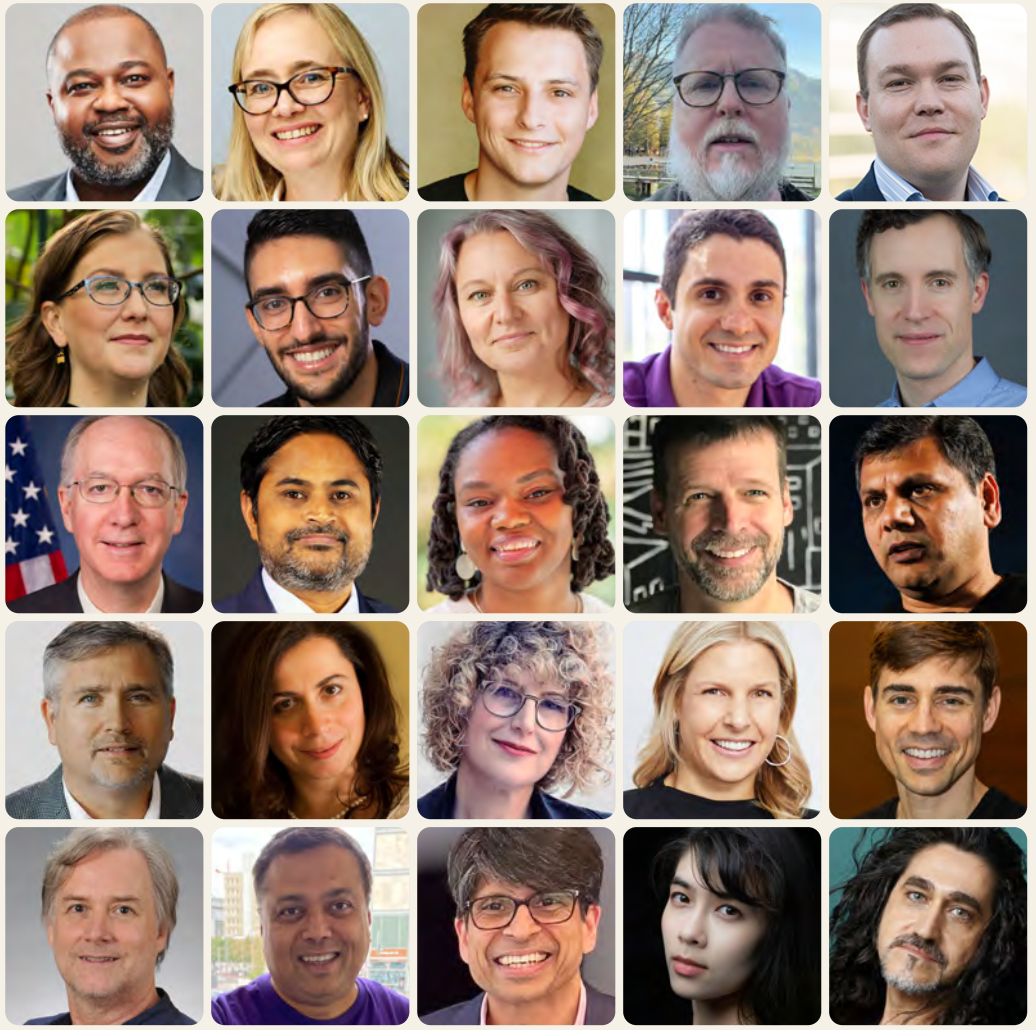
The Identity 25

Okta's annual look at the top movers and shakers in the Identity world



okta

okta Ventures

Contents

The Titans of Identity

Organizations are grappling with new challenges: fluid global workforces operating across multiple time zones, AI-enabled fraudsters, deepfakes, and a plethora of new devices creating an ever-expanding attack surface. The struggle to implement Identity solutions to safeguard access — to equip workers and customers with the digital tools they need, while protecting enterprise assets and customer data from relentless cybercriminals — seems to grow more difficult each year.

Modern digital life is only possible thanks to Identity innovators, who've been working diligently, sometimes for decades, to create reliable technologies, standards, regulations, and practical solutions to secure this expanding new frontier. The Okta Identity 25 was created specifically to honor the incredible contributions of these Identity innovators.

Nearly every digital experience we have, from logging on to a website to paying for an e-commerce transaction to voting, is rooted in Identity management. And behind all these experiences is a group of cutting-edge innovators helping to build simpler, more secure, and scalable Identity-centric technologies. They work in different disciplines and capacities — standards organizations and university departments, government agencies and research facilities, innovative startups and leading global businesses. But together, they're making the world a safer place to live, work, and transact in.

The Identity 25 is an initiative designed to recognize the leading lights in the growing Identity space. With this inaugural report, Okta Ventures seeks to elevate the emerging leaders who are working together to improve Identity, security, and privacy for businesses and their clients, for consumers, and for global citizens.

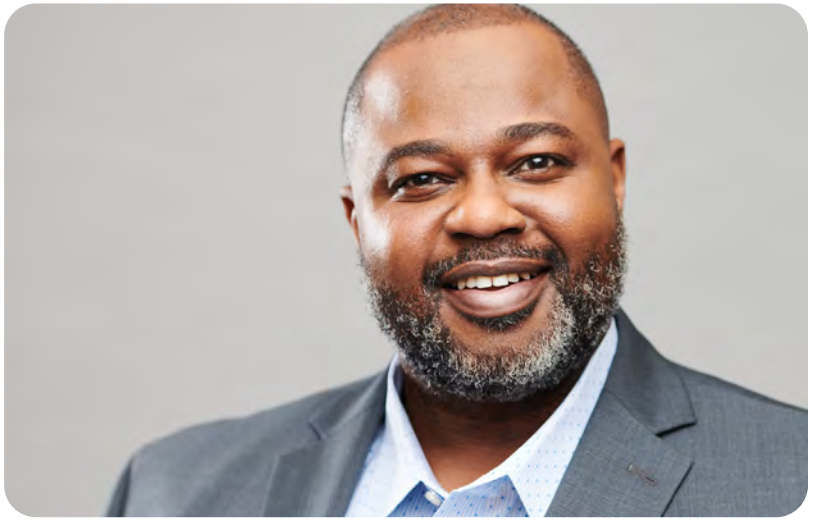
This year's Identity 25 list includes academics and activists, public servants and entrepreneurs, standard-setters and technology pioneers. Some create laws to thwart Identity criminals, while others agitate for individual rights and privacy, or combat fraud and abuse. Some are developing new technologies; some are teaching the principles of strong Identity to the next generation of leaders; and some are setting the standards for a safe, interoperable digital world. (To nominate an entrant for next year's ID25, see the instructions at the end of this report.)

These brilliant innovators are only beginning to develop the systems of tomorrow, and they'll no doubt continue to create and inspire solutions we can't begin to predict. With the Identity 25, Okta honors the magnitude of their achievements and the depth of their commitment as they advance Identity standards, technology, and processes to better the lives of our shared global digital community. Enjoy reading about the community of people who make your digital life more secure, private, and empowered and their predictions for the future of our complex, ever-expanding digital world.

IDENTITY 25 HONOREE

Solomon Adote

Chief Security Officer (CSO) State Of Delaware



> I have faced some formidable threat actors in my career. Some are patient and meticulous enough to take two years to breach an environment."

As Chief Security Officer for the state of Delaware, Solomon Adote understands firsthand just how critical smart Identity management is to digital security — and the challenges involved in deploying and maintaining Identity-backed security systems at scale. His office provides leadership to a state of more than one million people across critical areas like risk assessment, disaster recovery, and continuity of government. It's an ongoing, ever-evolving challenge.

With more than two decades of experience in cybersecurity, including key posts for large enterprises outside the public sector, Adote's up to the task. Before being appointed to his current post in 2018, he led the global IT cybersecurity team for FMC Corporation, a multibillion dollar agricultural sciences company composed of nearly 100 manufacturing and management sites. Prior to that, Adote was the team leader and senior information security engineer for e-commerce giant QVC.

"I have faced some formidable threat actors in my career," Adote says today. "Some are patient and meticulous enough to take two years to breach an environment." Some bad actors he's faced are highly organized criminals; others are affiliated with or sponsored by nation-states with the resources to unleash what he calls "a flood of attack traffic" against targets. The experience has hammered home just how dependent modern security is on ironclad Identity management.

Adote uses the metaphor of a locked house to illustrate the critical nature of Identity today. Standard security policies are the equivalent of strong walls and reinforced steel doors. Those home defenses are great in theory — but they're completely useless if an intruder can steal your house key. Organizations that haven't yet invested in modern Identity management, Adote says, are guarding their critical assets with their least skilled resources, who could unwittingly hand the keys to clever hackers and bring the whole enterprise down.

"The bad guys were the first to realize the value of Identity," Adote notes wistfully. Early cyberdefenses focused on the challenge of hardening network architecture — strengthening the walls. But as that challenge grew ever more difficult, threat actors shifted to the far easier task of stealing the keys from authorized users to gain access.

Adote has made Identity the foundation of Delaware's security strategy, and he sees encouraging developments in the field, including harnessing the power of AI to bolster firewalls and harden intrusion prevention systems. The key, he believes, is collaboration: setting up systems that require users to share information that can help everyone spot intruders, and that security teams can use to detect anomalies and secure their organizations.

"Identity vendors must become industry-leading cybersecurity organizations," Adote says, "setting trends in threat detection and response. They must provide a comprehensive lifecycle for Identity. To effectively safeguard their customers, they must themselves be the most secure organizations in the world."

IDENTITY 25 HONOREE

Marie Austenaa

Head of Digital Identity, Visa

> “Consumers want an Identity solution that protects their privacy and lets them be no more than ‘the same person as last time.’”

As the Head of Digital Identity for Visa in Europe, Marie Austenaa lays out a broad vision for the Visa brand: one that safeguards digital access with strong Identity controls while keeping access simple for consumers. “My ambition is to bridge the gap between payment and Identity and make it as easy and secure to prove who you are as it is to make a payment,” Austenaa says.

Austenaa’s position gives her a unique perspective. “Clearly, the US and Europe have taken different paths with regards to digital Identity,” she notes. “The EU and UK governments have a central role in both issuing digital Identity credentials and creating the trust framework for how they operate. In contrast, while individual American states have started to offer digital driver licenses, in the U.S. the most advanced services for reusable digital identities come from private sector companies such as CLEAR.”

Austenaa believes Visa is uniquely positioned to learn from both and produce an approach that works in highly regulated environments and in more relaxed ones. Interestingly, some of the work the company does for individuals whose identities are more difficult to verify, like refugees and migrants, informs Visa’s efforts in more developed markets, where folks generally have more easily verifiable credentials. “We take learnings from one region into other regions, and from different types of individuals and are able to think differently to protect consumers’ privacy and to create a secure service.”

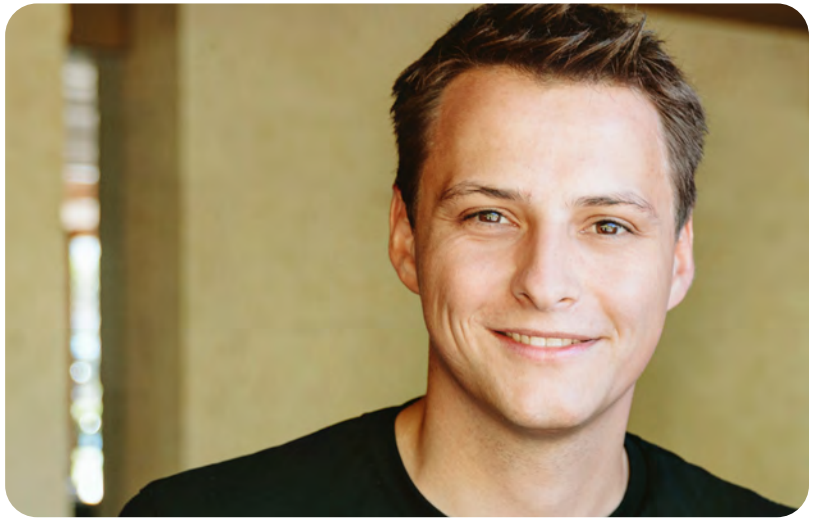
Austenaa also chairs the governing board of Linux’s Open Wallet Foundation, where she’s laying the groundwork for a private-public collaboration to create best-in-class open-source digital wallets. “My ambition is that consumers have a wide choice of wallets,” she says. These wallets are interoperable and secure, preserve privacy, and give consumers multiple options for easily and securely proving their identities and making payments.

