2026

The Identity 25

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

okta

okta Ventures

Contents

Identity is the control plane

AI is quickly changing the rules for legitimate businesses, cybercriminals, workers, and consumers. As our digital lives continue to expand and evolve, securing identity has never been more important. Thankfully, a small army of heroically forward-thinking developers, strategists, standards-setters, business leaders, and other prominent figures dedicated to identity are there to guide and protect us.

The Okta Identity 25 was created to celebrate these often unsung stars of the identity space. Each year, we honor pioneers in all aspects of the field, from software creation to standards evolution to academic theory to strategic implementation. We're happy to present this year's honorees, whose tireless efforts continue to support us all by keeping digital transactions safe and simple, protecting privacy, empowering underserved populations, and a whole lot more.

The breathtakingly rapid expansion of our digital lives has introduced new levels of convenience and connection, while simultaneously unleashing a new generation of sophisticated security threats. In this dynamic and challenging environment, a select group of innovators, leaders, and visionaries are working to forge a sustainable future for digital identity.

This report celebrates 25 heroes helping us chart a path through this complex, ever-evolving landscape. Their work is more critical than ever as we confront these new challenges. The rise of agentic AI, for example, is flooding the Internet with non-human identities capable of executing complex tasks without direct human oversight. Authenticating these entities presents a fundamental challenge to our traditional models of access management.

Similarly, the proliferation of deepfake technology poses a significant threat to the integrity of all digital interactions. Highly realistic AI-generated forgeries of audio and video content can be used to undercut traditional identity controls, bypass biometric security systems, spread misinformation, and perpetrate fraud on an unprecedented scale. Deepfakes leverage our own identity security tools against us, and this already represents a critical front in the broader battle to secure and manage digital identity.

We are also witnessing a wave of innovation in how we authenticate legitimate humans at scale. Governments around the world are rolling out national digital ID cards and mobile-first identification systems, creating new opportunities for more seamless and secure access to a wide range of public and private services. From Estonia's pioneering e-Residency program to the European Union's ambitious new Digital Identity Wallet, these initiatives are laying the groundwork for a more interoperable and user-centric future for digital identity.

The 25 individuals profiled in this report are at the forefront of all these developments and more. They are the architects of new standards, the builders of innovative technologies, and the champions of a more secure and equitable digital world. Their stories are a testament to the power of human ingenuity to keep pace with rapid technological change. Join us in a celebration of these heroes of digital Identity, whose work will help shape our digital lives for years to come.

IDENTITY 25 HONOREE

Will Allen

Product, Snowflake Intelligence & Agents at Snowflake

“We all have work to do here to bring real value and clarity to users and merchants alike. What comes next is the exciting part.”

Will Allen, currently leading product for Snowflake Intelligence and Agents, told us recently about how his shopping habits have changed: All his customer journeys now begin with ChatGPT. “It has transformed how I think about purchasing anything,” he says. “A car, beef jerky, hiking poles…” But supercharging his own shopping is only the beginning: At Allen’s prior role at Cloudflare, he dove into the complexity that agentic commerce is sure to bring. “How can merchants set the rules on how agents browse inventory?” he wonders. “Which agents can then go on to actually make a purchase, and how can they do so autonomously but with oversight? How do you elevate your brand and the personal connection to your customer if the purchases are made by an agent?”

He helped Cloudflare extend Web Bot Auth, a new way to cryptographically authenticate agent traffic, into agentic commerce by integrating it with Visa’s Trusted Agent Protocol and Mastercard’s Agent Pay to help merchants. “First, merchants can identify an agent and distinguish whether a particular interaction is intended to browse or to pay,” Allen explains. “Next, merchants can link an agent to a consumer identity and indicate to agents how a payment is expected.” Allen says that identifying trusted interactions and increasing security gives merchants new tools to defend their brands, protect their customers, and grow trust. As agents continue to interact with the broader Internet, proposed standards like Web Bot Auth are foundational.

This former philosophy major has always been keen to understand how we know things, and that curiosity informs his new role in helping to build Snowflake Intelligence and their agent platform. “When you are interacting with agents across your enterprise, your identity is critical: knowing who you are and what data you can have access to shapes and transforms that interaction. It’s one of the areas I find so impactful about building agents on Snowflake: you get access to both the data and the governance that is so critical to running any business.”

As the COO at Behance (which he describes as “like LinkedIn for creatives”), Allen became passionate about empowering designers, photographers, artists, and architects not only to do their best work but also to retain attribution for it, and even to find more opportunities.

When Adobe acquired Behance, Allen continued to pursue that passion by launching the Content Authenticity Initiative (CAI) and helping to set up the Coalition for Content Provenance and Authenticity (C2PA). These initiatives answer questions like where a particular image came from and how it’s changed, by making content’s provenance a permanent part of its metadata. Every image generated by ChatGPT now, for example, has its provenance baked in.

Storing a record of content manipulation isn’t a value judgment, Allen’s quick to point out. “It isn’t about saying AI-generated content is good or bad, or that any edits are malicious,” he clarifies. “But thanks to the work of the C2PA, there is now a path to a shared understanding of what actually happened.”

IDENTITY 25 HONOREE

Dr Joseph Atick

Executive Chairman at ID4Africa

> “ID4Africa lets people say, ‘I count, because I have Identity that everybody recognizes. I can own my home, my business. I can assert my rights.’”

In a career that spans four decades, Dr Joseph Atick has been an academic, discovering algorithms fundamental to the biometrics industry. He has been an inventor, creating the world’s first commercially viable face recognition technology and introducing the concept of biometric passports. He has been a company founder several times over. But with all of these feats under his belt, Atick calls ID4Africa his greatest source of pride.

More than a decade ago, Atick co-founded the movement, driving digital identity transformation across this enormous, diverse continent. Among ID4Africa’s achievements: creating over 500 million digital identities for people who were previously invisible. “ID4Africa allows people to say, ‘I count, because I now have identity that everybody recognizes,’” he says proudly. “‘I can open up a bank account. I can own my home, my land, my business. I can assert my rights.’”

Atick retired from a successful business career in 2010 in order to devote his time and talents to promoting identity in the developing world. His initial forays into public service included world-class identity projects like India’s Aadhaar, and he recognized a broader opportunity than merely enrolling millions safely. Atick saw that digital identity could be a fundamental pillar for development, and he invited World Bank officials to think of identity as a worthy investment opportunity like roads, highways, and digital infrastructure. And he convinced them, resulting in the launch of the Identification for Development (ID4D) initiative. “My co-founders and I were convinced that if everybody had an identity that was robust and inexpensive, it would stimulate the economic and social development of countries,” Atick says. To date, ID4D has invested over $3 billion in digital identity and continues to see powerful returns.

But Atick wanted still more. To really drive change at scale, he needed the flexibility and speed of a startup—impossible within the World Bank’s structure. So, in 2014, he and two colleagues founded ID4Africa and embraced a new approach. “People will tell you that the genius of ID4Africa has been the adoption of the most successful governance model,” he says. “We motivated countries to take matters into their own hands.” Rather than trying to impose grand but unworkable visions across dozens of disparate countries and cultures, ID4Africa encouraged local officials to create and implement systems to meet their own citizens’ particular needs, supported and informed by the expertise and successes of the 48 member states. “Unlike the U.N. agencies, where the thinking comes from headquarters, ID4Africa thinking comes from the field,” says Atick. ID4Africa has become a platform for knowledge exchange, attracting expert thought leaders and suppliers. He expects that in the next three to five years, the number of “invisible people” in Africa without digital identity will approach zero.

Atick expresses a lot of gratitude for this opportunity, and is delighted that his innovations are simplifying people’s lives and making this very large corner of the world ever more secure and more connected.

IDENTITY 25 HONOREE

Christopher Bramwell

Chief Privacy Officer, State of Utah

> The individual controls their identity. The state's role is only to endorse it and to ensure the individual has mechanisms to protect it."

Christopher Bramwell is building a system that puts control back in people's hands. As Utah's first Chief Privacy Officer and Director of the Utah Office of Data Privacy (appointed by Governor Cox), Bramwell pursues a disruptive premise: To be durable, digital identity must be anchored in individual control, not convenience, and shielded from institutional capture. "Identity is the keystone," he says. "Without solving that, we cannot meaningfully solve privacy."

