identiq

How Providerless Technology is Changing the Way We Validate Users Online

THE PAYPERS   ONE WORLD IDENTITY   ENTRÉE CAPITAL

Contents

1 How Providerless Technology is Changing the Way We Validate Users Online

“On the internet, no one knows you’re a dog”
Peter Steiner, The New Yorker, July 1993

On the internet, no one knows if your teenager has “borrowed” your credit card, no one knows if that online dating profile is a real person, and no one knows if that property you’re renting for a weekend away actually exists.

Trusted identities or not, our digital interactions have become a vital and inextricable part of our everyday lives. We want the convenience and the added scope and scale the internet has brought us. What we need now is security as well as convenience. Companies and consumers crave trust.

The great challenge for online businesses is: How do you trust someone you don’t yet know?

It’s a pressing problem. While the user on the other end of your onboarding process or transaction isn’t likely to be a dog, they might well be a criminal. One report found that 13.7% of all sessions are attacks[1] and Nilson reported that fraud losses worldwide reached $27.85 billion in 2018, and are projected to rise to $35.67 billion in five years.[2]

With those kinds of numbers in play, fraudsters have every incentive to become organized, professional and effective. And they have. The most successful are the hardest to catch, with the greatest motivation to keep finding new vulnerabilities and ways around new defenses. Smart fraudsters come to your site with a clean history, with no links to past nefarious activity - their IP, device, email, and phone will all have good reputations. How do you know whether to trust someone you don’t know?

The answer, often, is that you don’t. Companies feel they can’t afford to get it wrong - so they err on the side of caution. That’s why losses due to false declines, which already far outstrip losses from actual fraud, are predicted to grow to $443 billion by 2021.[3] That’s even more alarming than the revenue lost to criminals.

There’s a limit to what one fraud team, in a single company, can do on its own. When it comes to new users and new accounts, they’re always working with their hands tied behind their backs. They don’t know this user. So how do you trust someone you don’t know?

You work with other companies, who do know them. You go providerless.

2 Why Collaboration is Crucial for Fighting Fraud

By Karisse Hendrick

Karisse Hendrick's experience in fraud prevention comes from time in the trenches managing fraud for a leading retail rental company, developing training courses for numerous companies and for the MRC as in-house industry expert and program manager, and intensive consulting work with merchants from diverse industries. She also writes reports and articles to help merchants keep up with new trends, runs a consultancy business and hosts the popular podcast The Online Fraudcast.

A little over a decade ago, I was managing the fraud department for a brand new online business model. I quickly learned I'd never find all the knowledge I needed within my own company. Joining a trade association and attending conferences enabled me to introduce new strategies to my leadership. It helped me fine-tune our fraud prevention, reducing both fraud losses and mistakenly rejected sales.

As my career evolved, I followed my passion to support online merchants and continually foster education and collaboration opportunities for hundreds of online companies worldwide. Education and collaboration are at the heart of everything I do.

> No company can handle fraud effectively in silos. As I keep saying, "the bad guys work together, so should we!"

Working on our podcast with former cyber-criminal Brett Johnson I've learned even more about how criminals work. As with online businesses, most criminals specialize in a particular industry or skill. They're judged on their contributions to the group. Criminal networks that share everything from their skills to detailed tutorials are strong because of the information they share.

I've introduced fraud professionals at competing enterprise companies (competitors in every arena except fraud prevention) and seen the relationships blossom. I've helped create industry-focused groups (e.g. event ticketing, travel, and online gaming). The results are nothing short of magic. It's even the basis for a powerful support structure - since fellow leaders at competing companies understand just what you're experiencing.

Moreover, your competitors are probably seeing the same new attacks you are. It might even have migrated to you after they beat it last month. Sharing what works helps everyone improve their own strategies. Knowing more about the big picture helps you make better decisions. But until now, we've had nothing to combat the lightning speed at which fraudsters steal and share stolen data. As a merchant I spoke with recently put it, "Shared blacklists are a great way to catch last month's fraudsters."

That's what grabbed me about providerless technology. It gets us out of the cat-and-mouse game in which fraudsters win if they can use stolen, synthetic, or made up identities faster than companies can catch them. Instead, providerless technology allows us to focus on validating the majority of users, who are already known to be trustworthy by other companies and services. It's a whole new level of collaboration - especially when coupled with a fully private network, which gives merchants all the benefits of going providerless without the risks of sharing and centralizing actual data.