Consumers still struggle to understand the importance of Identity security, and are suspicious that their personal information won’t be kept private. Austenaa likes to point out, however, that consumers are eager to adopt digital Identity solutions when the benefits or needs are clear: like for proof of vaccination, or for staying in an Airbnb home. But they balk when they fear they’re being tracked or monitored, which is perhaps understandable. “Providing an alternative where all consumers can protect their privacy, have a real choice in what information is being shared, and be able to remain no more than ‘the same person as last time’ is possible with a truly evolved digital Identity,” Austenaa says.

IDENTITY 25 HONOREE

Alex Blania

CEO and Co-Founder, Tools for Humanity



"As AI advances, distinguishing machine-generated from human-generated content or interactions will become increasingly important."

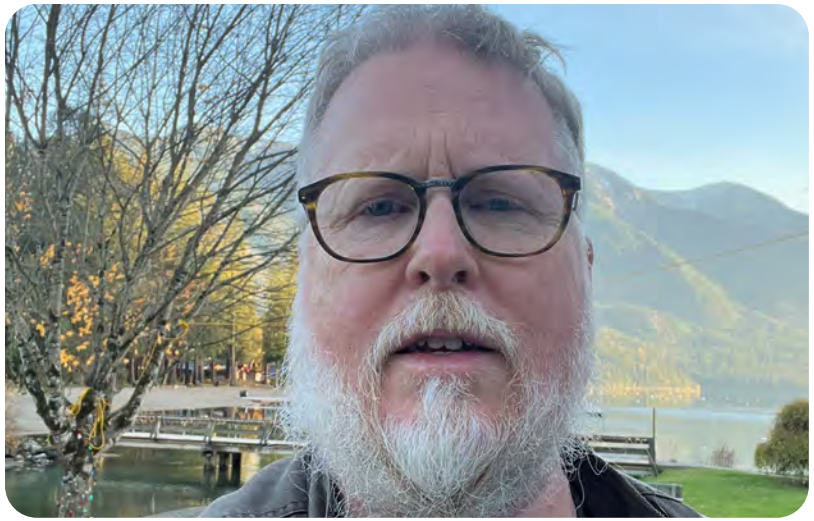
Alex Blania co-founded Tools for Humanity (with Sam Altman) to bring a unique vision to life: securing equal global access for everyone to enjoy the opportunities that today's emerging technologies present. In service of this dream, Tools for Humanity helped launch Worldcoin, a privacy-preserving, open-source protocol that promotes direct access to the global economy through a combination of blockchain, the digital wallet World App, and a "digital passport" called World ID, already in use by more than five million individuals.

Identity, of course, is the key to making it all work. "In order to ensure that everyone benefits fairly from the opportunities AI presents, the protocol had to define proof of personhood," Blania says. "Without being able to prove personhood and uniqueness, networks will be prone to opportunities for fraud." This proof of humanity will only increase in importance, Blania warns, as the effort to create a more just global economic system progresses.

To help bring this vision to life, Tools for Humanity developed a hardware solution called the Orb, a custom-designed, state-of-the-art device that verifies humanness using iris entropy, which is significantly higher in entropy than that contained in a fingerprint scan, according to Worldcoin. Blania says the Orb houses an enormously complex array of sensors, cameras, and electronics. But its elegant and simple shell — a gleaming sphere — represents the planet and embodies the Worldcoin mission to serve as an Identity and financial utility for everyone on Earth.

Blania's own background in industrial and mechanical engineering, physics, and computer science — and his appreciation of great design — stems from his childhood in engineering powerhouse Germany. "I built a lot of robots and participated in quite a few engineering and science competitions," he recalls. A sample project: Build a robot to monitor destructive beetles in the forest so caretakers can take preventative rather than reactive measures. "Robots brought me into engineering early on, which ultimately drew me to work to solve challenges surrounding Identity and proof of personhood at a global scale."

Blania is confident that progress will continue in Identity security and global proof of personhood. That's good news for the 4.4 billion people who today lack a legal, digitally verifiable Identity. "It is encouraging," he says, "to see that more time and attention is being dedicated to this field to make financial and Identity systems more accessible." The vision: a global society in the not-too-distant future where everybody on the planet can easily and reliably prove their humanness and uniqueness in any digital space.



IDENTITY 25 HONOREE

John Bradley

Senior Principal Architect, Yubico

> “Giving people a way of controlling and securely storing their cryptographic secrets is what large parts of security depend on.”

John Bradley knows humans are terrible at keeping passwords, and he thinks we need backup. “To be completely secure without completely re-Identity-proofing someone every time, there is probably an ongoing need to manage some number of physical devices,” he says. This could be a hardware security key, a phone, or even your AppleID, which is backed by a hardware security key. But without the hardware, modern digital security’s a non-starter. “Essentially, all Identity problems devolve into key management problems.”

Bradley got his start at a BBS company that became an internet access provider and later worked at an early “cognitive authentication” company that hoped to identify unique individuals based on how they filled in patterns and other behavioral tests. (“Eventually, that might become practical,” Bradley says, “but not given the technology that we had then, and probably not given the technology that we have now.”) He’s helped develop key standards and specifications for FIDO2 and OpenID. (“Standards is about 80% politics and 20% technology.”) He helped add the authentication protocol layer to OAuth, and he’s been arrested at the White House. (“It’s complicated,” he says.)

Today, as the senior principal architect at Yubico, Bradley is helping companies understand the evolution of trust. “Let’s say a student in Alabama is applying to King’s College, Cambridge. How does Cambridge know it can trust this high school transcript from Alabama?” he asks. “There’s not just one network of trust — we now have multiple interlocking webs of trust. That’s one of the things that I’ve been working on, which isn’t sexy yet because nobody understands that they have the problem.”

Bradley sees the world shifting partly away from two-party redirect federation — where users use Google or Facebook accounts to log in to any of hundreds of sites — to a more anonymous three-party redirect model like digital wallets. “Maybe it’s okay for Okta to know every place that you sign in, because in theory it’s all part of your work and your employer gets to say where you get to log in,” he says. “But is it okay for Google to know every place I have an account?” For consumers, wallets enable a more private world, where the State of Washington might issue your driver’s license, but they don’t get to know you used it at a marijuana dispensary.

The JOSE specifications he developed for OpenID Connect, which formed the underpinnings of today’s emerging next-gen three-party protocols, came out in 2014. (“So it only takes 10 years to be an overnight success,” he quips.) Today, Bradley would love for people to start backing up their iCloud keychains and Apple accounts with a hardware security key — or at least to use a hardware backup to re-establish their identity on devices. And he’d like big companies to nudge consumers along. “Apple doesn’t make you use their security settings, and Google doesn’t make you use advanced protection,” he laments. “Sophisticated anti-phishing authentication methods don’t work if folks don’t use them.”

IDENTITY 25 HONOREE

Christiaan Brand

Product Manager, Identity and Security, Google

> Passwords are the real problem. And as long as we're going to have them around, the best we'll be able to do is stick Band-Aids on top.

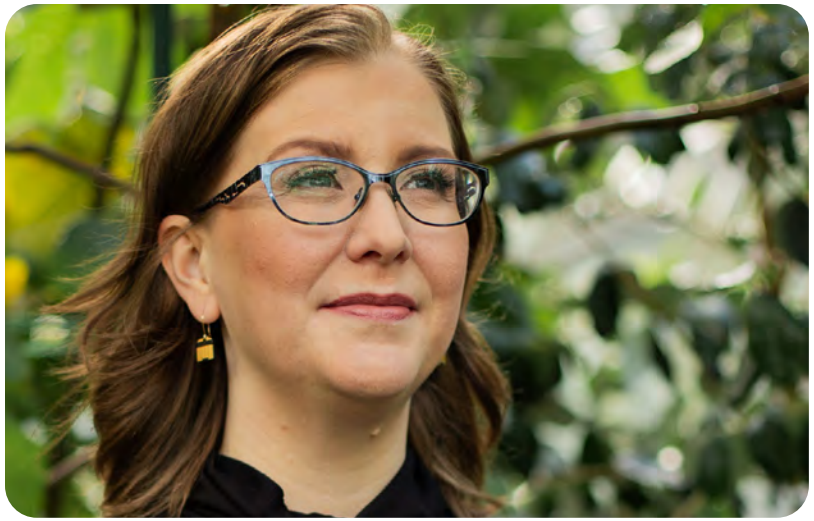
Christiaan Brand has worked in Identity and security for 15 years, and he's spent a lot of that time trying to take down one annoying, unreliable, persistent adversary: the password.

For Brand, now the Group Product Manager for Identity and Security at Google, this quixotic quest began in 2008 when he co-founded Entersekt, a company that helped financial institutions use push authentication to safeguard client accounts. "I soon realized that passwords are the real problem," he says, "and as long as we're going to have them around, the best we'll be able to do is stick Band-Aids on top. What we really needed was to reimagine the way that authentication works on the web."

In 2013, Entersekt joined the FIDO Alliance, an industry association creating authentication standards to phase out passwords; Google joined the alliance the same year. But customers haven't adopted, by and large, the strong authentication protocols that exist. Brand realized if the world was going to leave passwords behind, the biggest technology platforms would have to be involved in making solutions happen. Two years after his company joined FIDO, Brand joined Google.

Companies already knew how to build hardware-based security keys, but adoption was a challenge. The solution: Build the technology into the smartphones everyone already carried everywhere. "We had to meet users where they were," Brand says. In a blog post he co-wrote in May of 2023, he announced Google's support for these "passkeys" as an easier and more secure alternative to passwords: first for Google Accounts and later for Google Workspaces. Brand believes smartphone-based passkeys are on course to radically transform Identity. They're ideal for FIDO-approved multi-factor authentication because they seamlessly combine something a user has (the phone) with an extra layer of protection from something they are (e.g. biometric verification) or that they know, like a security code.

As co-chair of the FIDO2 technical working group, Brand works with large companies like Microsoft and Apple to define requirements and standards then implements them in the platforms that Google owns — in particular, Chrome and Android. Helping to define next-gen authentication protocols and then integrating them into products at scale is a remarkable achievement. "What I've been most proud of," Brand says today, "is taking the concept of phishing-resistant authentication, which started with the security key, all the way through the evolution to passkeys, getting it implemented by all the major platforms, and offering it to Google users as an easy to use, more secure alternative to passwords." Now that Identity has become a mature field, Brand believes it could launch exciting new career opportunities for the next generation. "I think we're going to see more emphasis on Identity leadership in companies," he says. "Perhaps we'll even end 2024 with some newly minted 'Chief Identity Officers' at large companies."



IDENTITY 25 HONOREE

Sarah Cecchetti

Head of Product, Cedar Policy Language, AWS

> The tools and standards we're defining in 2024 will establish interoperable fine-grained authorization as a mainstream standard, and fundamentally change the way we think about information security."

Sarah Cecchetti serves as the Head of Product for Cedar Policy Language, a groundbreaking open-source project. Her journey began as a developer at the University of Washington, where she was recruited by their Identity team. They taught her everything they knew about Identity. She dove headfirst into learning about new Identity standards and specifications by poring over documents, immersing herself in the work, and collaborating with other industry professionals. She then co-founded IDPro, a nonprofit professional association for Identity specialists, which was a significant milestone in creating educational resources and certifications for aspiring professionals.

