importance of systems like your website, which facilitates sales, and HR systems that manage Personally Identifiable Information (PII). Assess how the loss or compromise of these assets or systems could impact your business and classify them on their importance and sensitivity.



STEP 3: Identify and Assess Risks

If your company is starting from scratch, it's crucial to ensure that basic security controls are in place first. These include securing files and systems by encrypting devices, implementing strong password policies to safeguard accounts, and regularly updating software to patch vulnerabilities. Completing these first steps will make it easier to implement more advanced risk assessment and mitigation action plans effectively.

Smaller organizations can use checklists to ensure that basic security controls are in place, such as multi-factor authentication (MFA) and regular access reviews. This approach allows for a systematic evaluation of critical assets and identify any gaps in security controls. These gaps highlight areas of risk, to address vulnerabilities proactively and prioritize necessary protective measures. For a deeper assessment, a structured method such as a probability-impact matrix, can help. Assign a risk score based on the likelihood and impact, helping prioritize which risks require immediate attention. For startups, typical risks include the potential for cyberattacks (such as phishing, malware, and ransomware), the risk of data breaches through unauthorized access to sensitive information, the danger of insider-related malicious activities, and the risk of credential theft compromising user accounts.

STEP 4: Create and Apply a Risk Reduction Plan

Develop specific action plans for high-priority risks, outlining steps for mitigation, responsible parties, and timelines. Implement security controls and countermeasures to reduce the likelihood and impact of risks. Consider leveraging technology solutions like automated monitoring tools and cloud-based security services, which can offer robust protection without significant upfront costs. Additionally, consider hiring a consultant. Our Advisory Services perform double duty – for both cybersecurity and business advice. This holistic approach can help ensure that your risk reduction strategies align with your overall business objectives and support sustainable growth.

STEP 5: Stay vigilant and strive to improve your defences

Congratulations, you have built a strong cybersecurity foundation! But your work is nowhere near done. Cybersecurity is part of your business, so keep up with evolving threats and continuously improve to stay on top.

Cybersecurity demonstrates your commitment to your security, and that of your investors, partners and customers. By protecting your security, you are protecting theirs – and your brand. What's more important than that for a startup?



CONVERSATIONS
WITH LEADERSHIP
VOLUNTEERS



DHARMESH GANDHI

JASKARAN CHAUHAN, Editor of *GRIT*, sat down with **Dharmesh Gandhi**, Partner, SR&ED, Incentives and Capital Investments, EY Canada and Executive-in-Residence at NEXT Canada, to discuss the pressing challenges in today's tech landscape. Dharmesh shares his expert insights on guiding startups, navigating AI ethics, and shaping the future of cybersecurity. Let's dive into his visionary perspectives.

JC: At NEXT Canada, you mentor many startups. What advice do you give to early-stage companies?

DG: Perfection is the enemy of good. By that I mean, it is important to get a product to market and start getting feedback, even if the product is not where you believe it could be. That feedback is invaluable in terms of iterating the product, and ensuring you have a market.

EY has been at the forefront of helping businesses access SR&ED credits to drive R&D. In your view, how can government incentives better support innovation in cybersecurity and data protection?

To better support innovation in cybersecurity and data protection, government incentives could focus on providing targeted grants and tax credits for R&D in these areas, encouraging public-private partnerships for advanced research, and offering subsidies for small and medium-sized enterprises (SMEs) to adopt cutting-edge cybersecurity technologies. Additionally, fostering education and training programs to develop skilled professionals in cybersecurity can further enhance innovation.

With AI playing an increasing role in business operations and security, what are the ethical considerations that entrepreneurs should be mindful of when deploying these technologies, especially in terms of privacy?

As AI usage becomes more prevalent, it is important for companies to mitigate risks. The considerations include bias and privacy. An example of a biased AI system would be one tasked with generating insurance quotes for customers. Due to inherent bias in the system, a scenario could arise where minorities are paying more for insurance. Privacy is also a consideration as AI systems rely on vast amounts of data for training, however if sensitive information is included, there is a risk of data privacy breaches.

You've worked with organizations across various industries. Are there any sectors that you believe are particularly vulnerable to cyber threats, and how should they rethink their approach to digital security?

Cybersecurity threats are now widespread, placing every sector in jeopardy of being targeted by an attack. The industries that handle sensitive personal data, including life sciences, and financial technology sectors, need to reassess their cybersecurity strategies. The compromise of this sensitive data could precipitate subsequent attacks.

As someone who is passionate about fostering the tech ecosystem in Canada, what emerging technologies are you most excited about in terms of their potential to revolutionize data security?