Providerless technology allows us to focus on validating the majority of users, who are already known to be good by other companies and services.

It's a whole new level of collaboration - especially with fully private networks, without the risks of sharing and centralizing actual data.

It's been a while since we've seen anything game-changing in fraud prevention technology. We've been fine-tuning known methods for a while now. There's nothing wrong with that, but I'm not sure it'll take us all the way to the success that only comes from working together. I have a feeling that providerless might be the next leap we all need - as long as merchants are willing to truly work together. Ultimately, the willingness to collaborate with your peers is what really makes the difference.

3 Why Companies are Looking for Alternatives to Provider-Based Collaboration

> *"Data, data, data! I cannot make bricks without clay!"*
>
> Sherlock Holmes in The Adventure of the Copper Beeches by Sir Arthur Conan Doyle

On a day-to-day level, **fraud prevention professionals need to know which users and details are legitimate or fraudulent - even if they've never seen them before.** To do that they typically use external, extra sources of data - utilizing third-party data providers directly, or using fraud solutions and services that utilize these providers.

Providers aggregate data from many sources - partners, publicly available information, purchased data etc. - and use it to answer queries about users. One of their most important sources of data is the content of the queries themselves. Providers use this data to validate future requests. Companies using the service both pay for the service and (often unwittingly) contribute information about their own users. The end-user typically has no idea that's happening.

There's some simple logic behind the third-party provider approach. Aggregate enough data, the logic goes, and a provider will eventually have "seen it all." Companies can draw on that knowledge to make better risk decisions. To quote Kettering's Law, "Logic is an organized way of going wrong with confidence." Inevitably, there are problems with relying on providers.

The Disadvantages of the Provider-Based Approach

- **Data Freshness.** To validate identities, data must be fresh, reliable and accurate. But providers don't get data directly from consumers, and struggle to keep up with users' new jobs, addresses, devices, IP addresses, and even names - not to mention track which have been exposed in a breach.

- **Data Reliability.** With the provider model a single weak link in the information chain (either unintentional or deliberately misleading) poisons the database with confusing or irrelevant data that's unlikely to be removed or rectified. Companies relying on the provider never know where the data comes from, how many hands it has been through, or how reliable the source is.

- **Data Completeness.** Third-party providers only see a small part of a user's online life. Since it costs money to use these providers, companies only verify when a user's details change. So providers never see a user's holistic typical behavior (like the purchases they make, the rides they take, the subscriptions that run from month to month) because companies see no need to verify these interactions. Moreover, the external sources of information they use to supplement their databases are often skewed towards certain segments of the population, such as people with credit scores, leaving others out entirely.

- **Data Privacy.** The provider model works on the basis of companies sharing their users' data with third parties. But, while consumers might have chosen to trust you with their data, can you reasonably interpret that as an assertion that they're happy for you to send their data to Equifax?[4]

Provider-based methods and tools have been useful for decades, but it's not hard to understand why companies are now exploring alternatives. **Shifting privacy attitudes and legislation, large scale data breaches, the increased sophistication of the online criminal ecosystem and the growing pressure on many fraud teams to prove they're working to avoid false declines have all combined to make the third-party provider system seem inadequate to the task.** At the same time, advances in communication and technology have meant that comparing data points can happen almost instantaneously and costs virtually nothing.

4 Providerless Technology: The Latest Evolution of Collaboration

“When you need to innovate, you need collaboration”

Marissa Mayer, American businesswoman and investor, former President and CEO of Yahoo!

With the new technological developments of providerless options, whether the specific technology being used is blockchain, F.A.I.R., or one of the self-sovereign platforms, the data is fresh, holistic and not shared with third parties. When companies go providerless, they cut out the middleman of a provider (or several) and instead collaborate directly, peer-to-peer.

The Interesting Advantages of Going Providerless

- **Data Freshness.** Going providerless means companies are always working off fresh information that comes straight from the end-users themselves. Users interact with their favorite companies frequently. With providerless options, stale data disappears.

- **Holistic.** A providerless network gives a far more holistic understanding of users’ activities and how they’re using their data. Users interacting with sites and apps prove themselves continually and invisibly, keeping up subscriptions and using email addresses and so on. So a company on the network can trust them, even the first time they visit.

- **Catch Attacks Quickly.** Fraud rings and bad actors attempting to use the same stolen details on multiple sites also show up quickly and transparently on a providerless network. Since fraudsters typically do target many places at once or in quick succession, that transparency is very valuable in identifying attacks speedily and keeping up with data that's been compromised.

