THE FUTURE OF IDENTITY 2.0

Digital identity in a new world – the future came faster

Steve Ritter – Chief Technology Officer, Mitek

Steve Ritter

Chief Technology Officer, Mitek

When I wrote The Future of Identity toward the end of 2019, I said we were at a pivot point in history. Identity was profoundly changing. The very concept and the practical role it plays in our lives would be far different in the years ahead than in all the centuries before.

It turns out this was putting it mildly. None of us could know that with the onset of the pandemic, a pivot point would become an abrupt inflection point—leading to a hockey stick of tremendously accelerated change.

Since then, the number of people needing to transmute physical identity credentials into digital identities has skyrocketed. So has the number of businesses and government organizations whose success—even ability to perform their core missions—depends on being able to verify these identities without interacting in person.

Since then, because many organizations were unprepared, tens of millions of people around the globe have been materially harmed, some by inability to access their accounts or receive government assistance, some by fraud. Yet the crisis has created momentum for widespread adoption of modern identity verification solutions. And seeds are being planted for a profusion of new digital products, services and business models that could benefit everyone.

What precisely has accelerated over the past year, and what could it mean for your organization? Here's my view of digital identity in a new world...

Unchartered ascent into the new digital landscape

We are riding an abrupt, steep curve of change. It is taking us into a new world where, like Alice tumbling into Wonderland, we'll find both delights and dangers.

To my mind, there are six significant identity-related change vectors, all increasing in magnitude and, since the pandemic, at sharply increased velocities. I see these changes as interrelated and will talk about them that way. We've also provided jump-to page locations for those preferring not to read through.

We're speeding from **digital-optional to digital-centric**

PAGE 3

Fraud is soaring — **better identity verification** is key to containing it

PAGE 5

More and more organizations are paying attention to **who enters their "front door"** – since it affects almost everything that comes after

PAGE 6

Striking the right balance between **less friction and more security** is becoming critical to operations — not just at onboarding but throughout customer journeys

PAGE 8

Trust is emerging as the primary enabler of business growth

PAGE 10

"Who are you?" is a question of rising consequence as the information age lasers in on understanding individuals at scale'

PAGE 15

We're speeding from digital-optional to digital-centric

All over the globe more people are going online, often in pursuit of daily necessities. Those already online are spending more time there and trying out new digital products and services. Our economies are becoming digital-centric, and it's going to become increasingly difficult for anyone to opt out.

We can see accelerated digital transformation in e-commerce. On average in 2020, across the UK, Germany, France, the Netherlands, Spain and Italy, consumer online sales rose by 31%, says Statista.

In the US, says Digital Commerce 360, it jumped by 44%—nearly triple the growth rate of the previous year. This was enough to push total retail sales to its highest growth rate in nearly 20 years—despite declining sales in other channels.

You might assume that's all Amazon, but not so. I think it's significant that the top 100 retailers after Amazon accounted for more than 74% of this growth—and the top 20 each saw their own annual growth rates top 85%.

75%

of US consumers have tried a new shopping behavior since COVID-19 started.

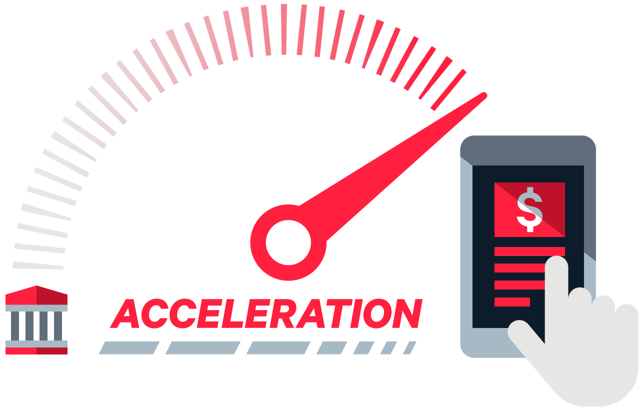
"The Great Consumer Shift", McKinsey 2020

50%

of consumers now interact with their bank through mobile apps or websites at least once a week, compared to 32% two years ago.

Accenture Banking Consumer Study 2020

We can see similar acceleration in financial services. Fidelity National Information Services, which works with 50 of the world's largest banks, reported a 200% jump in new mobile banking registrations and an 85% jump in mobile banking traffic in early April 2020 alone. In the same month, says Bank of America, baby boomers and older consumers accounted for 23% of first-time digital logins and 22% of new mobile deposits—and that number was still holding at about 20% in the bank's Q3'20 financial results. In May, Key Bank told CNBC it was seeing double-digit month-over-month growth in online usage. A September JD Power survey found that 44% of retail banking customers said they were using their primary bank's mobile app more often.