While working as a consultant, Cecchetti collaborated with NIST to update the standards for measuring Identity security. "NIST measures things: How much is a gallon? How heavy is a kilogram? And in the 21st century, they started measuring Identity: How secure is an Identity solution? The standards for that hadn't been rewritten for a long time, and they were starting to show cracks," Cecchetti shares. This experience contributed to her recruitment by Pam Dingle at Ping Identity, and later by Darin McAdams at Amazon, where she has since worked on several projects that have expanded her knowledge and expertise in the field.

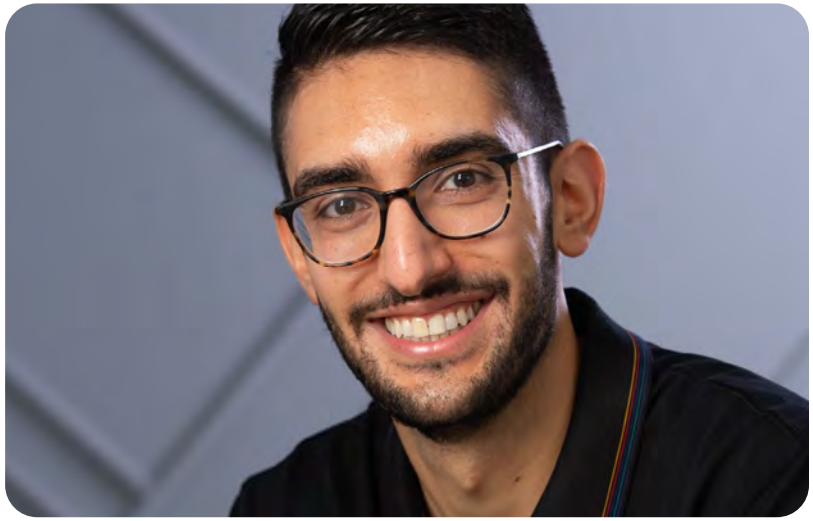
Cecchetti continues to contribute significantly to the Identity industry's growth. That's no small feat at Amazon, a company that authorizes high volumes of API calls rapidly, logging over 500 million calls authenticated per second. To address customer requests for utilizing Cecchetti's authorization solutions in their applications, Cecchetti and her team developed a unique and performant language using automated reasoning, a specialized field of computer science. "We are the first company in the world (as far as we know) to build an authorization service in a mathematically provable language so that the security of the service can be proven," Cecchetti says. The service is built on Rust programming language for optimal speed and safety. This groundbreaking innovation — which has not existed before in the informational security world — allows Cecchetti and her colleagues to efficiently confirm access to resources across large organizations with numerous users and permission policies.

Looking ahead, Cecchetti sees the greater potential of these technologies. OAuth was originally intended for interoperable authorization, which allows organizations to establish rules concerning the access levels they grant under specific circumstances. However, it has instead primarily been utilized for interoperable *authentication* — merely ensuring that users are aware of their passwords. "It's actually capable of much more, and the tools and standards that we'll be defining in 2024 will bring interoperable fine-grained authorization into the forefront as a mainstream standard," Cecchetti promises. "This will fundamentally change the way we think about information security on the internet."

IDENTITY 25 HONOREE

Armon Dadgar

Co-Founder and CTO, HashiCorp



> “The biggest challenge I see is that most organizations focus only on human Identity rather than thinking about machine and application Identity.”

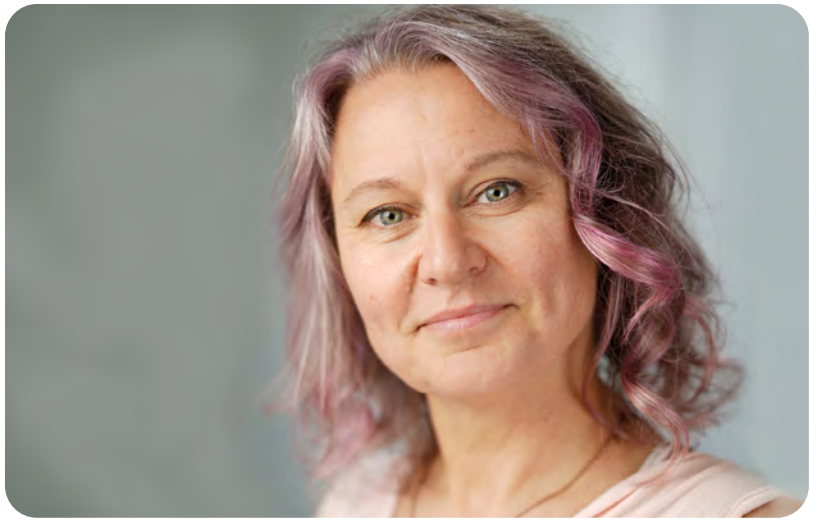
At the University of Washington in 2008, undergraduates Armon Dadgar and Mitchell Hashimoto worked on a research project that leveraged then-emerging public cloud technology to simplify digital access for university scientists. After graduating, the two worked together as software engineers at a mobile advertising network, where they had to home-grow much of the management tooling that powered the platform’s cloud infrastructure. They noticed a broad need for cloud automation solutions and knew Identity would become central to the security of cloud infrastructure, which opened up a business opportunity.

HashiCorp was born in 2012, bringing a fresh, Identity-based cloud-native security approach to a market itching to adopt cloud and multi-cloud solutions. “Security lifecycle management is critical to building in the cloud, and Identity is foundational to building secure infrastructure,” Dadgar, now HashiCorp’s CTO, says. “I’ve been a longtime evangelist of Zero Trust approaches to security and why they are necessary for organizations adopting public cloud.”

Though the security threats enterprises face will surely continue to increase, Dadgar believes true Zero Trust is achievable. The issue isn’t the tools: Most of the human-user security gaps that attackers exploit today can be addressed with existing technology, he says, including passwordless authentication systems and modern privileged access management. The issue is that enterprises are slow to adopt a Zero Trust mindset and commit to a strategy for implementation, even as the number of endpoints, devices, and applications grows and it becomes ever clearer that traditional perimeter security models no longer work.

“The biggest challenge is that most organizations focus only on human Identity rather than thinking about machine and application Identity as well,” Dadgar says. HashiCorp’s products, like Boundary and Vault, are designed to provide a more modern approach to security threats, enabling organizations to securely enable low-friction access to multi-cloud environments at scale, through safely automated processes. “Workload Identity has become critically important, given the massive scale of cloud adoption,” Dadgar asserts. “And generative AI has the potential to significantly impact Identity management and security more generally, to help human operators better scale to manage the cloud-scale challenge of Identity management.”

There’s a lot of innovation happening on the product development front. But Dadgar treats industry events like the annual HashiConf conference (in Boston for 2024) as a chance to deliver product updates to customers and an opportunity to learn from the street what’s working and what isn’t. “My favorite aspect is hearing directly from our customers about how our products affect their organizations,” he says. “I always learn something new, and I come away from every conference energized to keep working for our community.”



IDENTITY 25 HONOREE

Pamela Dingle

Director of Identity Standards, Microsoft

> A huge wave of disruption is coming in Identity security, and we will need the next generation asking hard questions and postulating new best practices."

Pamela Dingle, a self-described Identity geek, characterizes her early job installing Netscape directory servers as Identity work before it was recognized as a thing. Her Netscape work caught the eye of a boutique consulting firm called Nulli Secundus, where she worked for nearly eight years starting in 2001. She then spent nine years as a senior technical architect at Ping Identity before becoming the Director of Identity Standards at Microsoft in 2018, where the commitment to open Identity standards was already strong.

Being a Director of Identity Standards ironically involves getting comfortable with a bit of ambiguity, according to Dingle. "To work in Identity standards is to work with uncertainty right up until the day a ratified standard eliminates uncertainty," she explains. "Many of the critical specifications that will drive the next decade of innovation are being developed now, but there are a lot of factors at play: You need to have the right momentum in the community, the right internal desire to implement, and the right tolerance for the iterative nature of contributing expertise and ideas." And all parties to the emerging standard must be prepared to settle on a consensus that may not exactly match anybody's original vision.

Dingle says the notion that the Identity community is moving towards a single security standard is a popular misunderstanding. "Neither Microsoft nor the industry are moving toward a single global set of Identity standards," she asserts. "It isn't that there are different camps. It's that all the campers are pitching tents in the same football field, with a full game in progress and the marching band circling all the tents. The goal isn't for a perfect specification — it is for repeatability, predictability, and secure stability."

As a corollary, this means nobody should expect older standards to disappear anytime soon, warns Dingle. "As long as older standards can remain crypto agile and are doing their jobs, they will continue to be workhorses in Identity Access Management (IAM) architectures everywhere," she predicts.

At gatherings such as the Burton Group Catalyst conference, Identiverse, and the Directory Experts Conference, a booming community of folks has long debated the finer points of IAM. Dingle says this "Identity gang" represents a community of thoughtful architects excited to discuss evolving standards and best practices.

"My personal journey in Identity was — and is — much more about the people than about the projects or the companies," says Dingle.

We're going to need that Identity gang's best efforts to stay one step ahead of the threat actors. "There is a huge wave of disruption coming in Identity security, and we will need the next generation asking hard questions and postulating new best practices," says Dingle. "My biggest hope for the Identity space is that we can make sure the next generation of Identity professionals are welcome and can effectively build on what has come before."

Why Identity Matters

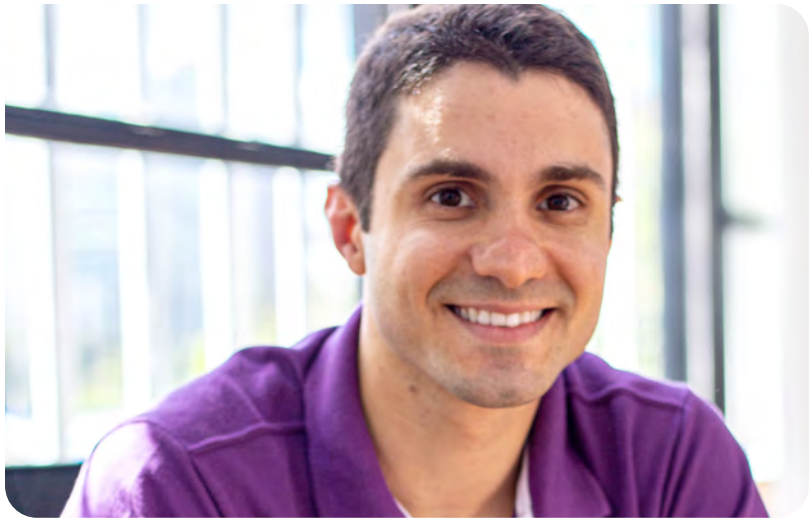
> “Strong Identity management laid the foundation for the next-generation security that cloud-first enterprises need.”

Why celebrate Identity now, in 2024? Because we’re at an inflection point where Identity and security have become inseparable. As business processes and customer activity accelerated their shift to the cloud in recent years — sped up, in part, by the pandemic — security challenges multiplied, and threat actors went on a feeding frenzy. What saved us from chaos was Identity management.

Specifically, strong Identity management laid the foundation for the next-generation security that cloud-first enterprises need. When remote teams demanded quick and secure access to their apps, assets, and accounts at any time and from any device, and when home-bound customers shifted the bulk of their shopping online, Identity management was the foundation that kept all that new remote access secure. And it’s all thanks to the groundwork laid by pioneers of Identity, including the ones honored here.

That’s why Okta chose this moment to start celebrating these visionaries who have worked tirelessly for years or decades, making significant contributions that have relentlessly advanced the cause of strong Identity. Those contributions include security, governance, and privacy standards, authentication and authorization tools that let businesses scale, automated onboarding, offboarding, and lifecycle management, and a lot more.

By highlighting the achievements of Identity pioneers, we hope to foster a deeper understanding of the ability of Identity technologies to tackle the security challenges of our time and inspire future innovation in this domain. We may not know exactly which Identity standards we’ll adopt in the coming years, what processes and protocols we’ll follow, or which exact tools will keep us secure in this ever-evolving threatscape. But there’s every reason to believe we’ll continue staying one step ahead of the threat actors, thanks to the nonstop contributions of people like the Identity 25, who never stop making sure we’re empowered yet safe, private yet connected, and well-prepared to confidently tackle the challenges of the decades to come.