As quantum computing continues to evolve, there are challenges and opportunities. Quantum computers, once established, will be able to break common encryption methods quickly and with ease. This in turn will lead to the development of quantum resilient systems which will increase overall security of data stored across all industries.

How important is it for companies to not only focus on compliance with data protection laws but also adopt a proactive, ethical approach to handling user data, especially as consumers grow more aware of their digital rights?

In today's fast moving technological environment, companies are challenged to keep up with emerging threats. Companies must however focus on the items which can cause reputational risk, and as such must ensure data protection laws are being followed. Moreover, they must seek to create a culture of internal rigor which encourages employees to identify gaps, such that new best practices can be implemented. As consumers become more tech savvy, and understand the risks of data exposure, they are already starting to make consumer decisions based on the companies which emphasize and deliver on a private user experience.



WHO'S

LISTENING

TO

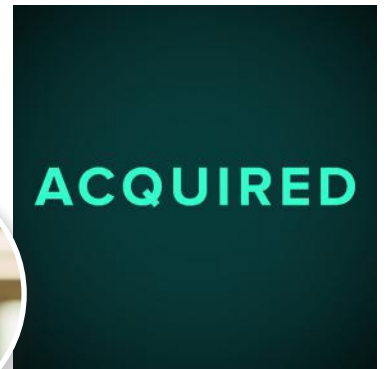
WHAT

Read about what our office co-tenants are listening to in their day-to-day. Be it podcasts about entrepreneurship, world politics or just life, we have it covered!



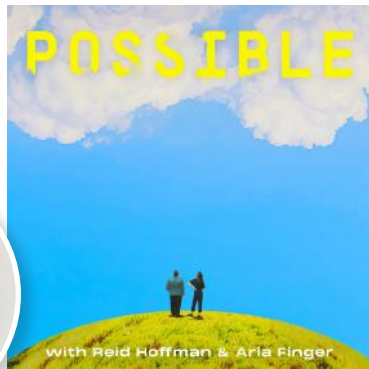
MARK COOMBS *CEO & Co-Founder Sleepout*

I'd recommend **Never Enough** podcast by Andrew Wilkinson. I've been following Andrew's story since I found out that his first company MetaLab made the design for slack. His obsession with Warren Buffett and Charlie Munger mirror my own and he has interesting takes you don't normally see in the startup world!



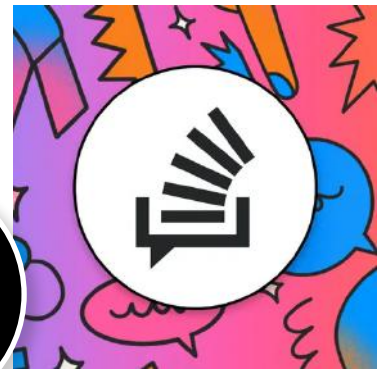
PETER CARRESCIA *Co-Founder goConfirm*

I've been listening to **Acquired** since their first season in 2016. They talk about the founding stories of great companies (Instagram, LinkedIn, Microsoft etc.), focusing on the founders and products that helped them grow to acquisition or IPO and beyond. They put in an incredible amount of research and time into every story. Worth the listen.



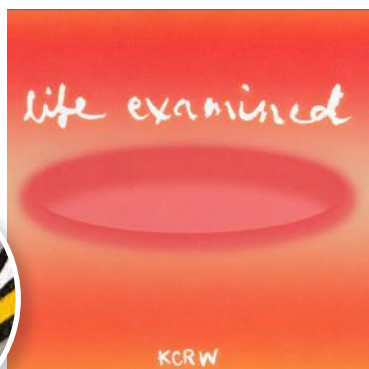
SCOTT MacGREGOR *Director, Digital Strategy & Design for Products at Hatch*

"What if, in the future, everything breaks humanity's way?" The minute I read the show's description, I was hooked. **Possible** explores the positive impact technology can have on our future if we use it effectively. I'm a big believer in ambitious optimism and am always on the hunt for shows that ignite that mindset in me. Leave the doom-casts behind and explore what the world could be like when we embrace our brightest future.



ILKIN NAMAZOV *Software Engineer at goConfirm*

The podcast I'm listening to is **The Stack Overflow Podcast**. As a software engineer, I want to stay up to date with the latest news in technology and anything related to improving software development. This podcast provides updates on current trends in software building, such as new updates to programming languages. Additionally, it shares interesting stories about startups and how they are built, which adds valuable insights.