Meanwhile, fintechs and other challengers to traditional banks have navigated pandemic-rocked markets quite well. According to a global study by the World Economic Forum (WEF), University of Cambridge and World Bank Group, they grew transactions by 13% in the first half of 2020. Some fintechs have reported much more spectacular growth: Current, for example, whose target customer profile fits that of many essential workers during the pandemic, added 100,000 new users in April and May 2020. Chime, which had 8 million customers before the pandemic year, now claims more than 12 million (a 50% growth rate).

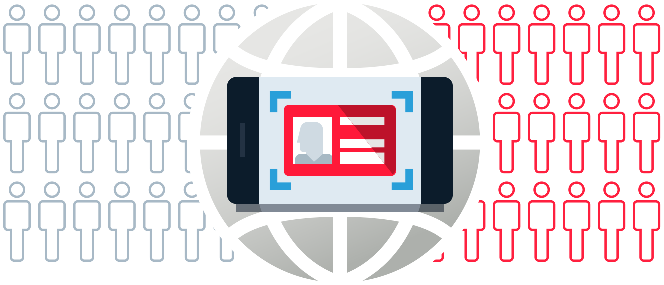
There's no doubt consumers are getting on the digital bullet train in large numbers—yet some don't have a ticket. For instance, in the US, credit bureau records are often used for identity verification. But as many as 45 million consumers have inadequate credit records or none at all according to the Consumer Financial Protection Bureau (CFPB), and that can be a problem in digital onboarding. And one New York state healthcare group—can you believe it—used credit bureau records to verify identities for COVID vaccination eligibility!

To avoid the exclusionary impacts of relying on credit-related data, and because personally identifiable information (PII) continues to hacked, more and more organizations are supplementing data-centric identity verification with document-centric approaches. This technique uses a government-issued ID—something over 90% of US adults and an estimated 79% of the world's population have—along with a mobile or internet connection. AI-based software instantly determines if the ID document is genuine and extracts data for identity checks and analytics. Most organizations also implement optional biometric facial comparison to match the user's selfie with the image on the ID, confirming they're the same person. When the software used to take the selfie also has liveness detection, you're able to tie the government ID to a real person.

That still doesn't put a ticket in every hand. The World Bank estimates that there are over a billion consumers globally who don't have a legal identity document or record of any kind. Also, there are plenty who aren't online yet. The World Economic Forum (WEF) had predicted we'd be at 50% by 2020, and the latest I've seen from Statista is 59%. So we're making progress, but still have a way to go. The bank's Identification for Development (ID4D) initiative, investing more than a billion dollars across 30 developing countries, is one of the efforts underway to change this situation and prevent digital exclusion.

In a digital-centric world, everyone must have access via a verified digital identity.

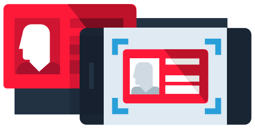
Currently, more than a billion people are excluded.



What is document-centric identity proofing?

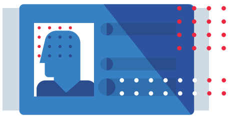
Use of facial biometrics, computervision and other AI to determine if an identity document submitted via digital channels is legitimate and belongs to the applicant

HOW DOES IT WORK?



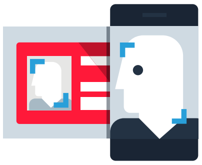
CAPTURE IDENTITY DOCUMENT

User interface (mobile app, mobile web or online onboarding) guides new account applicants to snap high-quality image of physical ID in first attempt.



VERIFY AUTHENTICITY

AI and computervision algorithms recognize and classify the ID document, extract data from it, and evaluate authenticity. Confirm is genuine and unaltered.



PROVE REAL-WORLD IDENTITY

User interface guides applicant to take high-quality selfie. AI face recognition biometric compares selfie with ID photo. Is the person in the selfie live? Is the same person as in the ID?

Fraud is soaring–better identity verification is key to containing it

Okay, this is the last section where I'll throw a lot of data at you—and it's ugly data. But this isn't an invitation to doomscroll, because ultimately I believe today's seemingly out-of-control fraud has a silver lining.

The data on fraud was alarming even before the pandemic. As we discussed in Mitek's white paper Fraud Trends and Techtonics, continued massive data breaches fueled a 72% increase in account takeovers from 2018 to 2019 (Javelin Research). In the same period, online payment fraud jumped from $26 billion to $50 billion—a nearly 100% increase (Juniper Research). Not only that, but in 2019 one in every five new accounts was likely fraudulent (NuData).

Since the pandemic, it gets much, much worse.

Fraudsters swiftly jumped on opportunities created by the forced shift to digital. Fraud rates in UK financial services shot up 33% in April 2020, when compared with previous monthly averages, according to data from Experian and the National Hunter Fraud Prevention Service. UK Finance, an association of more than 250 of the country's banking and finance companies, reported in Global Banking and Finance that more than £27 million was lost to online fraud in the first half of 2020. The biggest jump—at 181%—was in car and other asset finance applications.