IDENTITY 25 HONOREE

André Ferraz

Co-Founder and CEO, Incognia

> Connected cars, home appliances, hospital equipment, and many other objects could be manipulated against us."

More than a decade ago, André Ferraz's father Carlos introduced him to the legendary computer researcher Mark Weiser, who famously predicted a world of "ubiquitous computing" where the machines were everywhere, in every device, and nearly invisible. In the years that followed, Ferraz was fascinated by the man's ideas, and a little horrified as well. "A world in which every object is smart would provide a lot of convenience to people, but, at the same time, any invasion of privacy could lead not only to digital consequences but also physical ones," Ferraz would write later. "Connected cars, home appliances, hospital equipment and many other objects could be manipulated against us."

These concepts drove Ferraz as he embarked on an academic career in computer science: first at the Federal University of Pernambuco in Brazil, and then at Stanford and Harvard. A passage from Weiser's groundbreaking 1991 article in *Scientific American* about the digital future stays with him: "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it." To Ferraz, Weisler's vision was a guiding light. "It demonstrated to me how important frictionless Identity solutions would become as technology evolved," he says.

To find these solutions, in 2020 Ferraz launched Incognia, a company that uses location Identity to authenticate 400 million customers' smartphones in over 35 countries. His technology relies on a relatively simple and effective concept. The unique pattern of where customers travel over time can help verify their Identity as surely as a fingerprint or a facial scan. Layered with device integrity checks and multiple location signals, Ferraz says, the approach can foil threat actors' ability to engage in creating fake accounts, account takeovers, GPS spoofing, app cloning, and other tricks. "My goal with Incognia is to build innovative fraud prevention and authentication solutions that actually do not add any friction to the user journey," he says today. "This is a significant paradigm shift."

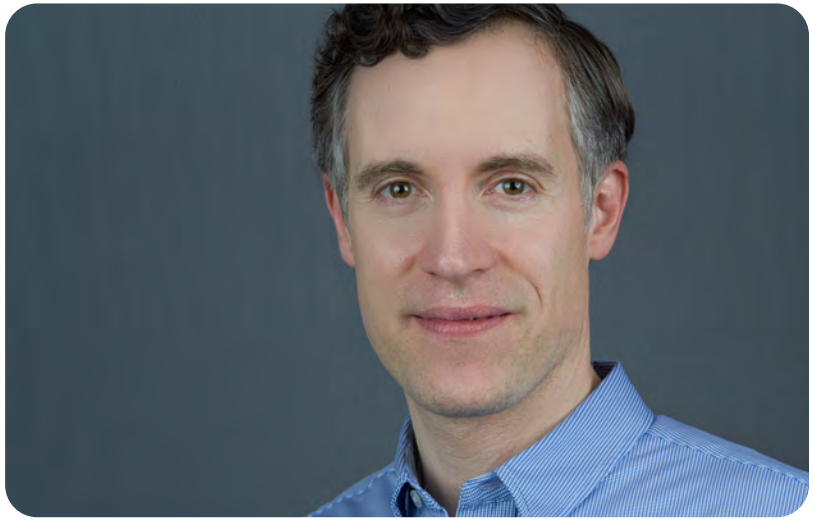
Generative AI is giving fraudsters powerful new tools to compromise customers' identities. Chatbots allow fraudsters to scale phishing attacks, and deepfake technology is becoming more sophisticated at cracking biometric authentication processes. But location intelligence gives customers an extra layer of security beyond verification codes and biometric data: It can, for example, help check devices, locations, and apps against a watchlist associated with fraud. Ferraz compares it to catching an intruder outside your house by identifying the set of lockpicks in his pocket.

As our science fiction makes clear, the potential for the machines to turn against us is always there. But Ferraz believes Mark Weiser's ideas contain a powerful insight to help secure customers' identities. "Today, our vision remains similar to Mark's: to help build a world where digital trust is unseen yet part of our everyday lives."

IDENTITY 25 HONOREE

Jonathan Finkelstein

Founder & CEO, Credly and SVP Workforce Skills, Pearson



> “Identity is everything that makes you who you are — including your unique skills, capabilities, mindsets, knowledge, and experiences.”

Entrepreneur magazine reported a startling fact in December 2022: The median tenure for salaried employees had dropped to just 4.1 years, part of a downward trend that had challenged S&P 500 companies for the previous dozen years. “It’s clear that the same experts and expertise your business relies on today are unlikely to be there tomorrow,” wrote Christopher Allen in the article. To retain talent, he proposed, companies would have to deliver credentials for useful training that helps employees advance, and HR pros would have to find better ways of assessing the skills of applicants.

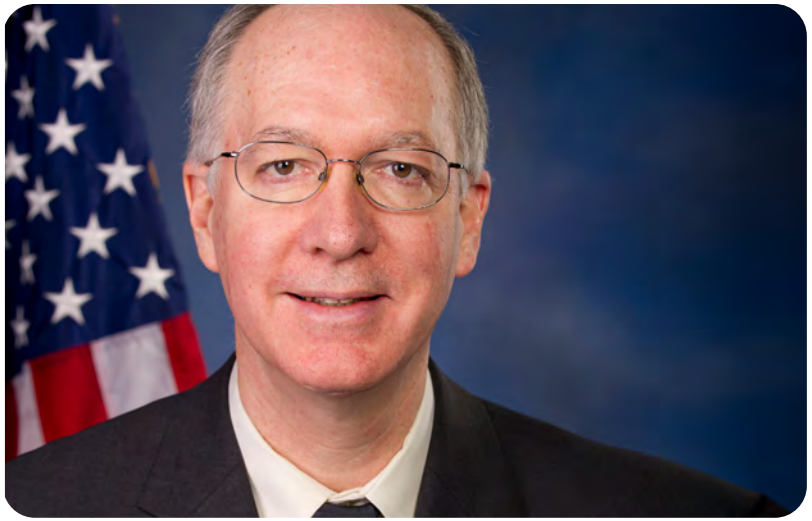
Jonathan Finkelstein has devoted his career to addressing both of those problems. In 2012, he founded Credly, which helps employers create and manage verifiable digital credentials for their employees. The Credly network makes it easier to search for the specific skillsets a manager needs, and creates direct connections between learning and workforce opportunities.

“To me, Identity has always meant far more than a name or number on an ID card,” says Finkelstein. “It’s everything that makes you who you are — including your unique skills, capabilities, mindsets, knowledge, and experiences. Much of my professional journey has centered on elevating those aspects of human Identity that make each person unique.”

Finkelstein is now an SVP at Pearson, which acquired Credly in 2022 and broadly tries to help individuals directly connect their skills to new opportunities and better career outcomes, helping organizations maximize the potential of their people. The workforce skills solutions that Finkelstein manages span strategic workforce planning, aptitude and role assessments, digital credentialing, language learning, the GED, and vocational qualifications. They give clients comprehensive real-time data on people’s verified skills and insights into future skills they’ll need.

Through Credly (and now Pearson), Finkelstein has been able to materially advance the way we think about managing the workforce in a digital age. “The network we built around verified skills and talent has redefined the landscape of credentialing and human capital decision-making,” he says proudly. “Credly has empowered thousands of organizations and millions of individuals to translate skills, learning, and credentials into professional opportunities with digital credentials, addressing skills gaps and improving workforce equity.”

Finkelstein sees more radical changes on the horizon, driven in part by AI, and he stresses that companies must find ways to balance assessment needs with privacy and data security concerns. In particular, he cautions, Identity management professionals can’t just replace old credentialing barriers with new ones. But if done right, Finkelstein believes this new model could create a more efficient and equitable future. “It’s a move from seeing employees as placeholders,” he says, “to recognizing them as unique repositories of human skills and capabilities, poised for strategic alignment and growth.”



IDENTITY 25 HONOREE

Rep. Bill Foster

Member, United States House of Representatives from the 11th District of Illinois

> “It’s imperative that we soon establish a secure, interoperable, digital Identity [and] … a framework of standards for all levels of government to follow.”

In a country where nuclear weapons are a pillar of defense strategy and where an insufficient number of graduates with STEM degrees is a drag on the economy, you might think there would be several physicists with PhDs in Congress. But you’d be wrong: There’s just one, and his name is Bill Foster. And he’s trying awfully hard to quickly spin his colleagues up to speed on technological issues the country must solve if it is to continue to lead and expand the free world.

Foster manages to stay above the usual partisan fray in Congress by putting his head down and working. Among his most important responsibilities is chairing the Financial Services Committee’s Task Force on Artificial Intelligence. And his proudest accomplishments include introducing the Improving Digital Identity Act. “It is imperative that we soon establish a secure, interoperable, digital Identity as we usher in the new digital economy,” says Foster. “My legislation would establish a digital Identity task force — comprised of members from key departments and administrations — in order to develop a framework of standards for all levels of government to follow when providing services relating to digital Identity verification.”

If passed, the bill would represent a major step for the public sector, which sometimes lags behind private industry in digital progress. And it could have policy implications as well. “We witnessed a huge spike in Identity fraud in the unemployment benefit context during the early stages of the Covid 19 pandemic,” Foster notes. “A new Identity framework would highlight that a strong-credentialed Identity verification regime will work to eliminate fraud, enhance consumer privacy, improve government operations, and make our digital economy more efficient.”

Foster is the man for the job: He comes to Congress with both private sector and science chops, and he’s been hard at work since he was old enough to vote. At 19, he and his younger brother co-founded Electronic Theatre Controls, Inc., a company that today manufactures more than half of the theater lighting equipment in the United States. Foster later worked as a high-energy physicist and particle accelerator designer at Fermi National Accelerator Laboratory and was a member of the team that discovered the top quark, the heaviest known form of matter.

Not bad for a politician who’s now been in Congress representing his Illinois district since 2008. Representative Foster would probably prefer that the competition for smartest guy in the room be keener, and he’d certainly like to have more allies in advocating for Identity security, but that’s all out of his hands. “I’ve always tried to leverage my knowledge to help inform my colleagues about issues that have technical components, and the digital ID space is a good example of that. I also encourage people with science and technical backgrounds to run for elected office at all levels. We need more technical expertise in Congress.”

IDENTITY 25 HONOREE

Ajay Gupta

Chief Digital Officer for the California Department of Motor Vehicles

> We are committed to learning from our partners to develop and implement the most secure and equitable digital credential solution for Californians."

In the 2016 Jason Bateman animated film *Zootopia*, Department of Motor Vehicle workers are portrayed as sloths. Ajay Gupta, the California DMV's Chief Digital Transformation Officer, is out to shift that inaccurate, pre-digital perception. "DMV service transformation is at the center of a sweeping program," he declares, "that is delivering a huge macroeconomic benefit by creating reusable, flexible, and secure Identity solutions for all government services." It's welcome progress for California drivers and potentially for citizens everywhere.

In delivering and expanding secure digital services for Californians, Gupta has been able to leverage decades of experience garnered in the private sector, including long stints at Deloitte and KPMG. This unique experience yielded valuable insights into differences between public and private approaches to Identity security. "Industry often views privacy as a hurdle rather than as a right in the implementation of their products," Gupta notes. For state government agencies, on the other hand, accountability and responsibility around privacy are paramount, despite the fact that, Gupta acknowledges, "we may not always have the best technical expertise."

This creates opportunities for the private sector to engage with government in some emerging tech innovations: not as a contractor, but more as a partner. Gupta says that his team's role is to show the way without knowing the way. "As policy enforcers, we are in the unique position of creating a responsible roadmap of emerging, unknown innovations," he shares. "But we often must rely on others to explore and explain the new ways of doing things."

This flexible approach can be likened to building a ship while simultaneously sailing that ship, and the key to successfully meeting that challenge is collaboration on all fronts. "We work with federal teams focused on digital credentials. We work with privacy advocates. We work with global standards teams," Gupta says. "We are committed to learning from our partners, because only through learning can we develop and implement the most secure and equitable digital credential solution for Californians." Gupta says that the only way to get the job done right is to establish and nurture these sorts of public-private and public-academic partnerships: Collaboration can be difficult, even in the best of times, but it can also be deeply rewarding.