The model Bramwell helped design – called State-Endorsed Digital Identity (SEDI) and enshrined in law as Utah's SB275 – inverts the conventional relationship between people and institutions. Individuals create and hold their own cryptographic identifiers; the government is an endorser, not an owner, and tracking is prohibited. "This is not just a new credential or app," he says. "It is a fundamentally different approach to identity." Shifting power from institutional issuers to the people they serve can begin to reverse decades of data governance noncompliance, he believes. Utah's Government Data Privacy Act, the most comprehensive U.S. state government data privacy law (also architected by Bramwell), requires new systems to immediately comply, and sets a realistic course for legacy infrastructure, shifting the conversation from blame to progress.

Bramwell's vision is to let individuals own their digital identity through cryptographic key control, with the state endorsing individual key control at time of identity proofing. The SEDI program is evaluating recently approved specs out of the Linux Foundation's decentralized trust projects that facilitate decentralized key management with unique capabilities that suit SEDI's perpetual digital identity approach.

Bramwell has drawn a hard line against centralized national identity systems, citing political risks and cybersecurity exposure. Instead, he wants to preserve anonymity and pseudonymity, rejecting proposals that would require full identity disclosure to access online platforms. In his view, privacy shouldn't be approached as a compliance overlay; it should instead be organized around comprehensive data governance, verifiable data and identity, and automation. "We reframed privacy as the innovation to move forward responsibly and restore public trust," he explains. "The goal was not to build the most restrictive system – it was to build a durable one." A system that treats individual dignity and self-determination as engineering requirements, not just principles.

Bramwell is active in the Internet Identity Workshop and increasingly engaged with the Better Identity Coalition and the ACLU on digital identity and privacy issues. His core belief: durable identity infrastructure requires technologies, civil liberties advocates, policymakers, and a multistate consortium of implementers working in concert to accelerate adoption. "Start with structure, not slogans," he advises. "Acknowledge where gaps exist, and treat identity and data governance as foundational infrastructure." The ten-year horizon Bramwell is focused on isn't a projection: It's a design brief that Utah is already working toward to restore verifiable trust in government.

IDENTITY 25 HONOREE

Joni Brennan

President, Digital ID & Authentication Council of Canada

> Watching competitors become collaborators around shared trust principles fundamentally changed what's possible in our market."

Joni Brennan, President of the Digital ID & Authentication Council of Canada (DIACC), is humble about her gamechanging role in the Identity world. "Early in my career, I assumed technical standards would drive adoption: If we build the best specifications, implementation follows," she says. "That was naive." But Brennan's experience ultimately produced a sophisticated understanding of organizations that has helped her make progress even when stakeholders are reluctant. "They don't adopt digital trust because the cryptography is elegant," she says, "they adopt it because someone helped them understand how it solves their specific business problem."

Brennan points to the DIACC's role in developing the Pan-Canadian Trust Framework as one of her proudest achievements. The framework has evolved from a collection of documents to the basis for interoperable digital trust and verification across the Canadian economy. "Watching competitors become collaborators around shared trust principles fundamentally changed what's possible in our market," she says. The success of the project is the culmination of lessons Brennan says she learned over two decades. "Technical excellence matters, and ecosystem design and stakeholder alignment determine whether frameworks grow value."

The Pan-Canadian Trust Framework certifies identity verification across Canada. But it's not just about convenience: The framework simplifies access for the millions of rural Canadians who can't easily appear at urban offices. "What used to require in-person meetings, physical document review, and repeated identity checks can now happen with verified digital credentials," she says. Lawyers, lenders, and others benefit from streamlined processes that enable trustworthy verification while increasing individuals' control over their own information.

Brennan's Canadian experience is valued at global forums, where dialog often assumes European- or US-focused models. One-size-fits-all solutions won't work in Canada, as she points out, where provinces are governed by disparate regulatory regimes, indigenous peoples have sovereignty, and bilingual populations are the norm. "Our governance model demands interoperability across jurisdictions while respecting autonomy," she says. "I bring the perspective that digital trust and verification infrastructure must work across quite different constitutional and cultural contexts."

Brennan cites individuals' limited ability to control their own data as a key reason that the public remains skeptical about organizations' commitment to protecting data. "Too many still treat digital identity as an operational compliance checkbox rather than as a strategic differentiator that protects and empowers," she says.

Still, thanks in part to her work, Brennan sees evidence that a shift is underway. "We're finally seeing digital trust and identity verification move from 'nice to have' to necessary trust infrastructure," she asserts. "That excites me."

IDENTITY 25 HONOREE

Lee Campbell

Identity and Authentication Lead, Android Platform at Google

"It often doesn't matter how secure or brilliant a specification is. If it adds user friction, it's a non-starter."

Lee Campbell operates at an intersection where massive scale meets individual user experience. His decisions impact billions of users – yet success sometimes comes down to whether a single person can easily sign into their account. As the engineering lead for Identity and Authentication on the Android platform at Google, Campbell designs the user and developer-facing APIs that power authentication and identity management across Android's entire ecosystem of devices, including televisions and cars.

It's a role that requires both a global view of the evolving needs of users and a microscopic attention to detail, and Campbell consistently delivers both. His most impactful contribution to date has been shepherding passkeys from a niche concept into broad adoption by nearly all major app and web developers. "Not only are we saving users from the real world pain that comes with account compromises, but our developers are seeing sign-in success rates shoot up, which means monetization goes up and SMS costs go down too."

Campbell's influence extends far beyond Google's walls. He's deeply embedded in the standards bodies shaping identity's future: co-chairing the Digital Credentials Working Group and the Agentic SIG, while also remaining deeply involved in the FIDO Alliance's development of passkeys and their use in payments. His pragmatic approach to standards work reflects his commitment to building technologies that function in the real world at scale.

"Traditionally, standards bodies write specs – they don't build user-facing products," he notes. "So if we wanted to design for everyone and bring phishing-resistant auth to billions of people, we needed a fundamental shift." That shift proved to be essential, as FIDO technology moved from strictly device-bound keys to syncable passkeys, introducing a more globally mainstream product.

Looking ahead, Campbell sees enormous potential in substantially disruptive changes emerging from both the public and private sectors. National governments around the world are rolling out digital IDs, with the European Union's eIDAS 2.0 regulation requiring all 27 EU states to provide digital national IDs by late 2026. "If we get it right, this change will be a huge win for security and privacy, and it will unlock a whole world of new use-cases for our users," he says. Private entities will be able to leverage internationally standardized APIs to issue any manner of credential, from employee badges to gym memberships.

Campbell's belief is that successful authentication technologies must prioritize user experience above all else. "Groups with the most success are formed of people wanting to ship real world products and considering everything that entails, not just focusing on the bits on wire," he says. It's a philosophy that keeps Campbell grounded as he contributes to the future of digital identity for billions of people around the world.

IDENTITY 25 HONOREE

Eva Casey-Velasquez

CEO, Identity Theft Resource Center

> “The bridge is built when we make it clear that robust, empathetic victim support is not a luxury or secondary concern...it’s a necessity.”

Eva Velasquez has spent decades fighting scams and fraud, with a particular focus on protecting people and helping victims restore their lives. For the past 13 years, she has headed up the Identity Theft Resource Center, a national nonprofit that provides free victim assistance, publishes research, and develops strategies and tactics to reduce risk and help people recover from identity crimes. At the ITRC, Velasquez and her team have successfully promoted a deeper understanding that identity crimes are personal violations that demand the same attention as violent crimes. “By making this shift,” she says, “we’ve helped almost a million people get back on their feet in 2023 and 2024. That’s real impact.” Indeed.

In particular, Velasquez would like to upend society’s tendency to shame and blame identity theft victims. “Unfortunately, we still make people feel dumb or lazy for not keeping up with tech that changes every five minutes,” she says, noting that industry and government, for their part, have made inadequate investments in education and recovery. She is encouraged by the trend towards biometrics as a way to diminish the value of stolen, static data. “A genuine commitment to human-centered security design,” she says, “inherently works with human nature, eliminating the need for complex, easily forgotten credentials to create systems that work with basic human behavior instead of against it.”

Before taking the helm at the ITRC, Velasquez spent 21 years protecting consumers and advocating for victims at the San Diego District Attorney’s office. “My job used to be to get the bad guys,” she says. “I learned firsthand how few resources we actually had for victims.” On learning that the ITRC was looking for new leadership, she saw the opportunity to empower and support identity theft victims. “People needed more. We needed to stop being so dismissive of this victim population.”