In the US, Security magazine said phishing attacks (aimed at stealing personally identifiable information for use in account takeovers as well as for creating synthetic identities for new account fraud) increased by more than 667% in March 2020 alone. By November 2020, ABA Banking Journal reported that account takeover attacks had increased by 72%.

Meanwhile, in ecommerce, TransUnion saw a 12% jump in online purchasing fraud in March-May 2020 vs. January-March of the previous year. A study by Sift, looking more broadly at fraudulent content aimed at "deceiving and exploiting consumers on ecommerce sites and within online communities," found a 109% increase January through May 2020.

Looking at the year as a whole, Javelin's 2021 Identity Fraud Study found that losses from traditional identity fraud dropped to $13.3 billion in 2020, a decrease of 21% from the previous year, due largely to changes in consumer behavior during lockdowns. But losses from new identity fraud scams targeted directly at consumers surged to $43 billion, sending total identity fraud losses to a record $56 billion!

Meanwhile, a survey by Brightpearl, says that while more than half of Americans have increased online spending since the onset of the pandemic, over 60% have experienced problems with their online purchases.

The picture is even less pretty when we look at government, especially in the US. Inadequate digital ID verification in federal unemployment insurance programs has created a bonanza for fraudsters. The administrator of the programs put it bluntly: "We literally have billions of dollars at this point walking out the door under these programs due to identity theft and lack of ability to deal with that verification."

State unemployment offices have also stumbled over identity verification. In California, most spectacularly, something like 1.4 million citizens were cut off from payments temporarily as the state's Employment Development Department (EDD) struggled to get a handle on fraud—possibly amounting to 30% of claims—by verifying applicant identities. Decades-

> *"If you conducted e-commerce transactions since the pandemic struck, you have probably been the target, or even a victim, of online fraud."*
>
> E-commerce Times, July 2020

old systems resulted in about half of claims requiring manual review by overwhelmed staff. NBC Los Angeles reported that fraud losses since the pandemic could add up to as much as $10 billion.

The surge of fraud attacks is not likely to subside when pandemic risk does. With the continued rise in connected digital users (many working from less-secure home networks) and more consumer, business and IoT devices coming online every day, the attack surface is expanding. New digital business models, spawning diverse third-party relationships, partnerships and ecosystems, will create more opportunities for fraudsters and complexities for defenders. Widening availability of 5G will increase the speed of criminal attacks.

You're probably thinking, "Enough there Steve, where's the silver lining?"

Here it is: Better identity verification in digital onboarding will help us fight this unprecedented rise in fraud. I'll talk about how that happens in the next section, but for now, let me just say that crisis causes people to act and organizations to change.

The California EDD recently implemented a modern document-centric identity proofing solution, which is now verifying up to 90% of claim applicants automatically. Colorado, Pennsylvania and dozens of other states are doing something similar—as are huge swaths of businesses, from insurance carriers to online marketplaces. A bipartisan Improving Digital Identity Act of 2020 is making its way through the US Congress. Gartner predicts that by 2022, 80% of organizations will use document-centric identity proofing as part of their onboarding workflows.

More and more organizations are paying attention to who enters their "front door"—since it affects almost everything that comes after

It's clear today that many businesses and government agencies can no longer perform their core functions without the ability to verify identities through an efficient, scalable digital onboarding process. What's more, the reliability of up-front identity verification can have far-reaching implications.

How well organizations control their "front doors" has a lot to do with the extent of fraud experienced long after onboarding by their organizations and customers. Verified digital identities are also bedrock in the growing competition to better understand individual consumers and tailor hyper-personalized offers and services to them.

In financial services, for instance, fraudsters who get through the front door by opening new accounts with an entirely fake or synthetic identity often bide their time, behaving like good customers long enough to acquire higher credit limits and open additional credit lines. Eventually,

> **"The future of customer experience: Personalized white-glove service for all.**
>
> *"Characterized by attention to detail, convenience, speed and emotional fulfillment, this high standard of service offers solutions, products and services that are tailored to each customer's specific and unique needs. It is central to a customer-first mindset and made possible by the availability of data and advanced analytics to track a customer's journey in real time."*
>
> McKinsey & Company, June 2020

they “bust out” to take as much loot as possible before disappearing. Traditional banks have been partly blind to such schemes because most haven’t shared accountholder data across lines of business and functions (like origination and collection).

This is fundamentally an Identity problem. Without the ability to know that the accountholder racking up charges on a credit card is the same person as the accountholder requesting an increase in a separate credit line, banks can’t form a full picture of an individual customer’s riskiness or understand the meaning of overall behavioral patterns.