Gupta acknowledges the tension that often exists between the public's desire to get public services equipped with the latest technology offerings and the potential for security risks as we move to an increasingly digital society. "The DMV team takes all precautions to protect the personal information of all our customers," Gupta says. "We are incorporating a combination of the highest international security standards as we build digital identities for the convenience of California's residents."

IDENTITY 25 HONOREE

Alexis Hancock

Director of Engineering, Electronic Frontier Foundation

> People have the will to choose the right tools, but it's up to the experts to provide those tools by default … making security mindless for everyone."

The pandemic changed people's relationship to technology, and for Alexis Hancock, it dramatically demonstrated the dawning importance of Identity. "I began to see a large push for digital storage of important credentials such as vaccine status," she says. "I'd worked on securing people's communications for a few years leading up to 2020. So my curiosity to investigate digital Identity technology felt natural."

As the Director of Engineering for the Electronic Frontier Foundation (EFF), a non-profit that famously advocates for digital privacy and civil liberties, Hancock researches issues like digital rights, encryption, and consumer technology, and has long focused on the impact of tech changes on ordinary Americans. "As a public interest technologist, I try my best to always insert equity in new technology, make security easy, and prevent harms from being done with new technology," she says.

Hancock has spent a decade developing web applications and researching digital rights, encryption, and computer technology to help policymakers and others do the right thing. Today, at EFF, she works to keep networks strong and encrypted by managing the Certbot project, a free, open-source software tool designed to help manually administered websites enable secure HTTPS. According to the EFF website, Hancock "believes in an open and equitable web through encouraging local tech literacy, educating other engineers, and advocating for better and stronger tech policy."

In a 2021 interview with *The Washington Post*, Hancock was blunt about the danger of a compromised Identity leading to private information being made public. "Whatever you say on Twitter in DMs between people? Imagine you were tweeting." When online privacy can't be trusted to live up to reasonable expectations, that's the users' problem — but it isn't their fault, she says. "People have the will to choose the right tools, but it's up to the experts to provide those tools by default, rather than making everyone go find the needed protections themselves," Hancock declares. "Making security mindless for everyone is the best defense we have in an expanding technological landscape."

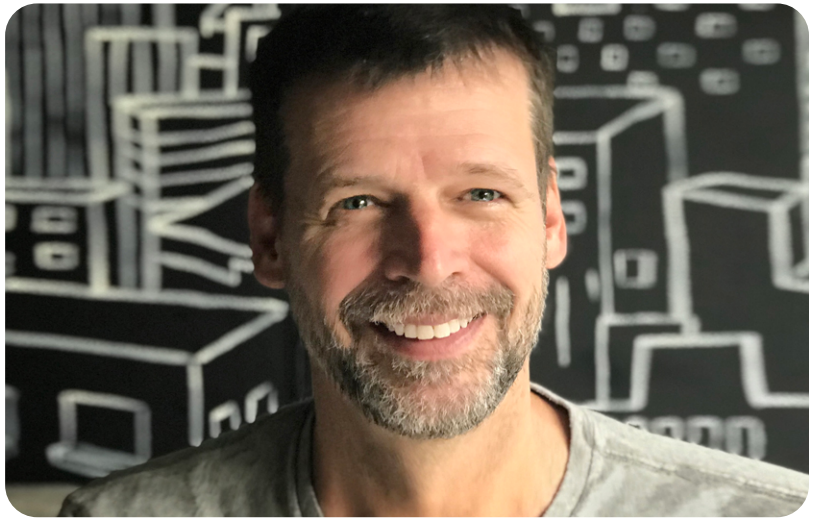
Hancock supports an open, equitable web, encouraging local tech literacy, educating engineers, and advocating for better and stronger tech policy. One of her proudest achievements was advocating for New York State legislation to protect the confidentiality of vaccine information. When this became law in January 2023, the EFF praised Hancock's work in limiting what data could be collected or shared.

More work needs to be done. There's a new legal framework coming out of Europe, for example, called "electronic IDentification, Authentication and trust Services" (eIDAS), but Hancock says the benefits are yet unclear. "It depends on how the framework is implemented, the amount of transparency the EU practices, and how much say citizens have in the process," she says.

IDENTITY 25 HONOREE

Dick Hardt

Founder and CEO, Hellō



“I’m an internet pioneer taming digital Identity. Cyberspace is the new frontier, and Identity security is crucial to securing the frontier.”

You may not have met Dick Hardt in person. But you’ve likely seen his 2006 Identity 2.0 presentation: one of the most impressive and far-reaching in the field. “That Identity 2.0 talk led to my giving 50-plus keynotes, plus invitations to participate in countless Identity workshops,” says Hardt, who says folks still tell him the presentation inspired them to work in the space.

And the influence went both ways, he remembers. “I got exposure to a wide range of perspectives from others in the industry.”

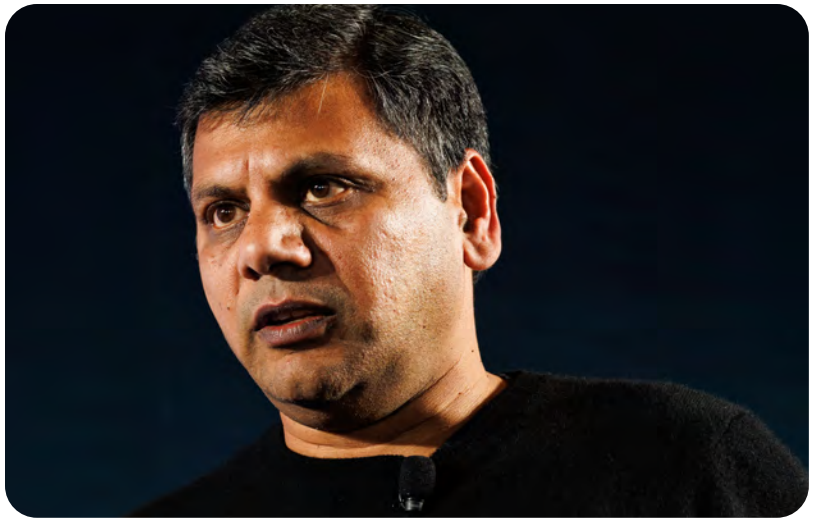
Hardt has focused exclusively on Identity since 2003, when he sold Active State, his six-year old open-source and anti-spam tools company. Still in high demand to speak at popular Identity conferences and to stand behind the podium at places like Harvard, Hardt has remained fully engaged in solving problems, not just talking about them, as a partner architect at Microsoft and a principal engineer at Amazon.

With a wealth of entrepreneurial and working experience, Hardt is concerned about the wide gulf existing today between the solutions created for enterprise Identity and those created for individuals. “We have standardized a lot of Identity for enterprises,” he says. “While there’s still lots of friction to deploy federated Identity, there’s at least a clear path for everybody to walk on. What we haven’t figured out is the path for personal Identity. How do we go online and have a reusable Identity to prove who we are as an individual?”

To explain the value of portable Identity, Hardt draws a parallel to the world of consumer credit before credit cards. “In the old days, if you wanted to buy something, you had to have cash, or you had to have built up credit with that merchant,” he explains. “If you went to a second merchant, they would also want cash, until you built a relationship and established credit. You didn’t have reusable, portable credit until you had general purpose cards where you could reuse the credit from your bank anywhere that accepted Visa. It doesn’t matter where the merchant banks or where you bank: If both parties are part of the Visa network, it all works.”

Hardt recalls how bought-in everyone seemed to be, relatively recently, on an Identity solution that is now understood to be deeply problematic. “Not even 10 years ago, we were still thinking that you would provide an identifier to start an Identity transaction. We’ve now concluded having the same identifier everywhere is a bad idea, because of all the correlation and privacy implications.”

This realization helped inspire Hardt to found his current company, Hellō, in 2021. Hellō’s solution to securing online Identity is to connect credential issuers and users with a system whose government is decentralized. (Hellō is governed by a multi-stakeholder cooperative that ensures users and organizations are both represented). This lets users bring the Identity they already have, and lets developers use existing OpenID Connect tech to create apps that leverage Hellō-brokered credentials. Safe and productive.



IDENTITY 25 HONOREE

Ashish Jain

Chief Product Officer, Arkose Labs

> Key shifts include a prevalence of Cybercrime-as-a-Service, the surge in generative AI technology, and a stronger focus on user privacy."

"In the past two decades, I've had the privilege of contributing to Identity initiatives at companies like Ping Identity, PayPal, VMware, eBay, and currently Arkose Labs," Chief Product Officer Ashish Jain says. "I've had the opportunity to develop solutions aimed at combating fraud and preventing malicious actors from infiltrating systems. This experience has exposed me to the darker aspects of Identity management, providing me with a more comprehensive understanding of the broader Identity landscape."

At Ping Identity in 2005, Jain led a team effort to create the first Identity provider supporting SAML, OpenID and Information Cards. At PayPal in 2009, he spearheaded the effort for the company to become certified by the National Strategy for Trusted Identities in Cyberspace, a collaboration of government agencies and private companies tasked with creating a viable Identity ecosystem. At VMware, he and his team were the first to develop and patent a solution to integrate mobile device management and Identity — one of the core tenets of Zero Trust security. And as the Head of Identity at eBay, his team built the Identity, risk, and trust platform that powered onboarding, authentication, account management, and fraud protection for more than 180 million customers.

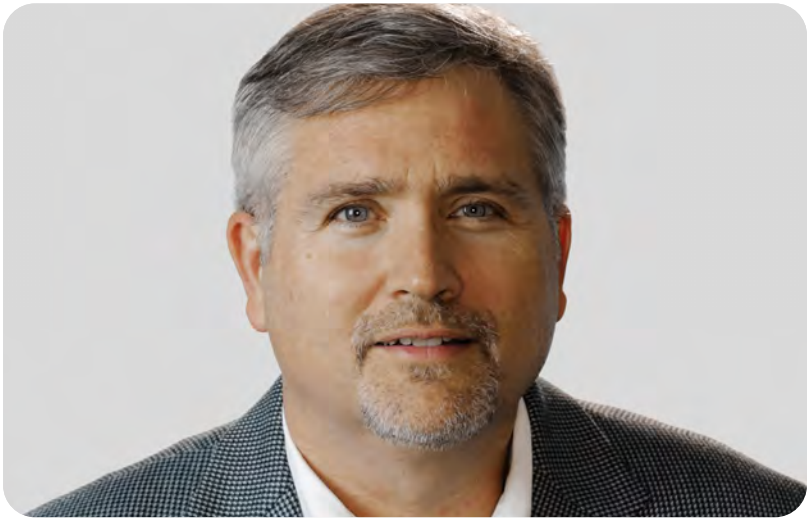
Currently the Chief Product Officer at Arkose Labs, Jain's innovations have included a bot management platform with integrated threat detection and mitigation, designed to safeguard against attacks like account takeover, credential stuffing, fake account creation, and SMS toll fraud. Accolades for this initiative include being listed in *TIME*'s 200 "Best Inventions" of 2023, ranking in Deloitte's Fast 500, and *Fast Company*'s Innovation By Design award. His expertise includes Workforce and Customer Identity scenarios, and his career spans roles as a solution provider/vendor and a large-scale customer. "I have often joked that the Identity domain/community is like a mob," says Jain. "You have the freedom to decide when to enter, but leaving is not a choice you can make."

Much of Jain's focus has been helping genuine users safely navigate the internet. But he also has extensive experience combating fraud and blocking bad actors, and this is where he sees things changing. "Heading into 2024, key shifts like the growing prevalence of Cybercrime-as-a-Service, the rise of generative AI, and a stronger focus on user privacy are heightening awareness of the critical role of Identity," he warns. "These developments are set to significantly impact Identity and fraud solutions." Jain, who has served multiple terms on the board of the OpenID Foundation, is happy about progress towards standardizing authentication in FIDO-certified passkeys, and about advances in Identity verification standards. These include verifiable credentials and systems that spot risk, using tools like device fingerprinting, IP reputation, and behavioral biometrics. "While adoption is still lagging and fragmentation persists," he laments, "there's considerable potential. And the trend is definitely heading toward improvement."