Velasquez is passionate about the need to attend not only to the nuts-and-bolts of identity theft prevention and recovery, but also to the emotional burden these crimes create. She describes the empowerment that her ITRC teams provide as practical, tactical “expertise in action” that gives victims the tools they need to rebuild. But in her mind, it’s not just about empowering victims – it’s also about emotionally supporting them. “ITRC offers the simple, profound act of bearing witness to someone’s struggle,” she says. “It’s our team’s training in compassion – our ability to listen, to validate, and to say ‘I am here with you. You are not alone.’”

Velazquez’s broad experience in law enforcement, in industry (she worked for several years at the Better Business Bureau) and on behalf of victims informs her complex and thoughtful views on effective identity protection. Narrowing the gaps among government, industry, and the public requires clear language, shared goals, and an acknowledgement of basic human behavior. “The bridge is built when we make it clear that robust, empathetic victim support is not a luxury or secondary concern,” she explains. “It’s a necessity.”

IDENTITY 25 HONOREE

Sarah Clark

Chief Product Officer and GM North America at Hopae

> “You have to be doing work that meets the needs of your customers. But there’s also something to be said for advocating for the next big thing.”

Sarah Clark, Chief Product Officer and GM North America at Hopae, has been a leader in identity for over a decade, but she points to a time early in her career at an Internet ad-service startup as especially formative. “It seems so crazy to think that, back then, it was an uphill battle to convince advertisers to try something out called targeted ad serving,” she recalls. “That’s when I learned that I love product and how to really create a blue ocean with something that was unknown to the market.”

Clark’s identity journey began more than a dozen years ago when she approached the board of directors at Mitek, which at the time focused primarily on remote check deposits and bill payments. Her idea: expanding into digital identity proofing. “It was a good fit for our existing computer vision-based platform,” she recalls. “We were one of the early innovators in DocAuth,” enabling the camera on a smartphone to capture an image of a physical government-issued ID, for example. “Pairing the authenticated image with a selfie biometric and liveness was groundbreaking at the time,” she says, though it has now become routine (and targeted, instead, by opportunistic fraudsters leveraging AI).

“The only way to truly be sure of an individual’s foundational identity at the first interaction,” for example an account opening, “is to have access to ‘root of trust’ credentials like a government-issued ID,” says Clark. “And that assertion needs to be bound to a biometric with strong liveness that can be used seamlessly for ongoing authentication.” She explains that typical interactions were vulnerable, historically, because tokenization was only partial. “We carry tokenized payment instruments in payment wallets, but until recently most of us carried physical identity cards in physical wallets,” she points out. But the future is here. “When identity is tokenized, owned, and shared explicitly by the individual, it can operate seamlessly with tokenized payments.”

Clark is encouraged by the changes regulators are driving. She points to the European Digital Identity Wallet as the kind of initiative that benefits both citizens and industry. This year, each member state will provide at least one wallet to any EU citizen, resident or business who wants it; by next year, all regulated industries and very large online platforms will be required to accept them. The fact that each of the EU’s 27 member states will have its own wallet will create fragmentation, but Clark says that her Hopae is focused on meeting this challenge. “Hopae is on track to become the first QTSP-accredited intermediary in the EU”, she says. Her focus is ensuring Hopae maintains the largest global coverage of eIDs, throughout EMEA, Asia, Latam and North America.

Clark’s success comes in part from an ability to give people what they want while also imagining what they need. “You have to be doing work that meets the needs of your customers,” she says, “but there’s also something to be said for advocating for the next big thing. A good product manager threads that needle.”

IDENTITY 25 HONOREE

Den Delimarsky

Member of Technical Staff at Anthropic

> "I am really excited about emerging standards that showcase how it's possible to move quickly with the evolution of the identity field."

Den Delimarsky, Principal Product Engineer at Microsoft, is like a programmer version of Steph Curry: He elevates his teammates' performances. "I help build developer tools and AI-powered experiences that make engineers more productive," he says. Delimarsky has been working in the security and identity space for the past three years, long enough to know that there is little overlap between security and development expertise. "Most developers do not want to be security experts," he says, "and they don't need to be."

Delimarsky's role as product management tech lead for Microsoft's Authentication Libraries gave him a solid foundation in authentication and authorization, allowing him to move into CoreAI, where he focused on identity-related issues on products like GitHub and Visual Studio. That led to prominent, interesting roles like Steering Committee Core Maintainer working on the Model Context Protocol (MCP). "Strengthening the protocol while providing good developer ergonomics for authorization is one of my proudest moments," he says. "It took a lot of collaboration across companies and required listening to community and developer needs."

Delimarsky is excited by the project, whose goals include eliminating the need for developers to build security systems by clearing the way to using established identity providers (IdP) rather than writing their own OAuth provider from scratch. The current MCP authorization specification requires work that would be unnecessary, he contends, if there were a robust authorization infrastructure in place. Lifting this burden from development will improve security and speed.

"When I first started in the security space, it struck me how slowly things moved," he says. AI turbocharged the pace of change, he said, driving the need for an accelerated path for identity standards. Delimarsky says that in addition to new standards, folks in the community need to coalesce around processes and approaches to identity that allow quick iteration while preserving rigor and deepening trust.

Delimarsky delights in making the complex seem simple. His exuberant explanation of flexible federated identity credentials: "I love this concept! I can eliminate a whole class of vulnerabilities from secret leakage by eliminating secrets altogether." The fundamental idea of flexible federated ID, he explains, is finding a way to automate the establishment of trust between two identity systems. "I can have GitHub Actions, for example, mint a hypothetical ID badge and then use that to pass to my cloud provider to access some hosted resources," he explains. "I am completely hands-off in terms of handling any keys. There are two identity systems that just share secure artifacts with each other." Delimarsky acknowledges there are challenges and limitations, but remains confident that progress is at hand. "I have high hopes for universally-accepted workload identity standards that will help move the needle in the right direction," he says.

IDENTITY 25 HONOREE

Greg Fair

Digital Identity Chief, State of California

> “The first question of the innovator is to see what is possible. But in practice, we must consider how technologies will be received by the people who use them.”

For Greg Fair, identity has never been a purely technical problem: It’s a human one. As California’s Digital Identity Chief, he launched a first-of-its-kind privacy-preserving digital identity framework, providing secure, equitable access to state services for millions of Californians. Before that, he spent nearly a decade at Google, ultimately leading the Privacy and Data Protection Office’s product management team. There, he oversaw privacy strategy for sweeping global regulatory efforts, including GDPR. His career has also spanned science education and the arts, a breadth of experience that has given him an uncommon lens on what technology actually owes the people it serves.

“Any technology is only successful if it is human-centric,” he says. “The first question of the innovator is of course to see what is possible. But when put into practice, we must consider how technologies will be received and applied by the people who use them.” He’s returned repeatedly to this principle, for example when navigating GDPR’s rollout, reconciling competing interests, institutional pressures, and real-world user needs.

Fair counts the co-founding of the Data Transfer Project as one of his proudest achievements. The audacious idea was to persuade rivals like Google, Microsoft, Meta, and Apple to build a common, open-source framework for data portability. Many in both the private and public sectors saw it as a zero-sum game: Surely data portability meant enabling users to simply leave one platform for another? “Once the conversation was reframed around the shared goal of user control,” Fair reflects, “and people recognized the new kinds of experiences a shared data portability ecosystem could support, the conversations became incredibly collaborative and the technical challenges somehow seemed much more tractable.” The project proved that a web where users own their data wasn’t an idealist’s vision – it was simply an engineering problem to be solved.

That instinct, to find common ground around shared goals, shapes everything Fair does. Through his advisory work with international governing bodies, he’s observed that trust is a deeply localized phenomenon, varying across cultures and institutions. Still, one constant stands out: “Governments will always hold a unique role in the trust ecosystem to ensure that all people can access services safely and equitably,” he asserts, adding: “whether those use cases make business sense or not.” It’s driven his work in California and continues to shape how he thinks about identity infrastructure at scale.

Looking ahead, Fair is focused on what he sees as the next inflection point: the convergence of verifiable credentials and AI. Together, he believes they will give end users direct agency over their identities and data, bypassing the intermediaries that currently slow service delivery for individuals. But he’s clear-eyed about the responsibility that comes with this potential. Balancing open, interoperable standards against making room for innovation remains a challenge. “The best, accessible, safest products will win out,” he says confidently...provided the industry stays focused on building the right foundations now.

IDENTITY 25 HONOREE

Devin Fensterheim

Executive Advisor at Social Security Administration

> "Today, sophisticated threats introduce new demands: to operate in an agile manner, remain robust, and adopt modern techologies."