That’s changing—the pandemic has catapulted banks that haven’t already connected the dots into doing it pronto. With a verified identity at center, they’re pulling together data on all of the individual’s accounts and transactions across the entire enterprise into dynamically updated profiles.

Such profiles capture the most meaningful information (not just data points, but calculated variables, data relationships and analytic predictions) in a super-condensed form ideal for use in real time by fraud detection models and other AI/ML. No surprise, these profiles can also be leveraged by other analytics as part of processes that score credit risk, assess affordability, determine eligibility for products, tailor a personalized set of offers or recommend a customer retention strategy.

In fact, identity-anchored, customer-centric methods like these will be essential for meeting rising consumer expectations for hyper-personalized products, services and communications. A 2020 Salesforce study of Trends in Financial Services found that 66% of respondents now say they expect companies to understand their unique needs and expectations; 52% expect companies to always personalize offers.

Fintechs, online marketplaces and other e-tailers are, of course, way ahead in the race to create individualized customer experiences. Unburdened by legacy organizational and technology architectures, they’ve always had a complete view of their customers. Now they’re leveraging it as they expand out from their initial niches to offer a widening range of digital products and services.

Slamming the door on synthetic identities

A 2019 report by the US Federal Reserve called out synthetic identity fraud as the fastest growing financial crime in the country. Since the pandemic, huge increases in phishing and other crimes aimed at exposing consumer PII are supplying even more building blocks for these fraudulent identities assembled of made up, stolen and/or slightly modified information.

Because synthetic identities look quite similar to legitimate identities, they often get by traditional analytic models. Identity proofing that includes a selfie snapshot or video is an effective deterrent, however, since most fraudsters engaging in this crime don’t want to use their own faces.

Also, because fraudsters frequently reuse pieces of PII, link analysis software that looks for these overlaps can also be quite effective. It can find, for example, phone numbers or addresses that have been used for other identities, including those associated with fraud or members of suspected fraud rings. Fuzzy logic enables link analysis to pick up near matches, where fraudsters have made minor alterations to real PII.

Still, some of these younger companies are vulnerable to fraud. Focused primarily on growth in the past, they were not always careful about who they took on board, often accepting credentials from third parties that had not performed reliable identity proofing. Consequences include the rising fraud levels I’ve mentioned. That’s why I was glad to read, in the WEF global study, that 40% of surveyed fintechs have recently implemented or are in the process of implementing enhanced fraud or cyber-security features.

Striking the right balance between less friction and more security is becoming critical to operations—not just at onboarding but throughout customer journeys

For the ever-increasing number of organizations needing to verify identities at digital onboarding, minimizing friction during the process is a priority.

US consumers made their feelings about that very clear before the pandemic. In a 2019 Mitek survey, consumers cited the top three benefits of establishing a digital identity as: 1. convenience (66% of respondents); 2. speed (49%); and 3. access (31%). At the same time, 76% of consumers said they were extremely or very concerned about the possibility of having their personal information stolen, and 60% said they feel powerless to protect their identity in the digital world.

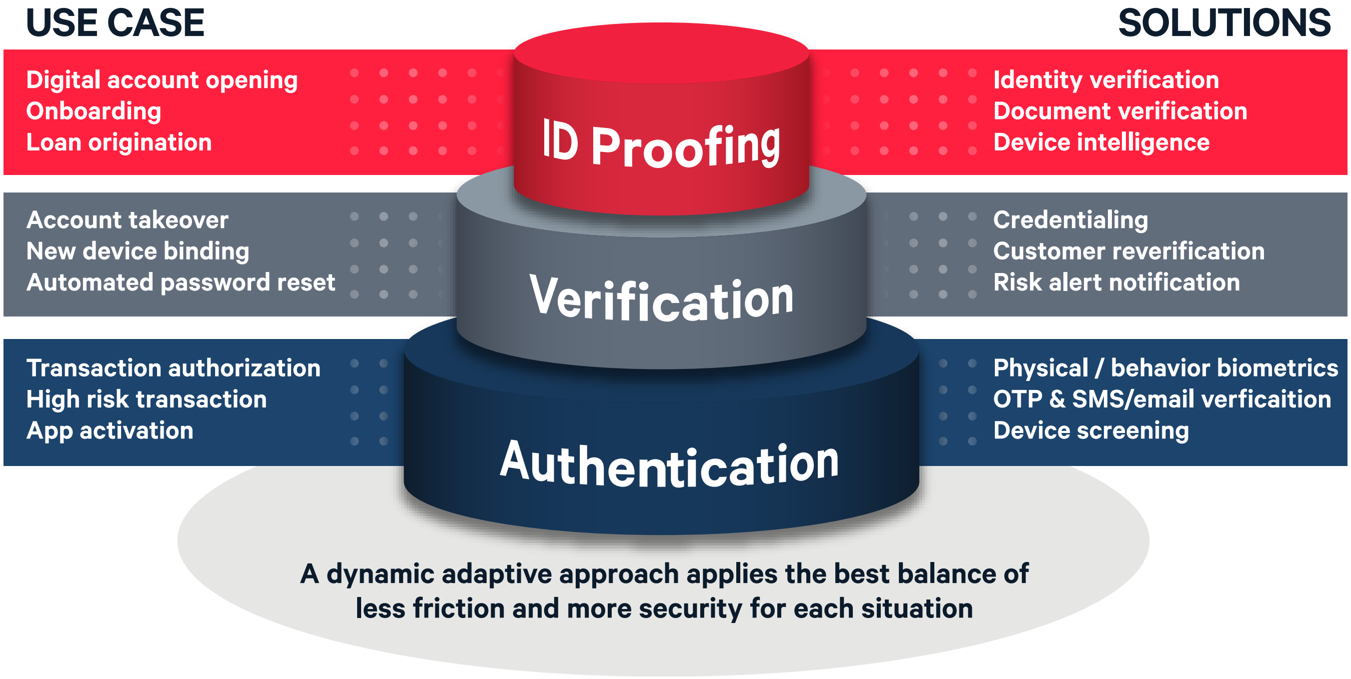
None of the studies I've seen in recent months indicate consumer preference for convenience above all else has changed. That's despite continuing concerns about security. In fact, a 2020 survey by Mitek partner Lightico found that only 66% of surveyed Americans believe their online transactions are secure or very secure. More than a third of us aren't so sure—and that's not good in an economy rapidly becoming digital-centric.