IDENTITY 25 HONOREE

Tom Kemp

Author, *Containing Big Tech*



> “I think the need and desire to have their identity secured and their data protected are universal across all residents of all states.”

“I believe privacy is an inalienable right, and that privacy rights need to be further extended and enhanced in an increasingly digitized world.” Tom Kemp wrote that back in 2020, in support of California’s Proposition 24, the California Privacy Rights Act that passed that year due in no small part to Kemp’s diligent efforts to market and socialize the idea.

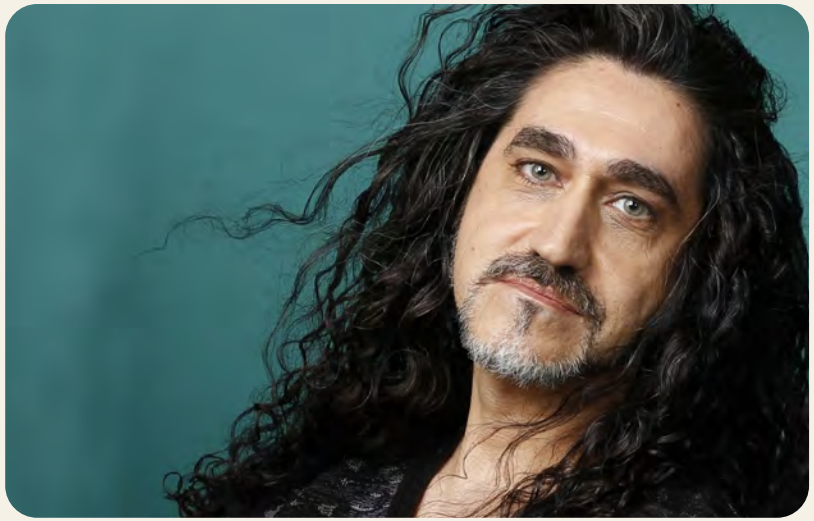
Kemp has been an entrepreneur for more than 20 years, and his experience in business has shaped his views on the intersection between Identity management and privacy laws. “I am fortunate to have started a very successful Identity company that had over 2,000 customers and over 50% of the Fortune 50 as customers,” he says, crediting his activism to the front-row seat he had watching how Identity-related challenges played out in the corporate world. He saw the same bad actors on the web targeting businesses and private individuals, and dedicated himself to pursuing advances in security technology and privacy protection.

Centrify, which Kemp co-founded in 2004, was an early Identity company that delivered directory-enabled networking through a single platform. The enterprise was generating $100 million in revenue by the time it was acquired. Kemp and his friend Adam Au now manage Kemp Au Ventures, a company that pools their personal money to invest in early-stage tech companies.

If you’re not lucky enough to be a startup with Kemp on your board, the easiest way to tap into Kemp’s keen insight is to read all about it. In August, Fast Company Press published Kemp’s book, *Containing Big Tech: How to Protect Our Civil Rights, Economy, and Democracy*. He says it assesses the challenges posed by giant tech companies, emphasizing in particular that AI is a major game-changer poised to revolutionize Identity management, for good *and* for evil.

“AI can be used to strengthen our security posture, with respect to hackers, by better detecting attack vectors,” Kemp says. “But hackers will look to use AI to steal personal data and even our identity through AI-powered deep fakes and social engineering. To me, investing in AI to stay ahead of hackers is key, but in general we need to make sure industry and society are ethically using AI.” Kemp believes there’s a growing consensus that we must build sturdy guardrails to protect consumers without limiting the potential for innovation that the AI revolution promises.

“People increasingly see their personal identity and data as the equivalent of copyright material,” says Kemp. “And they don’t want it being misused or fed into AI to serve other people’s purposes. I think the need and desire to have their identity secured and their data protected are universal desires across all residents of all states.”



IDENTITY 25 HONOREE

In Memoriam:

Vittorio Bertocci

Principal Architect of Auth0 and board director, OpenID

> "In a world that often felt like an echo chamber of repetitive ideas, Vittorio's voice was distinct — an Italian melody of originality and deep insight."

There was nobody more passionate about Identity than Vittorio Bertocci, and nobody who left a more powerful legacy in its service. Bertocci's 20-year dedication to molding theories of Identity into a powerful community and industry included the development of principal Identity-related technologies like OAuth, OpenID Connect, and Azure Active Directory. Until his untimely passing from cancer last year, Bertocci worked tirelessly to advance secure, user-centric digital experiences including internal and external education, product innovation, and customer integration.

Bertocci spent many years at Microsoft, focusing mainly on improving the developer experience and developing core claims-based platform components like Windows Identity Foundation and ADFS, ADAL and MSAL SDKs, and ASP.NET middleware. He was a brilliant technologist, a motivated self-starter, and a staunch proponent of industry collaboration. "The first Identity community that I joined was 'stack overflow,'" he once recalled. "And my peers knew Jack about Identity. And so, I had to go out to Google and find things out. That's where I started."

As time went on, Bertocci was able to redirect some of his creator's passion in the direction of advocacy. He relentlessly pushed for the advancement of crucial industry standards initiatives, and spearheaded efforts to educate technology professionals. Over the years, he dazzled audiences in live presentations, created an endless series of instructional videos, and wrote four books. In his spare time, Bertocci spun new ideas out through his popular blog, cloudIdentity.com, and podcast, "Identity. Unlocked."

Bertocci's passion, wit, and extensive knowledge made him a sought-after speaker at conferences like Identiverse, BUILD, PDC, TechEd, and Cloud Identity Summit, and many other global industry events. On stage, Bertocci revealed a unique capability to breathe life into even the most technical or tedious subjects and spin mundane talks into engaging, impactful experiences. As Joerg Resch wrote of Bertocci in KuppingerCole's blog: "In a world that often felt like an echo chamber of repetitive ideas, Vittorio's voice was distinct — an Italian melody of originality and deep insight."

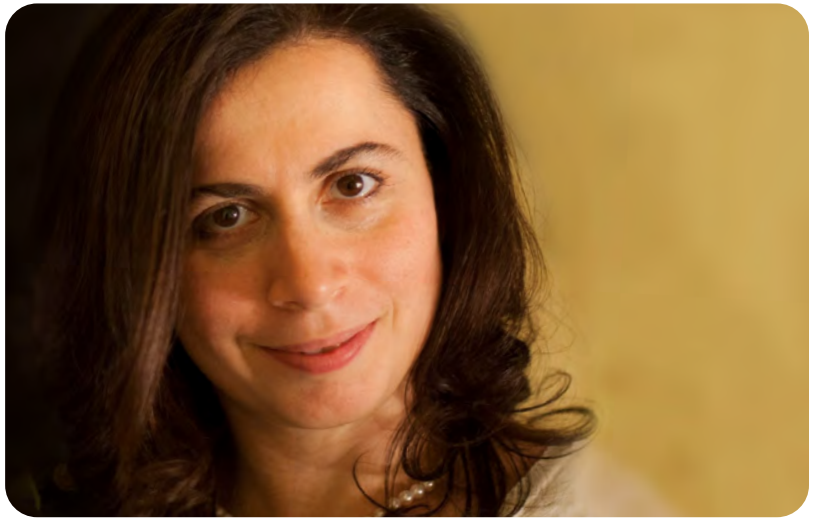
This humble 10th son of a janitor thrived for more than two decades at the intersection of Identity and technology. He understood the potential for Identity earlier than most, and he helped build the Identity industry and community that the world needed, operating under a firm belief that only by sharing our insights and expertise across organizations and companies can we truly succeed. "If you want to advance, you need to collaborate … to develop some level of trust," Bertocci said during a panel talk with industry leaders about the power of community. "We need spaces in which we can leave weapons at the door, walk in, and collaborate, truly, in the spirit of non-zero gain."

He will be sorely missed.

IDENTITY 25 HONOREE

Anna Lysyanskaya

Professor of Computer Science, Brown University



> My goal is to ensure that industry and policy leaders understand that it is possible to protect our privacy even while guaranteeing secure authentication."

Anna Lysyanskaya began researching cryptography out of pure fascination with the underlying math. Then she saw something that sparked her concern. "I realized that the dangers to personal privacy that emerge from using regular Identity management are real," she says. Today, as the James A. and Julie N. Brown Professor of Computer Science at Brown University, Lysyanskaya researches how to balance privacy concerns with the need for systems to authorize users quickly and reliably at scale. Her work has attracted a lot of attention, and she's won awards from the National Science Foundation and grants from companies like IBM, Google, and Facebook. Lysyanskaya has also been on the board of directors of the International Association for Cryptologic Research (IACR) since 2012 and was program co-chair of the Crypto conference in 2023.

In 2007, MIT Technology Review included Lysyanskaya in their annual list of "35 Innovators under 35." The innovation that caught their eye was a novel approach to a "zero-knowledge proof." Theoretically, these proofs allow you to enter a system and receive a digitally-signed credential using a pseudonym; the system can then test your credentials without having any other information about you.

"It turns out that proving that you are authorized to perform an action in a system (such as accessing a document) need not involve revealing your actual Identity," Lysyanskaya says. "Nothing about you needs to be revealed as part of proving that you are authorized, other than the fact that you're authorized." This form of Identity management not only respects users' privacy, but reduces risk — a leak can't reveal information that was never gathered.

IBM Zürich reportedly leveraged these ideas to create its Idemix project, which allows people to anonymize their personal information as they make purchases on the internet to protect themselves from Identity theft and other privacy concerns. The research also helped guide the Obama Administration's 2011 creation of the National Strategy for Trusted Identities in Cyberspace (NSTIC).

Currently on the board of the Electronic Privacy Information Center, Lysyanskaya is on a mission to teach leaders about the true promise of Identity management systems. "The few policy events I want to attend are those where I think high-level decision-making is taking place," she says. "My goal in attending those is to ensure that industry and policy leaders understand that it is possible to protect our privacy even while guaranteeing secure authentication."

One hopeful sign: The general public is becoming more sophisticated about the tools available out there. "The fact that cryptographic technologies, from digital signatures to zero-knowledge proofs to anonymous credentials, have entered the popular lexicon is very exciting," she says, "and hopefully bodes well for balancing secure authentication with personal privacy.

IDENTITY 25 HONOREE

Eve Maler

President and Founder, Venn Factory

> I began this journey by questioning digital consent. We're all tired of websites and apps spying on us and sharing — or breaching — our most personal information."

Eve Maler sees a lesson for Identity professionals in the successful capture of a serial killer.

"The Sacramento Killer was apprehended through family-member searches conducted with the help of popular DNA profiling companies," she says. The lesson: Your Identity is not just who you are, but your connection to others — even when it's something as intensely personal as your genetic code.

This insight is part of Maler's career-long quest to put the user first in Identity solutions. More than 20 years ago, Maler was at Sun Microsystems, tasked with creating a standard protocol for what was then just called "web security services." She co-founded and chaired the group that created SAML, staying involved through SAML 2.0, and has worked on a long string of Identity-related projects, including Liberty Alliance, different components of OAuth, and User-Managed Access (UMA).

"For a while now, I have been focused on making Identity relationships the center of the connected world," Maler says. "And it seems like this idea is finally getting the attention it deserves. It only makes sense that relationships between entities are starting to play a more important role in access control and other decision-making processes."

Maler did a great deal of her work while serving as CTO of the San Francisco-based company ForgeRock, where she's focused considerable effort toward giving users more control over their digital data than clicking "yes" on a consent form allows.

"I began this journey by questioning digital consent: We're all tired of websites and apps spying on us and sharing — or breaching — our most personal information," she says today. "Unfortunately, there is a manipulative pattern built into the very notion of consent: Once a service asks you to opt in, you are already at a disadvantage."

This loss of privacy and control costs companies as well as users, Maler believes — in eroded trust, and in huge fines when companies are later seen to have breached privacy regulations.