Devin Fensterheim leads the digital identity program for the U.S. Social Security Administration, a role with enormous impact and complexity. Each month the SSA distributes approximately $130 billion to over 70 million beneficiaries, working with public- and private-sector partners to provide secure access to more than 100 million digital users. These include retirees, people receiving critical needs-based assistance, the attorneys and medical professionals assisting claimants, and many others.

Proving the identity of many of the beneficiaries of SSA programs is challenging, because they lack the financial records and credit history that are the traditional bases of verification. When Fensterheim first began government work focusing on identity and fraud fifteen years ago, knowledge-based verification was adequate to create an account. "Today, sophisticated threats from all manner of adversaries, armed with AI and deepfake capabilities, introduce new demands to operate in an agile manner, remain robust to emerging threats, and adopt modern technologies," he says.

Fensterheim is dismayed that so many in the identity space continue to use social security numbers as authentication secrets – a miscalculation that fraudsters can exploit. When FDR ordered that the SSN become central to records systems of the United States, there were obvious advantages in establishing an identifier that an individual would acquire at birth and hold over a lifetime. The idea was sound 80 years ago, but as the information age dawned many organizations began using the SSN as a convenient secret, entrenching a vulnerability that exists to this day. "The persistence and immutability of the SSN that make it indispensable in our national identity infrastructure also necessitate that it be disclosed over a person's lifetime innumerable times," Fensterheim laments. "That universality is simply not compatible with the concept of the SSN as a confidential, unchangeable password that is known only to the holder."

The SSN was never really suitable as an authentication secret, he says, and its usefulness to fraudsters will evaporate only when legitimate organizations stop using its knowledge as evidence of identity.

Fensterheim says mobile driver's licenses (mDLs) are well-positioned to become the gold standard for online identity proof. "Millions of people have mDLs," he says, "but the opportunity to use them remains largely limited to TSA checkpoints and law enforcement encounters." He says that the effectiveness of mDLs in these limited scenarios creates momentum that should prompt leaders to develop and accept more digital proofs.

Fensterheim continues to be energized by the challenges of the identity space. "You must use available intelligence together with observed patterns to predict your adversaries' next move, just as they are predicting yours," he says. But through it all, he stays focused on improving his fellow citizens' lives. "The impact is immediately measurable, not only in dollars saved, but in preventing harm to people who would otherwise be victims of fraud."

Devin Fensterheim's remarks are his own and do not necessarily reflect the views, policies, and positions of the Social Security Administration or U.S. Government.

IDENTITY 25 HONOREE

Tariq Malik

Technical Advisor, Digital Public Infrastructure at The World Bank

> “Digital identity succeeds or fails not based on technology, but based on whether its governance can withstand political pressure.”

Tariq Malik’s career has taken him all over the world, from Michigan to Madagascar. He has spent 25 years advising governments and multilateral institutions building digital ID and civil registration systems that drive social protection and economic growth. And when assembling the elements of digital public infrastructure, he says, the pressure is on. “Expectations are often high, and institutions are often under strain, but the promise is always the same,” he says: “Efficiency, inclusion, and better service delivery.”

During Malik’s long stint as Chief Technical Advisor at the United Nations Development Program (UNDP), he led a team of 4,500 registration officers that completed universal registration of adults in Malawi in 180 days. Earlier, he worked at Pakistan’s National Database and Registration Authority (NADRA), spearheading one of the world’s largest biometric registration efforts. NADRA enrolled over 145 million of his fellow citizens, then used digital ID to create social programs to empower women, protect internally displaced persons, combat corruption, and reduce poverty.

Malik is encouraged by the movement away from passwords. “Passkeys in particular are eliminating passwords at scale,” he says, “while standards-based verifiable credentials enable selective disclosure of cryptographic claims rather than wholesale data sharing.” He predicts that the sea change will come when machine-readable rules, consent, and policy enforcement are embedded in identity flows. “The technology is largely ready,” he says. “The real bottleneck now is institutional capacity to operationalize governance digitally.”

Malik’s success driving adoption and enrollment highlights a growing concern for those at risk of being left behind. A recent report from the Institute of Development Studies, “Biometric Digital-ID in Africa: Progress and Challenges to Date,” found that biometric ID systems can exclude millions from government services and the rights of citizenship when digital identity systems become mandatory. Malik believes that those who choose to opt out of such programs have well-founded fears. “They fear misuse of their data, lack confidence in redress mechanisms, and sense that power is exercised without accountability.”

Malik contends that implementation of digital public infrastructure (DPI) needs to focus on cultivating trust, not forcing compliance. In order for DPI efforts to succeed, “they must be pre-conditioned on civil liberties, not merely accompanied by them.” Such systems must feature three things, he says: strong legal and institutional safeguards aligned with international human rights norms, meaningful oversight and accountability mechanisms, and privacy-by-design approaches that include consent management, purpose limitation, and clear pathways for redress or opting-out.

Malik sees parallels between identity system implementation and good government generally. “Adoption ultimately follows not sophistication, but predictable governance, visible safeguards, and systems that reinforce citizen agency.”

IDENTITY 25 HONOREE

Lara Mossler

Head of Platforms & Product, Security at Airbnb

> Our entire identity infrastructure was built on the assumption that a human is on the other end. That assumption is about to break."

For Lara Mossler, Head of Platforms & Product, Security at Airbnb, identity isn't just infrastructure: It's the central nervous system of the modern organization. As a leader in a discipline that has enjoyed increasing recognition as the responsibilities and impact of identity professionals have grown, Mossler maintains that great work in this space should be nearly invisible. "Security should be felt as trust," she says, "not friction."

Mossler's journey began at Capital One, where she built identity and authentication infrastructure for one of America's largest financial institutions. "That work gave me deep foundations in how identity systems operate at scale," she explains: "the fraud vectors, the regulatory pressures, and the very real tension between security and usability that defines this field." At Airbnb, she built an authorization platform that governs access control across the entire organization, shifting the company from fragmented, team-by-team access logic to a centralized, policy-driven platform.

Mossler's approach to leadership is varied and unconventional, including training in neurofeedback, certification as a death doula, and education at a Swiss finishing school, an unusual toolkit for mentorship. "Peak performance comes from regulation, not just ambition," she says. "Most of the people I mentor don't lack talent or ideas: They lack the ability to stay grounded when the stakes feel high." She works with mentees on their strategies and their nervous systems, helping build tolerance for discomfort and an ability to sit with ambiguity long enough for the right answer to emerge.

Supporting diverse teams has long been a strength of Mossler's, and her broad technical range affords her the ability to negotiate minute details while keeping focus on the big picture. She's worked across NFC authentication, machine learning for fraud detection, authorization platforms, and AI agent architectures, and often acts in the role of translator as well as leader. Looking ahead, Mossler is focused on what she believes is the next frontier: machine identity and authorization for AI agents. "We're entering an era where AI agents will act on behalf of humans: booking travel, managing workflows, executing transactions. And our entire identity infrastructure was built on the assumption that a human is on the other end. That assumption is about to break," she warns. Watching the evolution of protocols like MCP (Model Context Protocol) closely is inspiring her to build in this space herself. "The identity industry needs to move from 'who is this person?' to 'who is this agent, who authorized it, what can it do, and how do we revoke that authority in real time?'"

Mossler is thrilled that identity is being recognized as the critical control plane for AI governance and organizational trust. But she worries that too much of the industry is thinking incrementally, bolting AI onto legacy paradigms rather than rethinking identity from first principles. "Whoever controls agent identity controls AI's blast radius," she observes. "That's an enormous responsibility, and I hope the industry rises to meet it with the seriousness it demands."

IDENTITY 25 HONOREE

Nicole Perlroth

Founding Partner, Silver Buckshot Ventures
and Venture Partner, Ballistic Ventures

“I covered the most consequential decade for cyberattacks in history. That convinced me it was time to put down the pen and pick up a shovel.”

“May you live in interesting times” is an often repeated ironic blessing supposed to be based on an ancient curse. Longtime venture partner Nicole Perlroth would no doubt agree that those working in the identity space today do live in interesting, troubled times, thanks in part to the malicious efforts of hackers around the world, including military and government hackers from rogue nation states like China.

Perlroth’s podcast, “To Catch a Thief: China’s Rise to Cyber Supremacy,” is a 9-part documentary that tracks that country’s state-sponsored digital criminals from “the most polite, mediocre hackers in cyberspace” to the “apex predator” that threatens America’s very infrastructure. Perlroth’s gift for storytelling (she is software company Rubrik’s Chief Cyber Raconteur) has landed her three Signal Awards so far, including Best Documentary Podcast.