- **Data Privacy.** Providerless solutions do not create or require a huge, centralized database into which companies pour precious user data. Such databases, of course, are very attractive targets for criminals. Instead of the database model, each company remains in control of their own users' data.

Providerless technologies are emerging partly out of new technological advances and partly out of the growing public and regulatory interest in limiting the exposure of consumer data to third parties. **Companies using providerless technologies are hoping to get more accurate results, get ahead of the privacy shifts, and future-proof their identity validation methods against any further legislative developments.**

It's also a practical business consideration. 85% of US consumers said they wouldn't do business with a company if they had any doubts as to whether their data will be kept safe, and 71% said they'd stop doing business with a company if it gave away their sensitive data without permission.[5] No one wants their team to be on the receiving end of one of those statistics.

5 The Fraud Challenge with Fast, Frictionless Payments: Collaboration Might Be the Answer

By Mélisande Mual

Mélisande Mual is the publisher and owner of The Paypers, one of Europe's leading sources of news and analysis for professionals in the global payments and e-commerce industry. She has become a prominent voice in the payments, risk and fintech industries. Prior to The Paypers, Mélisande held several leadership positions in global media and telecommunication companies.

The world of global payments is increasingly open to innovation and technological sophistication. At the same time, we are currently witnessing escalating fraud attacks from increasingly hi-tech criminals armed with the 14.7 billion(!) records which have been breached since 2013.

This is the backdrop against which we need to see global innovations in the realm of payments - for example, the move to Real-time Payments. By shrinking the transaction's processing window, the time to detect and act on fraud is greatly diminished. This creates the need for a new approach to risk assessment. Moreover, we see a global move to open banking, and data sharing is at the heart of this global movement. So what do fraud teams need to know?

Be Clear About Categories

A widespread cliché is that there is no silver bullet to fight fraud. The industry is engaged in a technology arms race against the bad guys; regulation always comes late; and the industry struggles to meet implementation deadlines (PSD2/SCA). Data sharing initiatives among merchants and financial services in particular face GDPR restrictions. And lastly, consumers (and employees) are often the weakest link in the line of defense.

The ways in which the e-commerce and banking industries can analyze their defense can be roughly divided into the following categories:

- Technology (AI, Machine learning, biometry, homomorphic encryption, secure multiparty computation)
- Rules and regulations (PSD2/SCA, 3DS 2.0)
- Data sharing and industry collaboration
- Consumer education

Here I will focus briefly on some best practices of data sharing in e-commerce and financial services, because this is an area that can help move the needle and yet which is often given less attention.

Industry Collaboration is Evolving: From Best Practices to Data

Fraud prevention professionals have traditionally been particularly strong when it comes to industry collaboration. Knowing they're all fighting the same criminals, fraud fighters are often willing to work together even if they're from rival companies.

The Merchant Risk Council is a particularly good example of this. The MRC launched in 2000 shortly after the internet boom, when merchants came together to talk about online fraud problems never experienced before. It began as a passion project built by a team of dedicated volunteers, all busy with day jobs and working on the MRC on nights and weekends. Discussing evolving fraud tactics and sharing best practices has, over time, expanded to facilitate data sharing among member merchants.

Similar levels of cooperation are equally vital in payments and banking. New channels (APIs) and instant payments create more vulnerabilities and thus great opportunities for fraudsters. New fraud cases will occur and therefore industry collaboration is key - to trace vulnerabilities at an early stage and to share best practices.

The Apparent Challenge: Data Sharing vs Privacy

For all its advantages, data sharing is not without risks. It has implications for data privacy (GDPR), data security, and competition. In Europe we have not (yet) seen data sharing initiatives and industry collaboration initiatives in financial services being launched to address fraud prevention.

New technologies, called Privacy Enhanced Techniques (PET), might come to the rescue. Recently the World Economic Forum released a whitepaper,"The Next Generation of Data-Sharing: Using Privacy Enhancing Techniques to Unlock Value."[6] In this whitepaper, new technologies (differential privacy, federated analysis, homomorphic encryption, zero-knowledge proofs, secure multi-party computation) and their potential benefit for financial services are laid out in detail.

I hope to see broad implementations of these techniques to open new approaches for fighting fraud and financial crime, without sacrificing privacy. Done well, it could be game-changing.