"Giving people control must include capturing their real preferences for who can access what, when, and why," she says. "My work on the User-Managed Access protocol and Identity relationship management grew out of this need for a user-centric view of authorization." In 2010, Maler obtained a U.S. patent for a system designed to designate different Identity providers in separate "circles of trust" based on their relationship with the user.

What's up next for Maler is a new beginning. She's recently launched a new venture called Venn Factory, an Identity-focused strategic consultancy. "At Venn Identity, I'm guiding enterprises and tech vendors on their journeys of embracing the future of Identity."

IDENTITY 25 HONOREE

Caryn Seidman Becker

Chair and CEO, CLEAR

“Our vision was to build a secure Identity company and take it beyond travel so that you can use it in all the things you do in your everyday life.”

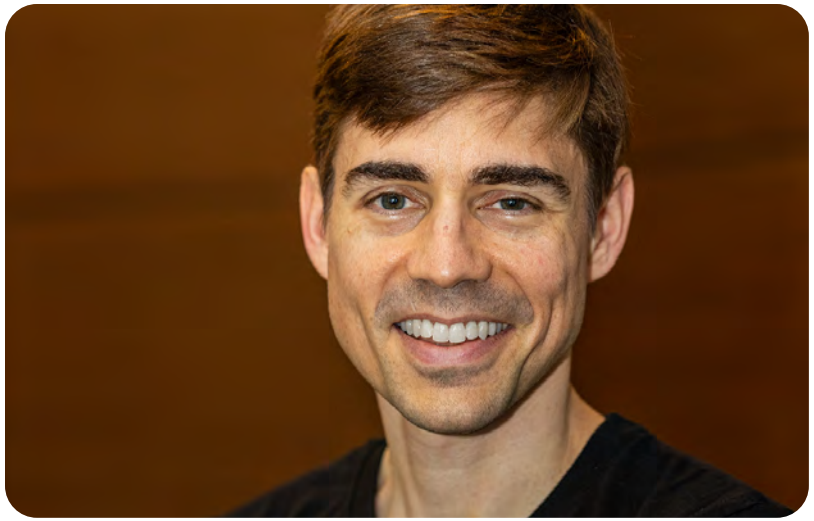
The Identity challenge of our time is secure authentication that doesn’t impede the user experience, and one of the most prominent companies putting this ideal into practice is CLEAR. Under Chairman and CEO Caryn Seidman Becker, the company’s technology offers the promise of secure but frictionless experiences for its members. “We started in travel because travel is the place where Identity, customer experience, and security collide. But the vision was always so much more,” says Seidman Becker. “It was to build a secure Identity company obsessed with the customer experience, and take it beyond travel so that you could use it in all the aspects of your everyday life.”

Seidman Becker’s route to Identity security was unusual. As a student at the University of Michigan (and a huge Wolverines fan), her dream was to be a sports journalist. She worked three summer jobs before her senior year, including as a sports intern at a Toledo TV station covering the Mud Hens and as an investment banking intern. “I was surprised when the investment banking job appealed to me the most,” she recalled. She joined an investment firm after graduation, eventually starting her own asset management firm called Arience Capital.

As an investor, Seidman Becker learned about biometrics and became a believer. She recalls that she was also a jittery frequent flier. When Arience shut its doors in 2009, she saw a unique opportunity in CLEAR. “CLEAR would allow me to leverage different areas of my expertise, solve a problem I was personally dealing with as a nervous flier, and make a difference in the world.” Under Seidman Becker’s leadership, CLEAR has already begun ambitious plans to expand easy, secure authentication experiences beyond air travel to healthcare, financial services, digital marketplaces, stadiums and hotels, rental-car check-ins, and more.

Seidman Becker says that CLEAR’s free Identity verification service on LinkedIn gives consumers and businesses the confidence of knowing that the people they encounter on the networking platform are real and that their Identity is authentically represented. So far, the data reportedly shows that individuals who have verified their profile on LinkedIn with CLEAR receive 60% more profile views, 50% more comments, and 30% more messages from other professionals.

Similarly, in healthcare, CLEAR partners with leading institutions like University of Miami Health System and Wellstar Health System to help each patient create a universal health identity. This seamlessly connects their disparate health information (like their insurance, copay, credit card, and electronic medical records) using a single sign-on, HIPAA-compliant account. “We started CLEAR because we knew Identity is foundational and would unlock so many experiences in our daily lives, both physically and digitally,” Seidman Becker says. “And today we are seeing the rest of the world understand the importance and need for Identity.”



IDENTITY 25 HONOREE

Mark Straub

CEO, Smile ID

> “Identity in resource-constrained markets is a key part of the solution to unlocking tremendous value and creativity in emerging economies.”

Smile ID’s Mark Straub is on a mission — one that’s critical to improving futures for the people of an entire continent. “The thing that drives me is the opportunity to change the trajectory of the lives of large numbers of people in Africa,” he says. “To change the future of people’s lives — it’s really a once in a lifetime opportunity, and I feel it’s worth spending my life on it.”

Smile ID’s vision is to ensure that all Africans, anywhere in the world, can easily verify their identities. But Straub’s first glimpse of an Identity solution working on a massive scale came while working in India. He had the unique opportunity to spend time with the original technical team behind India’s Aadhaar national ID system, the world’s largest biometric identification system. “Learning from the Aadhaar team was personally fascinating and professionally transformational for me,” Straub recalls.

But putting that vision into practice was no small challenge. “The rise of generative AI presents unique challenges to large financial institutions that face intense demands from customers to make money available globally, all the time, while also protecting safety and security,” he points out. “Digital KYC [Know-Your-Customer] Identity companies like Smile have to provide solutions that deliver the same level of confidence as a bank officer would achieve face-to-face, but with only digital images and signals from a device and network.”

When Straub and his team started Smile ID seven years ago, there was a movement funded by the UN and non-profits dedicated to ensuring that all people around the world could obtain a “legal identity” by 2030. Among other things, this movement resulted in the establishment of the ID4Africa community and an annual conference (in which Smile ID participates). “Our unique focus on Africa means that we engage in regular dialogues with our public-sector counterparts,” Straub explains, “sharing best practices on how national ID design and delivery — especially digital APIs — impact adoption by individual citizens and by the private sector.”

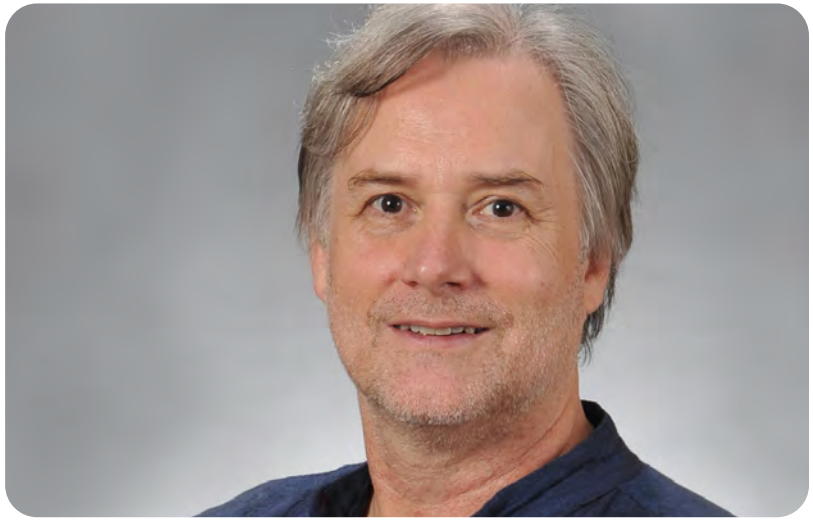
Straub is particularly proud of the lengths to which Smile ID goes to address a common technical issue: namely, the challenge of integrating multiple device types, operating systems, and use cases. “We now have over a dozen integration options, including a suite of mobile and server-side SDKs,” he shares, “as well as a no-code solution (Smile Links) that can be used by a startup or a bank officer without writing a single line of code.”

The results are compelling. By the time you’re reading this, Straub projects, Smile ID will have verified no fewer than 100 million identities across Africa. This represents a small fraction of the continent’s estimated 1.4 billion population, so there is a long way to go, but it’s a milestone to be proud of on a long and important journey.

IDENTITY 25 HONOREE

Paul Syverson

Mathematician, U.S. Naval Research Laboratory



"My focus is on giving domain owners more control over the authentication of their site's identity rather than leaving this entirely to Internet authorities."

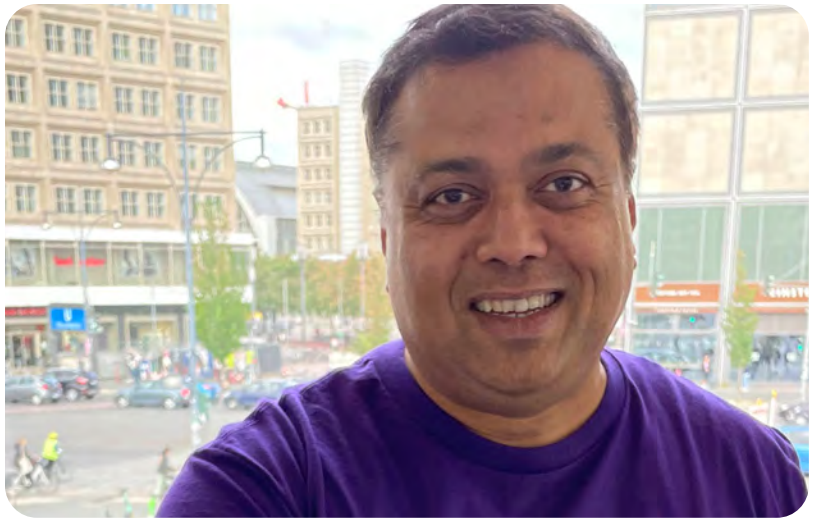
Paul Syverson has been a researcher for more than 30 years and has authored over 100 publications. But one of his projects is far more "Internet famous" than anything else he's done: He and two other computer scientists created the Tor network in 2002, which allows millions of users to explore the web anonymously with more than 6,000 servers.

A mathematician at the U.S. Naval Research Laboratory, Syverson has spent his career thinking deeply about Identity. His PhD dissertation in logic at Indiana University Bloomington formally represented the different types of knowledge someone could have about an identity, such as whether two identities are the same or whether an identity has a specific property. Syverson joined the U.S. Naval Research Laboratory in the late '80s, and by the mid-90's he'd started work on "onion routing" to help protect the identities and affiliations of government users on the public internet, and of public users visiting government sites. ("Onion routing" encapsules online communication in multiple layers of encryption, like the layers of an onion, protecting both parties' identities from prying eyes.) By 1996, the lab had created a publicly-available, Navy-run prototype network, with virtual relays on a single server.

In 2002, Syverson, along with Roger Dingledine and Nick Mathewson, took onion routing to its logical extreme by launching the Tor network. Tor has been an invaluable tool for dissidents, whistle-blowers, and victims of domestic violence to speak out safely, for ordinary users living where internet access is blocked, and for others. But media reports often focus on Tor's sensational dark side: as a tool for criminals to engage in anonymous criminal activity. Syverson explains why the good far outweighs the bad. "Technologies are often initially identified with proscribed and problematic use cases before their broader value is recognized," he says. The printing press, he notes, was seen as a national security threat in 17th-century England. And web encryption followed a similar path: It was originally considered an essential tool to enable secure e-commerce, and was only later accepted as standard security practice for accessing all websites.

Emphasizing that he's speaking for himself, not the lab or the Navy, Syverson predicts that as the complexity of the web increases, users will need anonymity options that are more flexible. "If you are connecting to a new-to-you medical site to query about a sensitive ailment," he says, "you may want to initially be as anonymous as possible." Another scenario: Some services that process sensitive medical data, like HIV test results, might accept anonymous requests but want to verify credentials like citizenship.

Syverson believes that Identity professionals will need new tools to manage this nuanced security environment. "I do expect the management of digital self to continue evolving," he predicts, "in fascinating and sometimes unexpected ways."