Perlroth’s time as a technology, cybersecurity, and digital espionage reporter for *The New York Times* was, by her estimation, “the most consequential decade for cyberattacks in history.” She began shortly after the discovery of the malicious Stuxnet worm and left after the 2020 Russian cyberattack that victimized major organizations worldwide including the United States government, NATO, Microsoft, and at least 200 others. Those events bookended a stretch of investigations that “rooted out thousands of cyberattacks and helped compel the first U.S. hacking charges against the Chinese military and the blacklisting of Israel’s NSO Group.”

Shortly after the 2020 election, Perlroth asked herself: “Did I want to keep writing about this problem, or did I want to see if I could help solve it?” She was motivated by the realization that the attacks were worsening, that the targets (our infrastructure)were becoming more critical, and that the barriers to attacks were falling. So she left the newspaper and joined the Department of Homeland Security’s Cybersecurity Advisory Committee and the Council on Foreign Relations’ Cyber Task Force.

Simultaneously, Perlroth began advising startups and quietly assembled what she calls a cyber moonshot fund, Silver Buckshot Ventures. The name, she explains, speaks to the reality that “there is no silver bullet in cybersecurity. What we need is buckshot: targeted solutions aimed at the root causes.” She encourages clients and investors to consider three questions:

1. Will this meaningfully reduce our digital attack surface?
2. Is this team uniquely equipped to drive real adoption—not just invention?
3. One day, when the history of cybersecurity is written, will this mark a chapter?

Earlier this year, one-third of Silver Buckshot Ventures’ portfolio companies appeared among the 30 most promising cybersecurity companies by Notable Capital’s panel of CISOs. Her choice to add advisor and investor to her resume – to “pick up a shovel,” as she puts it – seems to be paying off.

IDENTITY 25 HONOREE

Anna Pobletts

Head of Passwordless at 1Password

The idea that logging in can be better than the current, friction-filled process is something that everyone can—and should—get behind."

"I think a truly passwordless future is inevitable," says Anna Pobletts, Head of Passwordless at 1Password, a global leader in identity security. Her confidence stems from an understanding that the challenges of logging into websites and apps are universally loathed and relatable – and therefore are doomed. "The idea that logging in can be better than the current, friction-filled process," she says, "is something that everyone can, and *should*, get behind."

Pobletts was a founder and the CTO at Passage, the Texas startup where she and co-founder Cole Hecht saw passkeys as a technology that offered, for the first time, both enhanced security and a more seamless UX than passwords. "We saw that passkeys are a big leap forward to more modern authentication that is human-centric and moves the state of security forward," she recalls. Pobletts and Hecht were obviously onto something, racing from founding in 2021 to $4 million in funding in 2022 to acquisition by 1Password later that year. The acquisition let her put all that startup stress behind her so she could refocus on leading engineering teams. "I'm most passionate about building solutions that solve problems for people," she says.

Pobletts' entrepreneurial success provided just one of many experiences informing her vision. "I've worked in security and identity from many different perspectives, including government, consulting, product companies, and standards," she recalls. And she has seen plenty of cool technology that fails because it doesn't help people in their daily lives, saying: "Solutions must work for the human behind the computer."

Pobletts sees a good fit between 1Password's evolving approach to authentication and the impact of AI agents, which are forcing a reconsideration of how we authenticate humans as well as non-humans. "AI agents are taking real action in the browser on behalf of users: filling forms, triggering workflows, and interacting with business systems," she explains. "Traditional security models break down when credentials get hard-coded." Part of the solution, says Pobletts, is to enable agentic workflows without revealing secrets to those agents. Techniques like just-in-time credential delivery, human-in-the-loop approval, and robust encryption can prevent the spilling of secrets. "Treating AI agents as identities subject to governance, oversight, and least privilege," she says, "has real potential to strengthen both security and usability across the identity ecosystem."

Pobletts remains fascinated by the human side of authentication, and recalls testing a simple, gorgeous passkey-only flow. "One participant – a non-technical user – did everything right, process-wise," she recalls. "But when he landed in the app, his feedback was that it couldn't possibly be secure, because it was too easy. It's the kind of feedback we've seen before," says Pobletts.

Authentication has to be strong enough to work and believable enough to be trusted by end users so it has a chance at wide adoption. This 'just right' zone is somewhere between too hard (i.e., intrusive) and too soft (i.e., suspiciously easy). And Pobletts remains dedicated to finding that sweet spot.

IDENTITY 25 HONOREE

Boonsun Prasitsumrit

CEO, National Digital ID Company, Ltd

"The focus should not be on explaining what digital identity is, but on enabling practical applications that fit naturally into people's daily lives."

Boonsun Prasitumrit has spent seven years as the CEO of Thailand's National Digital ID Company (NDID). Unlike peer countries trying to establish national digital identity from scratch, Thailand already had a national ID program, with a physical credential featuring a smart chip in the hands of nearly all the country's 70 million citizens. But because of a lack of clarity on standards for how to use the data on the chip, the national ID was seldom used for useful things like account opening or accessing government services. "A decade ago, the concept of digital identity was still widely misunderstood," explains Boonsun.

Rather than tweaking the existing ID or clarifying standards, the Thai government established the NDID. The task for this public-private partnership: creating a trusted, convenient, and efficient ecosystem to advance Thailand's digital economy and participation in the global economy. Boonsun says that the 200+ stakeholders who collaborated in the initiative coalesced around a key principle: "A national digital identity system must not have a single point of failure or a single point of risk. If identity infrastructure fails, the impact affects the entire country." This understanding drove the adoption of a decentralized model that would be better suited to resist cyberattacks, minimizing institutional risk. "The federated identity trust model we chose leverages the scalability, reliability, and customer-centric capabilities of existing institutions," Boonsun explains.

So how does it work? NDID doesn't store PII. Rather, it serves as a neutral trust director, maintaining blockchain-based transaction logs on a distributed ledger accessible by relying parties, identity providers, and authorities. "This approach distributes trust, responsibility and risk across the ecosystem," he says, "making decentralization not just viable, but essential for national-scale identity."

Boonsun describes the role of the NDID in the data exchange platform as taking place across rollout phases. "Digital identity alone does not create meaningful change," he says. "It becomes a true game-changer only when it is embedded in real, high-impact use cases that people actually use at scale." At launch, NDID enabled digital loan applications, credit bureau access, securities trading, and cross-bank digital account opening that didn't require visiting a branch. Future NDID services in the works include tax filing, life insurance applications and telemedicine consultations.

Boonsun understands that the adoption of powerful technology cannot occur without attention to building confidence and offering flexibility. "Alignment on assurance levels, regulations, legal enforceability, and liability models must come first," he says. NDID's strategy of focusing not on specific technologies but rather on real-life cases and on the trust of the exchange opens the door to further innovation and growth. "Verifiable credentials represent the second generation of digital identity," he says, "enabling trusted attributes to be reused securely with user content."

IDENTITY 25 HONOREE

Keshav Reddy

Founder at Equal AI

> The companies that win will not be those that collect the most data, but those that steward it most responsibly."

Keshav Reddy founded Equal in 2022 with a conviction that many in the industry were only beginning to voice: that digital identity and consented data access were foundational infrastructure for the digital economy. He arrived at that vision by watching 1.5 billion people share their most sensitive personal information with little awareness and even less control. "I started Equal because I realized that people were sharing their identity in many unconsented manners," he says, "and I thought there was a better way to do this."

That better way now runs at over a billion transactions annually. Equal integrates with more than 50 identity and financial data sources to power KYC, onboarding, fraud prevention, and income validation across India, a market that is simultaneously one of the world's most dynamic digital economies and one of its most challenging fraud environments. Equal was built to solve identity at scale, and the company's recognition as a 2025 World Economic Forum Technology Pioneer affirmed its global ambitions. "My proudest achievement," says Reddy, "is helping shift the conversation from 'compliance as paperwork' to 'consent as infrastructure.' Proving that privacy-forward systems can also be commercially scalable, he says, is the defining challenge of modern identity.

India is also among the most spam-affected markets in the world, and Reddy has turned his attention to the problem. To address it, his team built Equal AI, an intelligent assistant that answers unknown calls in fluent English, Hindi, or "Hinglish." It also achieves a 94% spam detection rate and (in internal trials) an 87% reduction in interruptions. This is about enabling intelligent representation for everyone, as Reddy explains: "Over time, our ambition is to build a daily-use AI layer for hundreds of millions of Indians—simplifying financial access, communication, and service delivery. We are building for India, but designing at global standards."