So finding the right balance between less friction and more security remains a top operational challenge. This is one of the reasons we're currently seeing widespread, rapid adoption of document-centric identity proofing solutions. They're relatively quick and easy for consumers to use, yet reassuring in regard to security. Typically, the process takes a couple of minutes for a user to submit pictures of the ID document and a selfie, followed by less than 5 seconds for the software to authenticate the ID and perform biometric face comparison.

Another advantage of document-centric identity proofing is that organizations have plenty of flexibility to adapt how they use it to consumer preferences in their markets and how they want to run their business. For instance, some organizations use document-centric identity proofing as the first step in onboarding. That way, information extracted from physical ID documents auto-fills digital forms—reducing friction and saving time for account applicants—and can be used by application fraud models and analytics performing background checks.

Other organizations start with data-centric checks—largely invisible and thus low-friction. They activate document-centric verification only when the identity can't be confirmed with a high enough level of confidence or when analytics find indicators of potential fraud.

Proving someone's identity should be revisited across the customer identity lifecycle and the flexibility to create the right balance of friction and security for different situations is becoming even more important as digital identity verification increasingly extends beyond onboarding across customer journeys. For example, months after onboarding, maybe there's a risky situation like a high-value transfer of funds or suspicious changes to account settings. Something like this could trigger a request from other security software, such as fraud detection analytics, for corroborative evidence. Identity verification might then prompt the user for a current selfie, compare it to the selfie and/or document image from onboarding (provided the user has granted permission for this information to be stored), then return the verification result to the requesting software.



USE CASE

SOLUTIONS

Digital account opening
Onboarding
Loan origination

ID Proofing

Identity verification
Document verification
Device intelligence

Account takeover
New device binding
Automated password reset

Verification

Credentialing
Customer reverification
Risk alert notification

Transaction authorization
High risk transaction
App activation

Authentication

Physical / behavior biometrics
OTP & SMS/email verficaition
Device screening

A dynamic adaptive approach applies the best balance of less friction and more security for each situation

I think there are going to be many places in customer journeys where identity verification can work with other software to reduce friction and increase security. The important thing right now is for organizations to choose software that's not only best-in-class for its purpose, but can cooperate as a solution layer on identity/security platforms.

These emerging platforms provide orchestration across components and enable organizations to set up decision rules, triggers and thresholds that determine what happens when. They make it possible to thread digital identity verification through the entire customer relationship in a manner that is adaptive and contextual. Each "stitch" taken has the perfect tension of friction and security.

Trust is emerging as the primary enabler of business growth

There's vast potential for new digital products and services to benefit both consumers and providers. But realizing that potential depends on our ability to make them safer from fraud than they are today. And that depends on consumers trusting enough to share their information.

At the moment, that trust is anything but a sure thing.

In the financial services, according to the 2020 Accenture Global Banking Consumer Study, customers' trust in their bank's ability to look after their data fell from 51% to 37% the two years prior to the pandemic. Interestingly, customers said they trusted their bank's ability to look after their long-term financial wellbeing even less—it fell from 43% to 29%.

That trend continued during the pandemic year, with the annual global Edelman Trust Barometer finding an additional 5% drop in trust for financial services from 2020 to 2021. Looked at over ten years, however, the barometer charts an 8% gain in trust for financial services vs. a 9% loss in trust for technology.