ZAMAN FOROOTAN *Global Practice Leader for AI and Machine Learning at Hatch*

I tune to **Life Examined** every week. The podcast host, Jonathan Bastian, spends the hour with his guests exploring science, philosophy, faith, and finding meaning in the modern world.



ADITHYA SUDARSAN *Software Engineer at goConfirm*

I really like listening to the **Build with Leila Hormozi** podcast. Learnt a lot from it, including building successful businesses and scaling them.

10

FOUNDERS TO WATCH



FLETCHER McLAUGHLIN

*Program Coordinator,
NEXT Canada*

Every year we have exceptional ventures go through our program and I have the pleasure of helping them grow through the year.

This year the following ten ventures stood out to me. I am excited to witness their progress as they continue in their entrepreneurial journey.



VISHAR YAGHOUBIAN

NEXT 36

TOOTHPOD is aiming to improve global oral hygiene through designing Toothpods, smart dental gum that cleans the mouth when there is no access to a toothbrush or toothpaste through anti-inflammatory, anti-microbial, and remineralizing agents.



KATE WALLACE

NEXT Founders

AVENUE STORIES is an a16z backed company building a platform for interactive stories. Readers can build their own story using AI or read an existing story from the library. Kids are obsessed with interactivity – they name characters and make decisions that change the outcome of the stories.



RAE JEONG & KELVIN CHAN

NEXT AI

MANEVA is at the forefront of transforming the manufacturing industry by developing advanced AI-powered digital workers. These AI agents are designed to understand and optimize factory processes with the same depth and insight as human operators, significantly enhancing productivity, efficiency, and quality control.



ARLYNE JAMES

NEXT 36

MY DORM STORE is a curated dorm shopping solution made by students, for students. Students can order everything to make their dorm into their home. We work with schools to design affordable packages and deliver everything before students arrive.



SAUMIK BISWAS & MICHAEL LAVDAS

NEXT AI

TENOMIX is a medical-technology startup that is revolutionizing the way cancer tissues are processed in pathology laboratories using robotics, ultrasound imaging and AI. With our patent-pending platform technology, we are currently automating a tedious, unreliable, and expensive process in the colon cancer staging pathway: the manual lymph node search process.



ANTHONY AZRAK & JAI MANSUKHANI

NEXT 36

OPENSESAME is making AI feel like magic. They help businesses detect when their AI systems are messing up by intercepting their AI calls, extracting valuable data from them and conducting a complete analysis to uncover where errors are occurring and what can be mitigated. They also allow companies to be more transparent by sharing hallucination data with their end user.



MICHAEL YU

NEXT 36

QUANTOFLOW is an all-in-one intelligent platform for client screening, transaction monitoring, and reporting for fintechs. They use AI to reduce the industry standard false positive rate by an order of magnitude, building the Palantir of Anti Money Laundering.



WENDY XIANG & MITCHELL CAMPBELL

NEXT 36

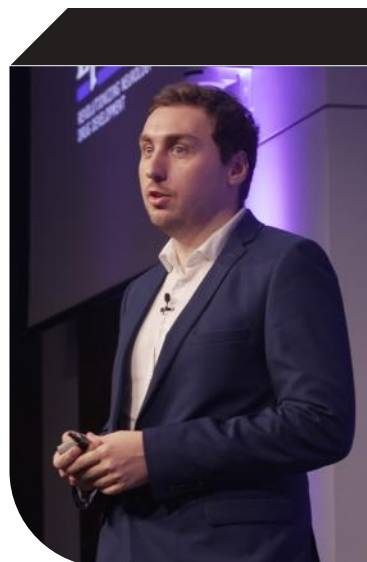
ANALYST3 is a deal sourcing and diligence platform for strategic acquirers that helps close transactions in weeks, instead of months.



QUINN DAI & GIN JIANG

NEXT AI

AFAIK.IO uses AI to build the future university for everyone to learn everything, following their personalized learning path, at a fraction of college tuition.