Looking further ahead, Reddy sees identity shifting from episodic verification to continuous trust signaling from a checkpoint to an operating layer. In this near future, AI systems will increasingly act as representatives of individuals, negotiating permissions and transacting within programmable consent boundaries. "Security improves because access becomes contextual and continuously evaluated," he notes. "Usability improves because individuals no longer need to manually manage every interaction." A potential complication: the industry's famous tendency to be ruled by the business needs of the quarter instead of their long-term goals. "If identity systems prioritize short-term growth over transparency, trust erodes," he worries. "And once trust erodes, the system weakens."

For Reddy, the imagined tension between privacy and business growth is a failure of design rather than an inevitable tradeoff. "I don't see this as a collision," he says. "Businesses don't need unlimited data. They need accurate, verified, consented data." The companies that will define the next era of identity, he believes, will be the ones that treat trust not as a constraint on growth but as a propellant.

IDENTITY 25 HONOREE

Drummond Reed

Director, First Person Cooperative

> “Protected proof-of-personhood credentials will be what ushers open-standard digital wallets and verifiable digital credentials into mass adoption.”

Drummond Reed has spent more than three decades in internet identity, security, privacy, and trust infrastructure, so it’s no surprise that he paused when asked to name his proudest achievement. It’s not his 2021 book *Self-Sovereign Identity*, which described decentralized identity as the third era of digital identity (after centralized and federated). “I still have people coming up to me at conferences asking me to sign it.” It’s not his work on First Person Cooperative and the First Person Network, though he predicts that one will have the biggest impact. It’s not the six years he spent as Chief Trust Officer at Evernym, or a similarly long stint at Respect Network, where he was co-founder and CEO. Reed’s resume is dotted with all kinds of highlights like these, including serving as a founding board member of the Open ID Foundation and forging an alliance with the Information Card Foundation to form the Open Identity Foundation. Impressive stuff, but not at the top of his list.

The accomplishment that gives Reed the most pride is the W3C Decentralized Identifiers (DIDs) 1.0 spec. He notes that it took seven years for that spec to be passed as a full W3C recommendation. “Those of us who worked on it so long knew that it would take a decade or more for it to fully take hold in the market because it is so low in the stack of new infrastructure,” he explains. Every major AI agent interoperability standard relies on DIDs, Reed says, “so they really will be the atomic building block: not just of decentralized identity, but of decentralized digital trust infrastructure as a whole.” That momentum continues, despite formal objections from big browser vendors with a desire to maintain asymmetric power.

As Reed sees it, AI agents will soon be bringing enormous changes to the way digital identity and trust are managed online. He says that there has always been a gulf between the way humans process identity and the way we have designed machines to verify. “People were never intended to have to deal with usernames and passwords, let alone cryptographic keys of any kind,” he says. AI agents will do all the heavy lifting required to establish and verify trust, performing tasks that only a small fraction of internet users could be reasonably expected to master. “Within five years,” Reed predicts, “the vast majority of our interactions online will be mediated by AI agents.”

Reed has a talent for making the complex simple, a skill that he’s carried over from his prior career as a writer. Visit the First Person Project’s site, and you will be greeted by a simple message: “Real People. Real trust. No intermediaries. A global infrastructure for social verification.”

The main goal of First Person, Reed explains, is to drive acceptance and implementation of zero-knowledge proof-protected proof of personhood. “They are the next leap beyond passkeys and CAPTCHAs,” he predicts. “I believe they will be the breakthrough that will finally usher open standard digital wallets and verifiable digital credentials into mass adoption.”

IDENTITY 25 HONOREE

Andrew Regenscheid

Manager, Cryptographic Technology Group, NIST

> The challenge in developing digital identity standards is not choosing between security, privacy, and user experience, but addressing all three."

Andrew Regenscheid, a cybersecurity expert whose time at the Department of Commerce's National Institute of Standards and Technology is approaching two decades, has played key roles in digital identity's history, and he is already involved in a ten-year plan to provide identity with a secure future. He took part in the five-year effort to develop and release the 2025 Digital Identity Guidelines and an eight-year collaboration that resulted in the first post-quantum cryptography standards. But 2025 is ancient history in cryptography time, and Regenscheid will also guide the phasing out of vulnerable algorithms by 2035. "Quantum computing poses a direct threat to the public-key cryptography that underpins today's digital identity infrastructure," he says. "We need to migrate to new cryptographic algorithm standards that are resistant to quantum attacks."

Although much of his focus during the most recent decade of his service at NIST has been on digital identity standards, Regenscheid has vast experience in real world applications including voting systems, firmware, platforms, and communications protocols. "A consistent theme throughout my work," he says, "has been applying cryptographic algorithms and tools to strengthen the security and trustworthiness of IT systems." In order for standards and guidelines to be useful, Regenscheid explains, they must reflect the needs of a large number of stakeholders from government, industry, and academia. "The revised Digital Identity Guidelines incorporate thousands of discrete public comments," he says, "and reflect significant advances in authentication technology, risk management, privacy protections, and user experience."

This kind of 30,000-foot perspective helps Regenscheid describe what he sees as an industry shift from incremental fixes to long-term issues. "We are now seeing new approaches, particularly passkeys and verifiable credentials," he says, "that come together in ways that reflect hard-earned lessons from the past several decades." The identity space never suffered from a lack of good ideas, according to Regenscheid; it just needed a plan for bringing it all together intelligently. "The integration challenge is where we've seen struggles," he says. "Different solutions evolving in parallel without aligning on how they are meant to work together." He sees the industry trending towards greater alignment across the ecosystem: more interoperability, less integration friction, and scalable deployment.

Regenscheid pushes back on the idea that achieving the goals of privacy protection, hardy security, and user convenience in digital identity requires compromise: In his view, these are mutually reinforcing goals. "The challenge in developing standards is not choosing between these objectives, but addressing all three at the same time," he says. "Achieving that balance is hard: not because the goals are in conflict, but because each is difficult in its own right." He remains optimistic that the industry is on a path of constant learning and improvement, consistent exploration of new approaches and technologies, and the collaborative creation of new standards.

IDENTITY 25 HONOREE

Justin Richer

Senior Staff Engineer, MongoDB

"A system with zero functionality and max security is useless. One with max functionality and zero security will be used…until something goes wrong."

As a Senior Staff Engineer at MongoDB, Justin Richer leads the identity engineering efforts for the Atlas cloud database team, building on two decades of groundbreaking standards work and hands-on development. Richer's journey began with bringing together collaboration systems that helped people work together at MITRE. Then the information security team delivered a reality check: We can't just share everyone's data everywhere. That focused Richer on a long-term challenge: "How do we make this secure but maximize the functionality that people care about?" Richer's progress toward this goal included becoming an editor of major security standards, including HTTP message signatures, and writing *OAuth in Action*. His work on OAuth 2 and OpenID Connect helped create the foundation for how billions of users authenticate across the web today.

For Richer, his proudest moments came quietly, watching adoption spread. "During the early work on OAuth 2 and OpenID Connect, I started to notice more and more places where the protocols were being used. I'd spy a 'client_id' in a parameter, or a 'scope' with an interesting value." These protocols exploded into widespread adoption, solving real problems in repeatable ways. "Developers were reaching for these tools because they worked, they could be understood, and they hit the right notes for the problems people were facing."

Richer's many valuable contributions include Vectors of Trust, a framework for describing the complex dimensions of user accounts that moved the industry beyond oversimplified single-number ratings. "A decade ago, we relied on Level of Assurance to wrap up all the concerns of a logged-in user into a single number. I worked to split those concerns apart in both Vectors of Trust and NIST SP 800-63-3," he explains. "Today, I still see the need for this split in more places as we reach for tools that allow us to describe the world we're in and reason about it more accurately."

Looking ahead, Richer sees the identity landscape shifting dramatically. "How we handle 'sessions' and things like them is changing based on what people expect and what technology can do," he observes. AI agents are introducing real-time connections between systems, challenging assumptions built into OAuth 2. "We're seeing proposed extensions to OAuth, such as new ways to register applications dynamically, as well as new protocols like GNAP and a wide variety of proprietary and experimental systems, that help us move into this more dynamic world."

Throughout his career, Richer has maintained a unique perspective shaped by his dual role as a standards editor and an implementing engineer. "Many years ago I realized that writing standards has a lot in common with programming," he says. "In both cases you're using a special syntax to get a particular behavior. The difference is that with specifications, your runtime platform is wildly unreliable: It's the mind of another implementing engineer." Through this standards engineering, Richer can leverage his skills across the wider programming world, and be a nontrivial part of solving problems he'll never see.