These numbers are problematic. Falling trust in recent years is bad news for banks at a moment when they're trying to expand digital offerings, including highly trust-dependent advisory services. Low trust in technology could also make it challenging for banks trying to move consumers to technology-intensive products and services.

In fact, lack of trust could slow overall growth of new digital economy business models and opportunities. A 2020 survey on European consumer attitudes toward Open Banking and payments by Strategy&

(part of the PwC network) found that despite increased interest in cashless payment methods since the pandemic, only 20% of respondents were willing to provide personal and financial data that could be shared with third parties. "Skepticism about security" is putting drag on Open Banking initiatives, say the report's authors, "slowing down the opening of the financial sector."

This issue of third parties is also starting to affect ecommerce, where until recently most shoppers haven't thought too much about what was happening with their data. Some recent studies suggest that one of the main reasons e-shoppers abandon signups is concern that their information will be passed on to third parties.

How do companies go about building consumer trust amid turmoil and change? One way is to realize that trust is a process, not an event. That's the key message of The Digital Trust Report 2021, a joint project of Mitek and 11FS, the challenger consultancy. The report provides a practical framework for implementing trust-building business processes.

Trust in facial biometrics

Many consumers are suspicious of biometrics in particular. Much of the concern is about facial recognition in one-to-many searches, such as those being done in airports or by law enforcement.

Last December, responding to worries about invasion of privacy and potential for biometric surveillance, Massachusetts moved to ban the use of the technology in policing, except for certain emergency situations. The same month, New York Governor Cuomo put a moratorium on the use of facial biometrics in public and private schools while the state conducts a study of the technology and its appropriate use. Other states in the US, including Virginia, Washington, Minnesota, Oklahoma and Florida, are adopting or considering their own restrictions. Sweden's data protection authority fined a local police department for unlawful use of facial recognition software. The European Commission is in the process of considering a ban on it in public places.

We'll have to see how this all develops—the danger is, of course, that companies will have to navigate a patchwork of regulations to do business regionally, nationally and globally. What we need is more informed regulation, standards that can be widely adhered to and full transparency by both providers and user organizations. I'm optimistic that we will get there socially, legislatively and technologically.

Biometric breaches and deepfakes

In 2020, the pandemic wasn't the only long-dreaded event to occur. We also saw a major breach of biometric data. The target was Brazilian biometrics company Antheus Tecnologia, which was storing unencrypted binary data representing 76,000 fingerprints on an unsecured server.

Also, in September 2020, the US Department of Homeland Security reported that inadequate safeguards the year before by Customs and Border Protection (CBP) had led to "a major privacy incident." Without authorization, a subcontractor had copied facial biometric data from the CBP's Vehicle Face System trial. The subcontractor's server was then hacked, and some of the data was subsequently for sale on the dark web.

Biometric data is in demand on the dark web partly because it can be used with AI algorithms to create deepfakes that look and sound like real people. To counter this rising threat, it's critical, of course, to better protect biometric data in the first place. Because biometrics can't be changed, stolen biometric data can cause lasting problems. Good reason not to over-rely on biometrics—and find ways of securely associating it with other types of identity verification information.

Organizations should also make sure the face comparison software they use in identity proofing includes certified liveness detection. Best-in-class solutions include both passive detection (captured in a single frame, so fraudsters aren't alerted it's even going on) as well as active detection, where users are asked to make certain movements such as blinks or nods. And because sophisticated deepfakes are getting better at spoofing common movements, identity proofing face comparison must continue to evolve to guide users through less predictable live actions.

Use of facial biometrics in one-to-one image matching, such as for onboarding, is much less controversial. Still, consumers are hesitant. A 2020 study by Mitek and PYMTS found that only one-third of US consumers are comfortable providing biometric information such as photos for facial recognition, fingerprints or voiceprints. That number rises to over 60%, however, when consumers are assured their information will be protected and won't be shared with third parties.

So organizations using facial biometrics for identity verification need to pay strict attention to keeping customer data private and secure (see the sidebar "Biometric breaches and deepfakes"). We also need to pay attention to the potential for discrimination.

A 2019 report from the US National Institute of Standards and Technology (NIST) found that some face comparison algorithms had a false positive rate (incorrectly matching two images of different faces) 10 to 100 times higher for African American or Asian faces than for Caucasian faces. In real-world use, that's a security problem, since a positive match means the applicant—possibly a fraudster—would likely be onboarded.

NIST testing also found that female and younger faces tended to have higher rates of false negatives (failing to match two images of the same person). That's a discrimination problem, since a negative result means the applicant would likely not be onboarded.