6 Providerless and the First-Party Data Advantage

“We all need a past - that’s where our sense of identity comes from.”
Penelope Lively, winner of the Booker Prize and the Carnegie Medal, and Dame of the British Empire

What if... You were an online business that knew which visitors were good customers - even the first time they came to your site? You’d be able to provide the ideal, seamless, friction-free experience you work so hard to facilitate.

Identifying Good Users Right From the Start

Identifying the good guys isn’t the same as being good at finding fraudsters. Think about airport security. Almost all passengers are good. Only a tiny minority are dangerous. Yet the cost of a mistake is so high that checking for this tiny minority is important enough to inconvenience everyone else.

For most people, every time you fly you need to wait in a long line, take off your shoes, remove all electrical items from your bag, take your jacket off and so on, before being allowed to board the plane. But if you’re a TSA pre-check passenger, or a Trusted Traveler, you go through a very thorough one-time check. You can then skip the long queues and extra steps every time you fly in the US.

Imagine if almost everyone went through the approval process. Good passengers would breeze through the airport. Only a small number of passengers who were new and unchecked, or suspicious in some way, would need to be thoroughly checked. The security team would then be able to spend their resources on these individuals.

How it Works with Providerless Technology

It’s the same when you go providerless. You’re not looking for criminals and trying to pick them out of the crowd. You see the legitimate customers, those who are vouched for by your peers, before you even start thinking about fraud. They get a fast, frictionless experience every time - which is just as well, because unlike with airports, online customers who aren’t pleased with their level of service simply go elsewhere. Of course, as well as increasing your approval rates and likelihood of customer retention, this approach also makes fraud prevention much easier.

Here’s the thing about first party data: Real users have real histories that reflect their real lives. That’s exceptionally difficult to fake. **And here’s the thing about providerless technology: the knowledge you can draw on is whatever the community knows. You benefit from the wisdom of the crowd.**

If you’re on a providerless network that can see real users’ patterns of data and interactions, and other companies trust those users, then you can too - even if you’ve never seen them before.

When companies work together, no user is a stranger.

Of course, there will be a small subsection of users who are in the “gray zone” - when not enough is known about them, or their accounts may have been compromised - and some judicious friction might be needed to validate their true identities. But, again, with providerless technology you can draw on whatever the community knows.

So once a new user or their new details have been validated two or three times, you have consensus. That consensus reflects and creates trust, enabling future friction-free experiences.

7 Providerless: Solving the Unknown Unknown

By Raphael Lawson

Raphael Lawson has been fighting fraud in diverse industries for fifteen years. As Group Head of Fraud at The Hut Group, he has developed the company's fraud protections to support its massive growth, while at the same time guarding against loss from fraud. He oversees predictive research, fraud management tools and systems, false positive prevention and chargeback management for THG's varied brands. Raphael has a Masters in Applied Criminology.

“It’s easy to stop all fraud. Just don’t make any sales.” This truism in our industry always gets a wry smile, because it’s so true. The challenge of fraud prevention is not blocking fraud; it’s blocking fraud without turning away good business.

As we all know, the potential cost to the business of being risk-averse is higher than the amount generally lost to fraud. We’re always stuck between a rock and a hard place. At The Hut Group we take this particularly seriously because we focus so much on providing an ideal customer experience. False declines are the absolute opposite of what we’re trying to achieve.

> The reason I became interested in the providerless trend was not actually as a fraud fighting tool, per se. What drew me in was the hope that providerless would be able to help avoid false declines.

After all if a network can develop a reliable consensus about good customers, based on their histories and their ongoing interactions with numerous sites and apps, then maybe we could protect those customers from the annoyance and frustrations of a false decline.

I'm certainly not dismissing the importance of preventing fraud, which remains the core of my role. But in my opinion, our industry's great challenge for the coming decade is going to be dealing with the problem of false declines. To do that, we should be looking beyond current practices to see what new ideas and technologies may be able to benefit us, our companies and our customers.

8 A Providerless Network Sees the Big Picture

By Noam Naveh

Noam Naveh is an identity and payment fraud prevention consultant with 15 years of experience in tackling fraudsters online. He helps payment providers and online merchants and marketplaces deal with the ever-increasing challenge of online fraud. Prior to his consulting business, he spent four years at PayPal's risk management department, working on technology infrastructure, real-time decisioning, and data sources. Before that, Noam was the Chief Analyst of Fraud Sciences, the startup famous for pioneering accurate online fraud detection, which was acquired by PayPal in 2008.