IDENTITY 25 HONOREE

Deepanker Saxena

GM and Head of Product, Socure

> "It was humbling to work in identity and still feel stuck in the identity loop. That experience reshaped how I approached the products we build."

Deepanker Saxena, Head of Product at Socure, did not plan on becoming an identity expert. As a software engineer over a decade ago, his work building gateway integration APIs, login systems, and onboarding flows was identity-adjacent. But in those days, identity was, as he puts it, "a technical requirement, not a defining problem." That all changed, he remembers, when he left India. "That is when identity became personal."

Upon his arrival in the United States, Saxena says he felt invisible to the identity ecosystem: a blank slate. Without an address, opening a bank account or acquiring a government ID was a titanic struggle. But getting a lease – and solving that address problem – required a credit history he didn't have. "It felt like a jumpstart problem," says Saxena. "I knew who I was, but the system did not." As an engineer, Saxena had often wished for exposure to end-users and their issues. Now here he was, and he felt inspired to leverage that perspective. "That experience reshaped how I approached the products we build."

For Saxena, running the leading platform for digital identity verification means understanding and dismantling organized fraud rings targeting, for example, financial institutions. But his approach to identity is personal, almost humanitarian. "For me, identity done right means two things: stopping harm, and not creating new harm." Saxener reveals that Socure invests heavily in accessibility and is continuously evaluating model performance across aspects like skin tones to eliminate bias and cultivate inclusion and fairness. "Inclusion is not just about supporting more documents or geographies," he says. "It is about ensuring people are not falsely rejected because of how they look, how old they are, or what device they use."

Saxena is a firm believer that in the identity space, security and usability can be complementary. He cites the shift towards portable identity grounded in cryptographic trust rather than repetitive document uploads. "When I think back to my own experience of proving myself over and over again, it becomes clear how inefficient and exclusionary static identity checks can be," he says. Verifying identity once, and only disclosing necessary case-specific attributes rather than full document sharing can reduce both friction and data exposure. Saxena is particularly encouraged by mobile driver's licenses, verifiable credentials, and wallet-based identity systems. He says that these are examples of a "real transformation that comes from combining portability with adaptive risk systems where security and usability reinforce each other rather than compete."

Saxena says that AI has brought into focus the need for identity professionals to ensure constant adaptation and evolution of their systems. "Identity is not a feature you ship once," he reminds us. "It is infrastructure you are responsible for over time." It's crucial to remember, he says, that identity programs exist not only to meet metrics but also to serve and protect individuals. "Identity systems are socio-technical systems. Product architecture and user experience decisions are often just as important as model performance."

IDENTITY 25 HONOREE

Baroness Joanna Shields, OBE

Founder and CEO at Precognition

> “I believe it’s time to solve for age online once and for all. The technology exists—what’s been missing is the will to align around trusted, shared infrastructure.”

Baroness Joanna Shields, founder and CEO of the AI strategy firm Precognition, is beginning her fifth decade as a tech pioneer and has had a hand in the development of image digitization, video streaming, and encryption with organizations like RealNetworks, Google, AOL, and Facebook. Her experience and knowledge have informed her important work over the past ten years protecting children online. “For years, age assurance online has been fragmented, invasive, and ineffective,” she says, “forcing people to repeatedly share documents or personal data while still failing to protect children.” Shields says that the time is now to solve for age online. “The technology exists,” she says. “What’s been missing is the will to align around trusted, shared infrastructure.”

Shields has worked in both the private and public sectors, and served as the UK Minister for Internet Safety and Security for two Prime Ministers. That experience made it clear to her that commercial and government organizations can be quite good at building systems that drive efficiency, growth, and engagement, while still failing to design for people. “Identity, safety, aging, and trust were often treated as edge cases rather than foundational requirements,” she laments. “Once technology reaches a certain scale, those omissions stop being abstract and start shaping real lives.”

Shields became convinced that such omissions could not be patched. “Responsibility can’t be bolted on after the fact,” she says. “It has to be designed into the infrastructure itself.” The key to protecting children online, argues Shields, is interoperable, privacy-preserving age credentials (in contrast to closed systems that require repeated document sharing). This ideal is the model being advanced by the OpenAge initiative and its AgeKey project, which she chairs.

Shields is encouraged by the shift in assumptions underlying new approaches, like the recent announcement from OpenAI that they will begin treating children differently from the outset rather than relying on downstream controls or self-declaration. “That matters,” Shields says, “not because it solves age assurance on its own, but because it recognizes that age needs to be a foundational input, not an optional layer.” Building identity, age assurance, and safety directly into the infrastructure of identity systems, in her view, could make protection automatic.

Shields rejects the idea that public safety and privacy need to be in conflict with each other. “During my time as a minister, there was a common assumption that you could either protect people or protect privacy, but not both,” she says. “I never accepted that framing.” Applying advanced analytical techniques to public data creates, in Shields’ view, a useful understanding of language, patterns, and networks. These can help combat not only child exploitation but also online extremism. “The real challenge isn’t access to more data, but designing better systems,” she says. “You can strengthen public safety, protect children, and build trust at the same time.”

IDENTITY 25 HONOREE

Taranjeet Singh

Founder and CEO, Mem0

> “When systems can remember who a user is, what matters to them, and what has changed, that is identity at its most fundamental level.”

Taranjeet Singh is the founder and CEO of Mem0, the universal and self-improving memory layer for LLM applications. He’s not there to create a delightful user journey—he’s trying to deliver an experience that’s invisible and unsurprising. “Memory is increasingly recognized as foundational infrastructure for AI,” he says. “The goal isn’t for users to admire the memory layer: It’s for them to never think about it.”

Singh recalls the frustration he and fellow developers felt when forced to re-explain preferences and context to each AI tool they used. “Switching between coding assistants, chat interfaces, or agents meant starting from scratch each time,” he says. “Even small changes in workflow erased weeks of accumulated understanding.” Singh says that the repetition seemed unnecessarily complicated and clunky, inspiring a small internal experiment that became OpenMemory. “We launched it publicly with minimal expectations. The response was immediate and surprising.” Developers embraced OpenMemory as a way to share context across workflows and tools, validating the sense Singh and his collaborators had that persistent memory was achievable and would be in demand. “User trust isn’t just about accuracy,” he says. “It’s about predictability.”

OpenMemory builds on standard interfaces like the Model Context Protocol (MCP) that are changing the identity game by decoupling identity and context, and standardizing how AI agents interact with tools, data, and long-lived context. Singh says that this decoupling makes portable context possible, enabling users to carry information and knowledge across applications rather than having to rebuild them for each one. This creates trust between parties on both ends of agent interaction. “As agents take on more autonomous tasks,” Singh says, “the layer that governs what they remember and how they personalize behavior becomes critical infrastructure.”

Singh says that agentic memory is more than mere total recall. The clear benefit, of course, is that memory eliminates the requirement that AI agents continually re-ask fundamental questions, freeing them to adapt their actions based on prior interactions, preferences, and resolutions. “The experience shifts from transactional to relational,” he says. But he acknolwedges that there is also a real risk of over-retention by these models. “Not everything should be remembered indefinitely,” he concedes, explaining that systems must incorporate scoped recall, expiration, and user control if they are to be trusted. “Without those safeguards, personalization can become stale, intrusive, or misleading. Forgetting, correction, and visibility are just as important as recall.”

Singh is enthusiastic about an approach to agentic memory that welcomes cross-industry contributions. “Open source can play a critical role here by establishing expectations,” he asserts. “When developers build on shared infrastructure, patterns emerge. Norms form. Standards follow.”

IDENTITY 25 HONOREE

David Soria Parra

Member of Technical Staff, Anthropic

> “Historically, the industry has leaned on deliberate standardization processes. Now it’s being challenged to move faster to keep pace with AI.”

In virtually every STEM-adjacent field or endeavor, there are heroes not only at the dawn of discovery but also at every other touchpoint. Identity is one of those fields, and Anthropic’s David Soria Parra, the co-creator of the Model Context Protocol, is one of those modern heroes, happening upon identity mostly by accident. “I worked on developer tooling and open source for decades,” he says, and it paved the way for taking on the responsibility of developing the MCP authentication spec. “This drew me into the identity world, connecting me with some of the best people in the industry,” he says. “It gave me an opportunity to dive deep into the challenges of authentication and authorization.”