IDENTITY 25 HONOREE

Atul Tulshibagwale

CTO, SGNL

> “Dynamic, continuous access management can mitigate the impact of Identity-related breaches, which can still happen after passkeys are deployed.”

An early trailblazer who has made a profound impact in the Identity space, Atul Tulshibagwale arrived in America from India back in the 1990s, during the infancy of the public web. “After the Netscape IPO, I figured it would be important to know ‘who’s on the other end’ on the internet,” he says.

And he never looked back. Tulshibagwale began his career in cryptography and was one of the first engineers at VeriSign. The certificate authority was helping create standards and protocols to authenticate digital document signers in the chaotic cyberspace environment, and he vividly remembers working with key players to solve problems during that tumultuous time.

These experiences ultimately inspired Tulshibagwale to start his own company, Trustgenix, developing federated Identity solutions to help users link their identities across Identity management systems so they could work across them securely and with no drag. “We not only helped define the SAML 2.0 standard,” he adds, “but also conceived the ‘federation server,’ which is now a component of almost all organizations.”

After HP acquired Trustgenix, Tulshibagwale eventually found his way to Google, where he developed the Continuous Access Evaluation Protocol. “CAEP allows publishers and subscribers to communicate a wide range of information about their active user sessions,” he wrote in a 2019 blog post, explaining that if anything changes about a session — a policy update or a device change — CAEP lets systems share that information quickly, to maintain security.

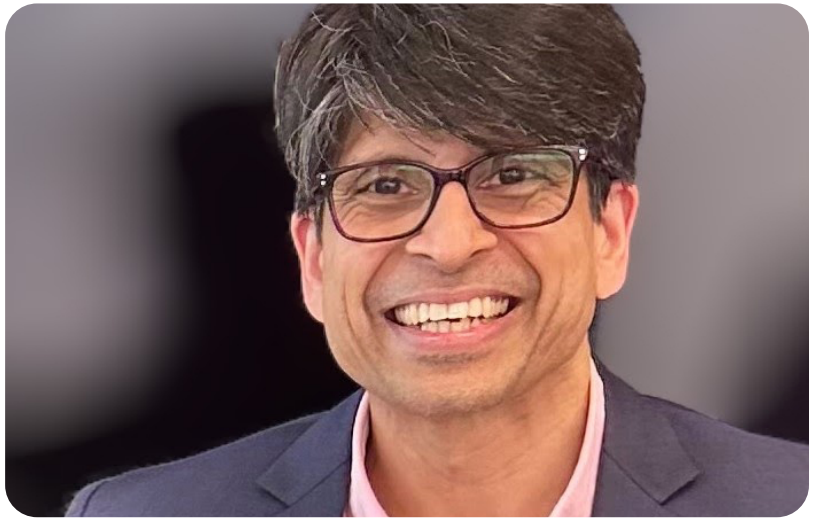
Today, as CTO of SGNL, Tulshibagwale continues to focus on Identity, motivated by his belief that authorization and access management are ripe for revolution. “I feel access management today is a bit of a Wild West, even though it is critical to security,” he says. SGNL helps companies de-risk by removing standing access privileges and replacing them with contextual, policy-driven access decisions so a lone Identity breach doesn’t trigger a massive crisis. “Enabling dynamic, continuous access management can mitigate the impact of Identity related breaches, which can still happen after passkeys are deployed,” he points out.

Looking ahead, Tulshibagwale is particularly excited by innovation in access security that can scale to global levels and doesn’t require manual steps to grant or deny access. But he believes changing threats and Identity needs will continue to bedevil the corporate world and that mere authentication is just the tip of the iceberg. In an article he wrote for Forbes earlier this year, Tulshibagwale laid out the division of duties that separates tech from policy. “It’s the CIO’s and CISO’s job to ensure authenticated users are only authorized to do what they’re meant to do once inside. The CEO and board are responsible for ensuring they do this effectively.”

IDENTITY 25 HONOREE

Pramod Varma

Former Chief Architect, Aadhaar



"It is essential that countries look at open source as a means to ensure the openness and sovereignty of national digital infrastructure."

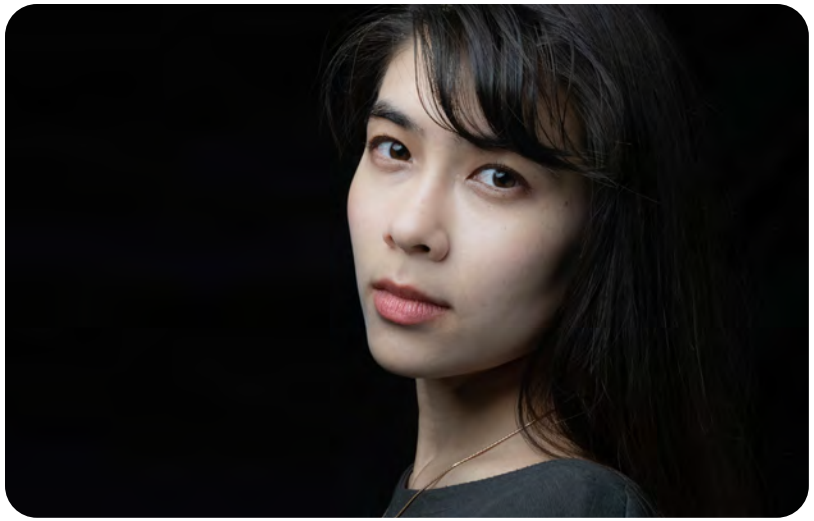
If anybody fears that deploying strong, biometric-backed Identity cards on a country-wide scale is an impossible dream, the example of Aadhaar should change their mind. This system, offering a 12-digit unique Identity number that can be obtained by all residents of India, is the world's largest biometric ID system, and it's a roaring success. Former Chief Economist of the World Bank and Nobel laureate Paul Romer reportedly called Aadhaar "the most sophisticated ID program in the world."

Pramod Varma was the chief architect of Aadhaar, which utilizes each ID holder's 10 fingerprints, along with iris scans and a facial photo, to assure that each unique ID number is assigned to exactly one Indian resident. Within seven years of Aadhaar's January 2009 launch, the initiative had scaled to approximately 1 billion people, and it currently covers 1.38 billion people who collectively use their cards around 2 billion times per month. An amazing success.

Varma laughs when asked about the challenges of creating secure, individual identities for the world's most populous country. "Challenges were plenty, including supporting 22 official languages, dealing with cultural variations, and rolling out across 600,000 villages," he recalls. There were marketing challenges, too. Varma says communicating the benefits of the system to his fellow citizens was a daunting hurdle, and teams had to account for extreme diversity and navigate fierce privacy debates. Despite the difficulties of deploying this system in a way that was secure, private, and effective at tremendous scale, Varma looks back warmly at the experience. "It was a privilege," he says, humbly.

Varma was also a key player in the development of India's digital health system, another enormous and important challenge. "India continues to lack key infrastructure for affordable primary and secondary care," he laments. It's a long-term project, and Varma is currently focused on simply laying the building blocks of an effective and efficient system, including verifiable electronic registries, an open commerce network using the decentralized Beckn Protocol, an interoperable and decentralized personal health records network, an interoperable open health services network, and an open data framework. "I expect that it will take a few more years to start seeing the impact of a unified interoperable digital backbone," he predicts.

Meanwhile, Varma continues to apply his talents to the development of critical tools, including digital signature protocol eSign, credentials system Digilocker, and interoperable instant payment infrastructure UPI. The key lesson he has learned, that he says he would share with anyone involved in trying to set up Identity at massive scale, is not to try boiling the ocean. "Keeping the system extremely minimal and simple — to do just one thing well — is the most important lesson for anyone trying to implement national ID systems," he advises.



IDENTITY 25 HONOREE

Kristina Yasuda

Identity Solution Architect, SPRIND, German Federal Agency of Disruptive Innovation

> “Decentralized Identity infrastructure unlocks access to education, healthcare, housing, employment, and freedom of movement.”

Kristina Yasuda’s efforts in the Identity space represent more than merely a career, more even than just her life’s work: This is a calling.

From the earliest days of her working life, Yasuda pursued projects that would impact lives, including a climate change initiative led by the United Nations, an effort to strategically drive attendance for the 2020 Tokyo Olympics and Paralympics, and a stint wrestling with legislative issues in DC on behalf of the Wildlife Conservation Society. As her technical skills in Identity security grew, so too did Yasuda’s interest in applying those skills to the public good.

“Having a functioning Identity system (either physical or digital) is truly a privilege and a game-changer that can unlock a lot of opportunities in people’s lives,” Yasuda says. She recalls a moment when she was working with refugees, slum dwellers, and single mothers in Bangladesh. “I found my passion — creating a world where everyone has equal access to opportunities. Digital Identity infrastructure is the key to unlocking access to education, healthcare, housing, employment, and freedom of movement.”

Working for NGOs like InternetBar.org Institute and IBO Zambia yielded significant wins for Yasuda and helped a lot of people. But her ability to affect change rose exponentially when she joined Microsoft nearly five years ago. Microsoft provides her with the resources to follow her passion, and the company’s commitment to decentralized Identity standards jibes with her own. Today, she’s excited about machine Identity and European Digital Identity wallet, work that she says has the potential to transform the lives of those residing in and visiting Europe.

Yasuda describes the world’s uneven progress towards decentralized Identity systems as the result of pursuing two simultaneous, parallel paths. “In the short term, there is a need to focus on ‘pragmatic’ standards that would allow building large, decentralized Identity ecosystems,” she says. “The work on more advanced concepts continues at the same time.”

There is an admirable humility in Yasuda’s approach. She deflected our questions about awards she has received from the likes of *Forbes* and MIT. “I think it leads to better standards when individuals’ comments in the working group are evaluated based on the technical merit, implementation experience and functional requirements as opposed to awards for past achievements,” she said.

But make no mistake: Yasuda is here to make change — and is sure to make her mark. “It would make me very proud if I would be able to say in the future that I contributed to secure, privacy-preserving, reliable, easy-to-use decentralized Identity systems that made the lives of the people better and richer.”

Where we go from here

Our Methodology

For the inaugural year of the Identity 25 initiative, Okta first assembled an all-star selection committee of Identity experts from across the field. This anonymous committee nominated a few dozen carefully considered candidates, including open source contributors, founders, IT specialists, technologists, academics, operators, and policy makers. They then met on multiple occasions to discuss the merits of potential candidates, ultimately winnowing down the broader list to just 25 selectees. Outreach to selectees included general and specific questions designed to elicit details to add depth to their bios and clarify their approaches to Identity. If you have someone you'd like to nominate for next year's Identity 25, please see the instructions at the lower right of this page.

The thought leaders, rebels, and agitators of this year's Identity 25 are clear-eyed about the future. Fraudsters armed with advanced AI and other powerful tools are going to test corporate and private security like never before, and governments and companies will find reasons — some good, some evil — to try peering into our private lives and personal data. It's not an exaggeration to say the promise of the future is balanced by a quickly growing hazard, with our companies, livelihoods, and basic human rights in the balance.

But we are not alone.

Identity heroes like the ones we've profiled here are on the case. With their dedication and expert guidance, we can continue strengthening digital Identity and stay one step ahead of hackers, overreaching governments and corporations, and other threats. And the future's in motion. Powered by ironclad Identity, enterprises can confidently scale up modern diverse and dispersed workforces. And consumers can safely transact online and off with digital credentials, knowing their private data is secure and in motion only according to their digital consent. We're making progress.

The Identity 25 is securing the unfolding digital world, and the next selectees are no doubt out there somewhere right now: building the tools of tomorrow, developing new standards, protecting digital freedom, and thwarting determined cybercriminals.

Thanks for joining us in a toast to these visionaries. See you in 2025!

Know an Identity pioneer you'd like to nominate for next year's Identity 25? Send your nomination, including a short paragraph describing why you think this nominee is deserving, to Identity25@okta.com on or before July 1, 2024. Include any relevant links to support your case. Okta's Identity 25 Selection Committee will consider your nomination and reach out by mail on or before October 1 informing you of their decision. Good luck!

okta Ventures

okta

About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.