In my engagement with clients and when I meet colleagues at conferences, we often lament the lack of collaboration between companies on fraud prevention. To us fraud fighters it makes perfect sense: fraud has become highly sophisticated, collaborative and organized while companies continue to operate in silos, reinventing the wheel time and again.

But until the advent of providerless technology such as F.A.I.R., collaboration on data - which is at the crux of fraud prevention - was impossible. I know this first hand, because I recently participated in a series of meetings between companies in an attempt to bring about such collaboration. This effort ultimately failed: business leaders were reluctant to work with competitors and lawyers were justly worried about privacy.

> **The almost sci-fi ability to consult the entire "community's user database" without ever sharing user PIIs is immensely valuable for every online business.**

We know that someone out there has already approved a user that is new to us, or has already seen this user's new device. If we can spare the user an annoying identity verification process while preserving fraud prevention firepower for fighting real fraudsters, it’s a clear win-win.

On the fraud side, there’s some interesting math that proves why we need to work together. Behind every fraudulent transaction is an ROI calculation for the fraudster: when the gains from a successful fraudulent transaction fail to justify the time, money and effort the fraudster invests in them, they will give up. One of the best ways to increase the fraudsters’ investment is to require them to come up with a new identity, a new device and a new payment instrument for each and every transaction.

In practice, this is achieved using velocity checks that prevent reusing the same assets excessively. When a fraudulent attempt is detected, all of the assets are “burned.” Even when initial detection fails, we can still notice repeated use and stop the attack before it scales. Alas, all the fraudster needs to do to circumvent these checks is go to a different online store, where these assets have not yet been seen. With the abundance of online stores, the fraudster’s assets can safely be used repeatedly, maximizing their value. Consequently, what we need is a “velocity check” that is shared by all the major online businesses. This is one of the clear advantages a collaborative data network can provide. Companies that opt out of such a network will ensure the fraudsters achieve increased ROI.

Combining these capabilities with the ability to strongly identify and provide a great user experience to the trusted users is a one-two punch to the fraudster, and a huge leap in capabilities for any fraud fighting organization.

> *Companies need to work together against fraud. It's just math.*

Beyond the immediate value, I think that data collaboration among online merchants, marketplaces and service providers is a very promising development. It may help us, one day, to tackle challenges that are quite intractable today. As an example, consider “chargeback abuse”, where buyers falsely report to their bank that, say, their new Nike Airs were actually an unauthorized purchase, even as they post selfies of themselves wearing them to their Instagram followers.

This phenomenon, according to multiple reports, is on the rise, and I’m constantly hearing people in the risk management community looking for solutions. It is a type of problem that no merchant can fight on their own, because even if they decide never to let this fraudster (yes, we should call them that!) shop at their store again, it’s not a real deterrent; the fraudster can repeat this trick at endless other stores. However, when merchants join forces, an effective management of this issue will one day be possible.

9 What About Privacy?

> *"Privacy—like eating and breathing—is one of life's basic requirements."*
> Katherine Neville, NY Times, USA Today & #1 Internationally bestselling American author

One of the reasons collaboration on a data level hasn't happened before is privacy. Companies have never wanted to share precious user data with one another for competitive reasons. Beyond that, the more consumers and regulators show that they care about privacy, the less appealing it is to risk sharing sensitive user data beyond standard practice.

The Problem With Privacy

Privacy isn't a feel-good issue anymore; it has teeth. From the legislative side, GDPR has already resulted in substantial fines for companies who were found not to have protected their users' data appropriately. From the consumer side, 83% say they would end their relationship with a company if they discovered their information has been shared without their consent.[7]

There's no doubt that the third-party provider model has issues from the privacy perspective. While fraud prevention currently benefits from anti-crime exemptions in GDPR and CCPA, **a system that is based on sharing sensitive user data with third parties no longer seems like a good way to practice business as usual - not least because of the question of trust.** A $30 billion retail company experiencing a material drop in trust stands to lose $4 billion in future revenue.[8]

Providerless and the Privacy Leap

But isn't providerless as problematic when it comes to privacy? The answer, as is so often the case, is: It depends. Sharing data freely between peers runs into the same difficulties as with third-party providers. Many providerless options, however, have chosen to incorporate elements of pseudonymity or, in some cases, full anonymity, as part of the structure of their network.