The accuracy of face comparison algorithms is improving rapidly, as the NIST report acknowledged, and we certainly need to continue making them better. Meanwhile, organizations should be sure the face matching solutions they implement use only top-performing algorithms—those achieving less than a 0.005 difference in face matching results across race/ethnicity and age demographic groups in the NIST Face Recognition Vendor Test (FRVT).

Trust in behavioral biometrics

Another type of biometrics where there's also rising concern, although it hasn't yet risen to the level of widespread public consciousness—is based on behavior. Behavioral biometrics identify us through patterns in our online activity (like habitually visiting certain websites or frequently making certain online transactions) and how we move our digital devices (like pressing, swiping, scrolling, typing and moving a cursor).

While identity verification has traditionally been performed using *something you know* (like a password or answer to a challenge question), *something you have* (like a document or mobile device identifier) and/or something you are (like a fingerprint or voiceprint), behavioral biometrics are based on something you do.

And we're talking, potentially, *millions of somethings you do*. That's because sensors in phones and code in mobile apps and webservers are picking up this information all the time—almost entirely without our knowledge.

The upside: Because we're unaware of this constant data gathering and analysis, it's a zero-friction identity verification method. As such, it's being promoted by advocates as the best way to get to password-less access as well as to improved security, since all of the data points being amassed and combined greatly increase the difficulty for fraudsters.

This approach is also seen as enabling zero-trust security, where our identities are, essentially, being continually verified. Providers like CrowdStrike offer zero-trust security solutions for enterprise networks. Unlike the traditional approach to network security, which has been "trust but verify," zero-trust requires all users to be authenticated, authorized and continuously validated in order to access enterprise resources.

Conceptually, zero-trust in the enterprise world and the consumer world are similar—except that in the enterprise world we know who is constantly collecting information about us. In the consumer world, we don't. Nor do we know what purposes other than identification they might be using our information for.

If you think about it, this trend is an expansion of what I discussed before about businesses connecting the dots of customer activity across all products and lines of business. Companies are creating dynamic profiles of highly condensed information, ideal for real-time AI/ML. The natural trajectory of such developments is to incorporate more and more external data from the expanding range of available sources. And, as I said, it's pretty much inevitable that these data-driven insights are going to be applied to a wide range of decisions and interactions—not just identity verification, but marketing, credit eligibility, debt collection and so on.

It's important to realize that the ML algorithms used to feed some of these profiles aren't engineered the way algorithms that assign credit scores are, and use of them isn't regulated the way credit scoring is. Instead of being supervised by data scientists and trained on historical data, they learn on their own in real time from current data. While there's tremendous upside potential for both businesses and consumers, there are also dangers. It's a little bit Wild West out there: Deloitte Tech Trends 2021 says some retailers expect to soon be using "emotional AI"—algorithms that determine mental state and intent.

Now think about what the trend could mean as it goes big. The New York Times Privacy Project did just that. They had one of the paper's columnists engage in normal, everyday web research and browsing, logging his activity as well as all the webservers that tracked him and the "staggering" amount of data they obtained. Most disturbing, they discovered one of the tracking servers had issued the columnist a 19-digit identifier number, which was shared with nearly a dozen other trackers and advertisers, and used by eight different sites!

You may have a personal identifier number you don't know about, but merchants and websites do.

An identifier number of that sort is likely tied to digital profiles. And these profiles are likely being used not just to identify us (Is this Steve Ritter?), but to characterize us (What kind of person is Steve Ritter?).

There's no transparency—not only are we unaware we've been assigned these numbers, but we don't know what they say about us. Nor do we have any reason to trust issuing organizations. (In fact, we don't even know who they are.) There's no control because we're certainly not given the choice of whether or not to provide this number and the data behind it to websites, vendors and other organizations.

Recently we've seen some major steps toward giving consumers more data privacy and control over how their information is used. There's Google's March 2021 announcement that it will stop selling ads based on individual consumer browsing data is a step in the right direction. And in April Apple added an App Tracking Transparency tool to iOS, which now gives users the option of granting or denying tracking permission to specific apps. We'll have to see how this works out—the devil is in the details. As the Washington Post reported in January 2021, another new Apple policy requiring a "privacy label" on App Store products, could mislead consumers. A blue checkmark indicates "Data not collected," but Apple was not verifying vendor claims at the time of the article, and when the Post's technology columnist spot-checked a couple dozen blue-checked apps, he found at least half of them were, in fact, collecting and sharing data.

(Meanwhile, the blue checkmark is reminiscent of the Twitter blue checkmark, discontinued in 2017 and being reinstated in 2021. That mark, an indicator of identity verification, was widely misinterpreted as an implicit endorsement of Tweet content.)

I'm sure you've guessed that I'm in favor of regulations that would require transparency as well as of technologies, like blockchain distributed ledger, that could increase consumer control. With these in mind, I'm optimistic about where behavioral biometrics are headed and the value they will ultimately bring to consumers and businesses.