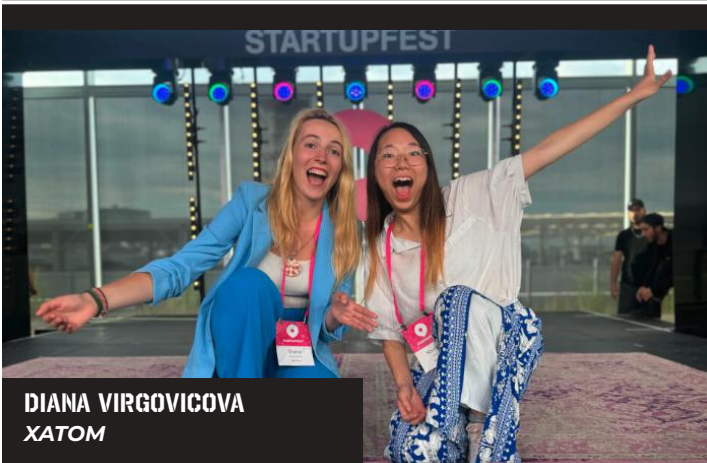
MARK AQUILINO

NEXT Founders

EPILOID BIOTECHNOLOGY is focused on providing improved preclinical assessment of new therapeutics before those drugs reach a patient. Epiloid achieves this through machine learning analysis of custom lab-grown 3D human brain tissues that can replicate human disease like Parkinson's disease and epilepsy.

COMMUNITY NEWS

NEXT CANADA COMMUNITY MAKING HEADLINES



DIANA VIRGOVICOVA
XATOM

Xatom's Diana Virgovicova wins three awards at Startupfest totalling \$250,000



MICHAEL STYCH
CONTEND LEGAL

"We use AI to make justice more accessible to ordinary people"
- In Conversation with Michael Stych



MAAYAN ZIV
ACCESSNOW

Maayan Ziv receives Meritorious Service Decorations from the Governor General



PARNIAN MAJD
FIBRA

Fibra raises \$1.25M in pre-seed round to advance fertility tracking underwear



MEGAN TAKEDA-TULLY
SUPPLI


Suppli secures seed financing

JAYIESH SINGH
ABLE INNOVATIONS

Six Healthtech Companies in Toronto to Know




IN RECENT MONTHS, our alumni have garnered attention for their successes in capital raising, team expansion and innovation. Click below to explore their accomplishments.



ABRAHAM HEIFETS
ATOMWISE

Why Atomwise sees a 'generational shift' in drug discovery with AI applied to screening



DAVID LYNCH
KLIR

Modular Water Systems and Klir partner for Water On Demand pilot program


IVAN TSARYNNY
FEROOT

Feroot Security achieves SOC 2 Type II compliance, strengthening digital safety




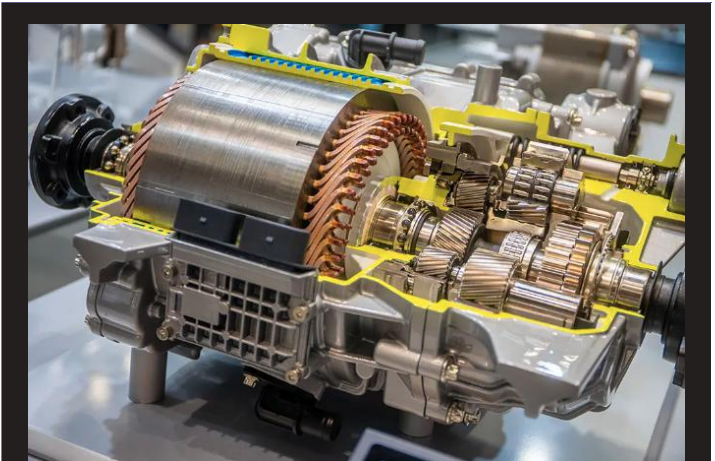
MICHAEL HELANDER
OTI LUMIONICS

OTI Lumionics selects Nord Quantique to test new quantum computing applications for materials science



CHRIS ATKINSON
FLEETOPS

FleetOps announces integration partnership with Turvo, bringing new capacity to the Turvo Transportation Management System

AHMAD GHahreMAN
CYCLIC MATERIALS

Cyclic Materials and SYNETIQ partner to recycle rare earth elements from vehicle motors




JOSH DOMINGUES
FLASHFOOD

Flashfood taps new CFO to complete leadership refresh



KARL MARTIN
NYMI

Nymi biometric wearable integrated with pharmaceutical manufacturing system



ZAK LEFEVRE
CHARGE LAB

Rexel Energy Solutions and ChargeLab partner to install EV chargers for Canadian businesses

GRIT

Elevate

Edition 16 | Winter 2025

This issue celebrates women entrepreneurs and their significant contributions to the Canadian business landscape. We honor their journeys, determination to break glass ceilings, and commitment to positive change.

Explore the insights and inspiration from these remarkable women who are paving the way for future generations.

Click [here](#) to get featured.

Women on the Rise

NEXT CANADA

GRIT is a NEXT Canada publication created 3 times per year.

NEXT Canada's mission is to provide lifetime founder support with the goal of building a more prosperous and competitive Canada.

Charitable registration #: 81519 8403 RR0001