This is, in part, serendipitous timing. Providerless technologies have developed at roughly the same time that privacy considerations became mainstream. It has become natural for companies exploring this new approach to also explore creative ways to make their creation private.

There's also a business reason. Providerless networks that achieve anonymity are able to deal with particularly sensitive pieces of information, such as credit card ownership or bank account details. That expands the scope of providerless technology, and its potential impact. Additionally, of course, making privacy part of the offering gives providerless options an edge over third-party models, since they could become part of business' attempts to future-proof against legislative change.

10 Why Privacy is Crucial to Providerless

By Uri Arad

Uri Arad has been fighting fraud and fraudsters for more than a decade and has seen the fraud and identity challenge from diverse perspectives: product, risk, and R&D. Before he co-founded Identiq to create the solution he'd been dreaming of for years, he was the Head of Analytics and Research at PayPal's risk department.

Anonymity enables privacy. In my opinion, the providerless solutions that will really make an impact - and change the way we approach both identity validation and data sharing - will be those that have anonymity built in from the ground up. And I'm not talking about pseudonymity, since so many studies have shown how easy it is to link real identities back to pseudonymous data. Researchers from two prestigious universities in Europe found they could correctly re-identify 99.98% of individuals in anonymized data sets with just 15 demographic attributes.[9]

> What's necessary is real anonymity. And it's more possible than you think.

A Fraud Prevention Example

Take Identiq as an example. We store no sensitive personal data in our system. As much as possible, we think companies should avoid sending users' personal data to third parties; we don't want to be an exception to what should be a rule. With providerless technology, we can validate identities without having any privacy exceptions made for us.

All we supply is the network for connecting companies together. Each company keeps its own data, based on its first-party knowledge of the consumer; nothing is transferred, nothing travels. But members can validate users or data points against each other's knowledge base of users and data. We call this technology F.A.I.R (Fully Anonymous Identity Resolution).

For Identiq, this is both a guiding philosophy and an inherently pragmatic approach. The more data is copied, the less its owner can keep track of it, and the more vulnerable it becomes to abuse. We've all seen where that leads. We want to be part of the solution - not part of the future problem.

The Power of Leveraging Real Anonymity

With Identiq, real anonymity is the watchword. When a company sends a query to the network, no other company sees:

- The content of the question
- Who's asking
- Who's answering
- What the answer is

People often find this part difficult to wrap their heads around, which is understandable - it's ultimately down to mathematics and well-known, reliable, seasoned cryptography, which takes time to explain. But it's not difficult to make it more intuitive.

> *We want companies to be able to validate users' identities without ever sharing any sensitive user data. With providerless technology, it's possible.*

Imagine you wanted to see if you have the same birthday as a friend, without revealing your age. You could use a trusted third party. But how much do you trust them? Alternatively, you could roll some dice with your friend to get a random large number, and add that to your ages. You could tell that new huge number to a third party. You don't need to trust them - because they don't know the random number, you're not giving them any information. All they can do is tell you if it's a match or not. If it's a match, you know you have the same birthday as your friend. If there's no match, you know you don't - but you don't know what your friend's birthday really is, and they don't know yours.

The math behind Identiq is considerably more complex, but that's the basic idea (though with Identiq, only one side ever gets an answer). You don't have to trust anyone with your data. No one else ever sees it, and no one can copy or share or do anything with it. That means that you can validate more sensitive information, like credit card ownership or bank account owners - because without third parties in the mix, you no longer have to fear a malicious or accidental leak.

We want companies to be able to validate users' identities without ever sharing any sensitive user data.

With providerless technology, it's possible - and it strikes us as being better for everyone. In fact, it strikes us as F.A.I.R.

11 Cryptographic Multi-Party Computation: How to Eat the Data Cake and Keep It Private Too

By Ran Canetti

Ran Canetti is a professor of Computer Science at Boston University. The winner of many awards including the RSA Award for Excellence in Mathematics and the IBM Research Outstanding Innovation Award, Ran is also the director of the Center for Reliable Information System and Cyber Security. Additionally he is a Fellow of the International Association for Cryptologic Research and associate editor of the Journal of Cryptology and Information and Computation. Ran's PhD is from the Weizmann Institute of Science, and during his career he has been a researcher at IBM Watson Research Center, a research scientist at MIT, and a professor at Tel Aviv University. He's a highly sought-after speaker and recognized world leader in the areas of cryptographic protocols and information security.