“Who are you?” is a question of rising consequence as the information age lasers in on understanding individuals at scale

I started The Future of Identity with this seemingly simple question. I’m ending this sequel to that paper with the same question, although it hardly seems simple anymore.

“Who are you” still somewhat depends on who’s asking, as most of us have different digital identities for the various online sites and providers we interact with. But with organizations selling and sharing identifier data and more places inviting us to “Connect with Google” or Facebook or LinkedIn, that’s changing. With it, the anonymity of the early web is evaporating.

The bonanza of big data used to be about analyzing it to understand markets, demographic groups and population segments. That’s still attractive:

In February the Wall Street Journal reported “a group of major hospital systems is launching a company to pull together and sell access to anonymized data on their millions of patients for uses including research and drug development.”

What’s even more attractive about big data today, however, is the opportunity it provides to extract insights about individuals—at immense scale. Consider all the mobile health apps many consumers allow to capture detailed, extremely personal data. A 2019 study by University of Toronto researchers, published in the journal BMJ, looked at 24 such apps, finding that 19 shared user data. There were 55 unique entities receiving or processing this data, including developers, parent companies and third-party service providers. “Little transparency exists around third-party data sharing, and health apps routinely fail to provide privacy assurances,” concluded the report authors.

If tech providers can’t be fully trusted to keep our private data private, how about government agencies? Are consumers going to trust the digital ID-based “immunity passports” currently being rolled out or considered in some countries? And what about the 2021 Davos Agenda discussion on digital identity, which includes the idea of “community vouching models,” where activities like paying bills regularly, giving blood or volunteering could be used to verify identity? Could such an approach veer toward China’s social credit system? Is all of this making you feel a little queasy?

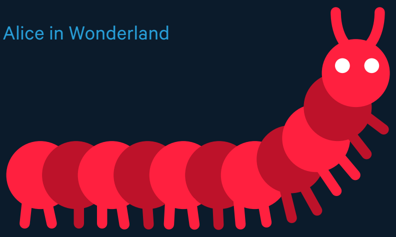
Thomas Koulopoulos, founder and chairman of the global futures think tank Delphi Group, is feeling both queasy and elated. In his book Revealing the Invisible, he says identifying and understanding the behavior of individuals (not only people, but machines, IoT devices and other entities) “is the killer app of the 21st Century.”

While acknowledging that the risks are as huge as the opportunities, Koulopoulos makes a good case, in my opinion, for why we can’t back up

“Who are you?” said the Caterpillar.

“I—I hardly know, Sir, just at present—at least I know who I was when I got up this morning, but I think I must have been changed several times since then.”

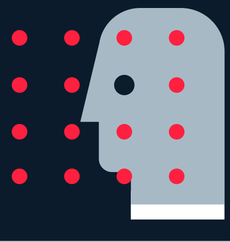
from Lewis Carroll’s Alice in Wonderland



out of the rabbit hole—we have to go forward. Understanding individual behavior, he says, is the only way we can cope with continued population growth and support developing countries where about a million people a week are emerging from poverty to join the economic mainstream. It's our best hope for responding effectively to emergent complex systemic changes, such as pandemics or environmental dominos tipped by global warming.

> *"How Behavior Became the New Global Currency"*
>
> *"The cloak of demographic anonymity has been lifted forever. Marketing is no longer about understanding a market segment; it is about understanding you."*
>
> Thomas Koulopoulos, *Revealing the Invisible* June (2018)

We can't slow down, but we can smarten up



Digital identity is at the very core of the new world we now find ourselves in. If we can't back out of the rabbit hole or slow down accelerating change, we can at least get a whole lot smarter about how we earn and keep consumer trust. It has to be top-of-mind in every implementation of identity-related technologies. People, after all, are not IoT devices.

Some of the changes we need to make are in technology implementation. There are good models being put forward, including the World Wide Web Consortium (W3C) Verified Credential Data Model and draft specification on Decentralized Identifiers. New concepts such as KERI (Key Event Receipt Infrastructure) are being explored to make decentralized identity management more feasible.

Some of the changes we need to make simply involve better communication. Mitek's research with PYMTS found that explaining to consumers in an easy to grasp way how their data will be used is a major trust builder. Yet a surprising number of financial services, online marketplaces and e-tailers today aren't doing it. We can fix that relatively easily. Time to start posting better signposts in Wonderland.

Tell us what you think.

Share your ideas, observations and experiences here.

Mitek

This document is for general information purposes only and is not intended to be and should not be taken as legal and/or regulatory advice on any specific facts or circumstances. All information provided in this document is provided "as is" without warranty of any kind, whether express or implied. Contents contained in this document may not be quoted or referred to for any purpose without the prior written consent of Mitek or its affiliates.