Soria Parra is generous when talking about his accomplishments in relation to collaborators and predecessors. “My proudest achievement is creating MCP and fostering a community of identity experts who helped develop it into a universal connectivity layer for AI,” he says. He is quick to acknowledge that MCP may be the latest standard, but it wasn’t the first. “OAuth and related standards fundamentally changed how we think about identity on the web,” he remembers. “We succeeded not just in defining a solid authentication story for MCP, but also in pushing forward associated standards like OAuth 2.1 and innovating on OAuth extensions.” All of these steps are guiding the purposeful, continuous evolution of the identity industry.

His long experience with AI has helped Soria Parra meet today’s interesting and pivotal moment in identity. “Historically, the industry has leaned on deliberate standardization processes,” he says, “but now it’s being challenged to move faster to keep pace with AI development.” Soria Parra and his MCP co-creator, Justin Spahr-Summers, have already been a part of the faster development cycles and smaller dev teams that AI makes possible today (and necessary tomorrow). Soria Parra is excited by identity’s shift from focusing solely on defining standards to prioritizing everyday usability. “The identity industry has shown that it can adapt to this new tempo,” he says. “The challenge will be finding the right balance between moving fast and maintaining the thoughtful diligence the identity industry is known for.”

There is currently great concern around the impact of AI not only on authorization and verification but also on job displacement. Soria Parra says that his work running an open standard has enhanced his appreciation not only of the potential of AI but also of the irreplaceable role of humans in the process. “There are things humans are uniquely positioned to do, like governance, creating a community, and building a vision,” he says, “and there are things where AI excels, like reproducing bugs from the tracker or building out new features. In an AI-enabled world, understanding what you add as a human and where to lean on AI matters more than ever.”

IDENTITY 25 HONOREE

Rao Surapaneni

VP and GM of the Business Application Platform, Google Cloud

> We are building a world where a 'digital twin' agent can handle your life's logistics, but only within the boundaries you set."

"There are no problems, just opportunities," is a famous innovator mantra to which Rao Surapaneni , Vice President and General Manager of the business application platform at Google Cloud, would likely subscribe. After all, it's not every day you hear someone that's excited about the potential created in the identity space by...fraudulent deepfakes. "The silver lining to the deepfake crisis," he says, "is that it is forcing the world to adopt hard, cryptographic identity over soft, visual cues."

Surapaneni is a key figure in the development of interoperable AI agents and agentic identity, and he has spent considerable time and effort meeting the "Identity for AI" challenge. He realized that AI's ability not just to think but to act presents an enormous potential security risk when that agent lacks a verifiable identity. "The insight I had along the way," he says, "is that identity must be active, not just static, and that we must shift from static authorization – who are you? – to active delegation: what have you authorized this agent to do right now?"

Surapaneni points to his work on two foundational open-source protocols that address some of the many challenges AI presents to identity. The first, Agent2Agent (A2A), is an open standard that gives AI agents a common language to communicate across platforms. Surapaneni led the establishment of the "Agent Card," a JSON-based public profile that serves as an agent's identity and outlines agentic capabilities, supported data modalities, and authentication requirements. The second, Agent Payments Protocol (AP2), focuses on the financial dimension of agent identity and uses "mandates," which Surapaneni describes as cryptographically-signed digital contracts providing proof that a human user has authorized an agent to make a specific purchase.

How? Surapaneni uses a theoretical agent task, "buy World Cup tickets the moment they drop, if they are under $200," to demonstrate the three mandates. First is the Intent Mandate, a tamper-proof digital contract signed by the human purchaser, often via a biometric scan. The contract contains constraints like "Maximum price: $200; Category: field 100- or 200-level; Expiry: next 48 hours." The Intent Mandate gives the agent a way to prove to the merchant that the potential purchase has been pre-authorized and prevents the agent from "hallucinating" a purchase or overspending. Second is the Cart Mandate, the merchant's guarantee to fulfill the exact order at or below that specific price. The agent verifies the Cart Mandate against the Intent Mandate, automatically rejecting the order if it violates any part of the Intent Mandate. If the intent and cart mandates are aligned, money moves via the Payment Mandate, with security preserved by shielding actual credit card information from the agent.

While Surapaneni's recent focus is on identity as it affects commerce, he says that the shift to "cryptographic veracity" brings greater convenience, control, and safety to much more than shopping. "The future of identity is autonomous but auditable," he says. "We are building a world where your 'digital twin' can handle your life's logistics, but only within the cryptographically signed boundaries you set."

IDENTITY 25 HONOREE

Phil Windley

Founder, Internet Identity Workshop

> I believe we'll look back on this time as when identity shifted from being mainly about logging in to being about making trustworthy decisions."

As Utah's Chief Information Officer, Phil Windley had a crash course in understanding the value of identity. He recognized that U.S. government structure, with its multiple agencies, information systems, and protocols, often forced people to perform overly complicated navigation to get things done. "Public services fail when they assume people can or should adapt to bureaucratic structures," he says. "I came to realize that identity was foundational to delivering better services." That experience led to a career focus on digital identity work, including founding the Internet Identity Workshop. "That realization continues to influence how I think about building identity systems that put people first."

Windley acknowledges that even the most elegant engineering solutions require broad adoption to be truly successful. "Identity has become foundational infrastructure," he says, "and the most complex problems ahead are not purely technical. They involve coordination, governance, and the design of systems that people can understand and trust." Windley and other leaders in the space recognize that conversations about the trade-offs between privacy, authenticity, and confidence are important if we're going to get to the identity design the real world needs, going forward. "Identity maturity helps us understand," he says, "that strong identity systems must function not only in ideal conditions but also in complex real-world environments."

Windley is happy to note a growing acceptance, in both government and industry, that identity can't remain trapped inside accounts and platforms. Instead, more and more decision-makers see digital wallets and verifiable credentials as essential infrastructure. But some holdouts worry him. "Vendor-specific implementation not based on open standards will continue to fragment the user experience," he warns. "Fragmentation causes inconvenience, raises integration and maintenance costs, and ultimately hampers adoption."

A believer in decentralized identity as a game-changing architectural shift, Windley nonetheless thinks the term itself is imprecise. "What really matters is 'first-person identity,' the concept that individuals and organizations can control and present their own identity directly," he says. This framework is a little easier for everyone to understand, and shifts the focus to outcomes rather than to wonky implementation details. In fact, first-person identity decouples identity and login accounts, he says, setting clear delineation lines among stakeholders: the trusted sources issuing credentials, the users holding those credentials, and the organizations deciding whether to grant the requested permission. "This enables systems that are more secure, more privacy-protecting, and often easier to use," he says, "because sensitive data no longer needs to be copied and stored everywhere it might be required."

Windley says that these are early days in first-person identity, and he predicts that adoption will occur in fits and starts. Nevertheless, he is firmly optimistic. "I believe we'll look back on this time as when identity shifted from being mainly about logging in to being about making trustworthy decisions."

Securing identity in the age of AI

Our methodology

Each year, Okta assembles an all-star selection committee of identity experts to help determine the honorees in the year's Identity 25 initiative. This anonymous committee nominates a few dozen carefully considered candidates, including open source contributors, founders, IT specialists, technologists, academics, operators, policy makers, and more. They then meet on multiple occasions to discuss the merits of potential candidates, ultimately winnowing down the broader list to just 25 selectees. Outreach to selectees includes 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 pioneers of identity celebrated in this year's Identity 25 are part of a long-term, concerted effort to secure our digital world, so that global collaboration, ecommerce, online transactions, and other digital functions can be safer and easier for all the world's citizens. As you've seen in these pages, these heroes are passionate about security and usability, about maintaining consumer privacy while expanding government and enterprise services, and about thwarting fraudsters trying to exploit security weaknesses to gain access to our assets and identities.

Whether it's strengthening authentication, developing next-gen identity standards, making sense of autonomous agents, or rolling out AI assistants to the masses, we can count on the tireless efforts of the Identity 25 to keep us moving ever closer to the secure and seamless digital future we all hope for. Individually and in collaboration, they're always hard at work behind the scenes: developing ever-smarter standards, chopping through governmental bureaucracy and enterprise competition, and delivering big identity breakthroughs and small gradual improvements. Yes, professionalized fraud groups are presenting increasingly sophisticated threats, like leveraging generative AI to create deepfake IDs that test our security controls at scale. But we're not alone, and we're lucky we've got these folks watching our back.

Thanks for joining us in celebrating this year's incredible visionaries… We'll see you in 2027!

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 Identity25nominations@okta.com on or before July 1, 2026. Include any relevant links to support your case. Okta's Identity 25 Selection Committee will consider your nomination and reach out 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.