Cryptography is an amazing conduit: It turns the inherent complexity of mathematics into mind-boggling methods for hiding, manipulating, and exposing information in ways that defy intuition… and yet work. Secure multi-party computation (MPC) is one such family of methods.

History of MPC

Already in the late 1970's, shortly after the invention of public-key encryption and digital signatures – which are the bedrock of all of today's internet commerce – cryptographers started asking themselves: Can a set of mutually distrustful parties, each holding a private piece of data, perform an agreed-upon computation on the union of their data, and make sure that everyone obtains the agreed-upon result of the computation and nothing else?

For instance, can two competitors perform a computation where they learn which one of them makes more money, without revealing to each other how much they actually make? (This is Yao's famous "millionaire's problem," one of the first that motivated this study.) Similarly, can two law enforcement agencies, each holding a secret list of suspects, learn which suspects appear on both of their lists, without revealing anything else? Can a set of colleagues jointly compute the average of their salaries, without disclosing their actual salaries to each other?

A rapid succession of inventions in the 1980's demonstrated that the answer to all these questions is, in principle, "Yes." Assuming the parties agree that they want to jointly compute some function of the (virtual) union of their respective datasets - they can.

> Using cryptography, there is a way for the parties to exchange messages that will allow each one of them to compute the desired function value, while exposing no private data beyond the result itself, and without trusting anyone else but themselves!

It's as if the parties had access to a magical "trusted party" that sees the private data of all parties, performs the desired computation, announces the results, and disappears. Furthermore, this holds, at least in principle, for any function whatsoever.

So Why Haven't We Been Using MPC For Decades?

As amazing as this ability sounds, it remained within the walls of academia for a couple more decades. One main reason was that the cryptographic mechanisms in use were highly inefficient, thus rendering this ability merely theoretical. Additionally, and perhaps more importantly, the fact was that the need for such solutions did not really present itself.

Around the late 2000's things began to change: First, the value of aggregated data became more and more crucial for applications. Second, the amounts of data that could not be shared due to sensitivity or privacy reasons skyrocketed as well. Third, the technology matured: Researchers developed significantly more efficient and readily available algorithms and even software packages for MPC in different contexts.

MPC: Helping Solve Today’s Challenges

Consequently, MPC solutions are becoming more mainstream and have already made some headlines. To mention one application out of many: In each of the years 2016-2019, some 120 employers in the Boston area (that together employ about 15% of the workforce) have engaged in an MPC for computing the average salaries of men and women at different stages of their career. (Sneak peek: The salary disparity between the genders is significant, and is not really improving. The good news is that at least we now know this for a fact – thanks to MPC technology that managed to make this endeavor compliant with the strict legal requirements regarding the privacy of employee salaries.)

In the context of identity management and fraud detection, MPC technology is a natural shoo-in: It allows companies to maintain their own local private customer databases, and at the same time get together with peer companies.

In the context of identity management and fraud detection, MPC technology is a natural shoo-in: It allows companies to maintain their own local private customer databases, and at the same time get together with peer companies. The connected companies can virtually pool all their customer databases in order to allow any or every company to match suspicious customer information against the entire virtually-pooled database – while respecting and preserving privacy and legal compliance regarding their own customer data.

12 Providerless and the Potential to Shake Things Up

By Ran Achituv

Ran Achituv, Managing Partner at Entrée Capital, has been part of the Israeli technology ecosystem for the past twenty years, working in fields ranging from strategy to M&A, P&L management, technology, and execution in both the corporate and defense intelligence markets. His experience includes founding the IDF's Satellite Intelligence Unit, senior roles with Israeli tech giants including Verint and Amdocs, where he was CTO, and even co-founding a number of startups himself. Ran has also been a lecturer at the Computer Science department of the IDC Herzliya, and holds an MBA from Kellogg.

Providerless technology is one of the particularly interesting emerging trends we've seen developing recently. It's exciting to see peer-to-peer solutions growing into their own, both technologically and in terms of market fit.

The providerless trend takes this one step further, bringing companies together to solve problems that used to be solely the province of third-party providers. We're starting to see enterprise companies move in this direction, and one of the interesting - and surprising - things about this trend has been how fast companies are willing to move along this path.

One of the interesting - and surprising - things about providerless technology has been how fast companies are willing to move along this path.

At Entrée Capital we've always believed in the power of collaboration. The business and expertise of a Venture Capital firm is to partner with the right young companies and provide the right guidance, goals and encouragement to make that partnership flourish for everyone concerned. At Entrée Capital we’re proud of our track record of choosing and supporting companies who help to shape tomorrow’s world.

I believe that this new technology has the potential to shake things up in a variety of industries, bringing not just technological innovation but a shift in the way things are done. It is my hope that privacy will be a cornerstone of this change, with providerless technologies facilitating a new approach to data privacy that will benefit both businesses and consumers.

> It's time to change our shared approach to data. Providerless is an excellent solution - using technology to change what is, effectively, a problem created by technology.

Some of that has already begun. It will be very interesting to see how the initial players influence what comes next. My guess is that the initial innovators will define the way the rest of the world uses consumer data. At Entrée Capital, we aim to work with companies who will make sure the change is one we all want to see.

13 The Linchpin of Digital Transformation

By Cameron D’Ambrosi

Cameron D’Ambrosi is an advisory principal at One World Identity, and hosts OWI’s State of Identity podcast, the premier podcast for the identity industry. Cameron applies a methodical approach to deriving identity industry market insights and intelligence. Prior to OWI, he was an Engagement Manager at Deloitte, combining a focus on streamlining customer experience with emphasis on compliance and efficiency. Cameron holds a B.A. in history from Fordham University.

In 2019, the total number of data breaches increased 17% from 2018 according to the Identity Theft Resource Center[10]. Data breaches are the result of an increasingly competitive and personalized digital economy, where almost any online activity - from buying groceries to searching for a new pair of sneakers - enables the creation of user data.

Identity lies at the core of how people engage online, not only with each other, but increasingly with services and sites as tailored recommendations, and seamless user experiences become the expectation. How we prove and verify identity online is the linchpin of digital transformation, and we’re witnessing the development of the underlying technology that will define the future of the global economy.

While current digital identities remain Balkanized, as technology continues to evolve, it will become more and more valuable for consumers to interact directly with companies, cutting out third parties as an additional place for data to be stored and collected. All this innovation and technology is continuing to move us along the curve, towards a world where consumers have more control over their identity and their personal data.

In OWI's 2020 Predictions, we anticipate an emerging wave of credential re-use. Technology like Federated Identity Management (FIM) and Single Sign-On (SSO) is the step bridging the current state of identity to the future of providerless technology.

> When identity verification is carried out using only first party data, companies can rely on validating against information that's always fresh.

Providerless technology means that consumers can gain an increased sense of assurance that their data is no longer routinely shared with numerous third parties. It's win-win for both enterprises and consumers alike, with demonstrable reductions in risk alongside tangible user experience benefits.

OWI was founded on the notion that identity is an industry in its own right - not just a subset of other industries. We expect to see this trend continue in 2020, as the need to comply with new privacy laws and adapt to user privacy concerns ushers in the next generation of innovative digital identity startups and technologies. We hope you'll join us on our journey in the quest to make identity better for everyone. Join us at KNOW Identity events[11] to learn more about digital identity, trust, and the data economy.

Providerless is win-win for both enterprises and consumers alike, with demonstrable reductions in risk alongside tangible user experience benefits.

14 How Providerless Technology is Changing the Way We Validate Users Online

> *“What seems today inconceivable will appear one day, from a higher standpoint, quite simple and harmonious.”*
> Max Planck, theoretical physicist, Nobel Prize winner who discovered energy quanta

Providerless technology represents a technological evolution, enabling companies to work collaboratively to solve problems that once required the involvement of third-party providers. But the technological aspect is not the most interesting, or the most relevant to the majority of companies and departments.

What’s really significant are the new options providerless creates with respect to data. **The ability to leverage consistently fresh, consistently holistic data could enable companies to move the needle on the level of service they are able to provide for their users.** It is this - the potential improvement in user experience, sales numbers and customer retention - that makes providerless stand out, and is the reason companies are beginning to evaluate providerless solutions, and are considering incorporating them into their arsenal.

The Changing Shape of Fraud Prevention and Privacy

For fraud prevention and identity validation, extra interest is felt because a network that throws good, legitimate users into high relief - rather than following the traditional approach of trying to catch malicious actors - represents a new direction in this competitive, high-stakes industry.

It is clear that privacy will be a key aspect in how providerless technology develops moving forward, and may also profoundly affect how willing companies are to make providerless options a part of their solution stack. It is too early to evaluate the different privacy possibilities in this very new field, but it is something companies should bear in mind when assessing the options available.

For fraud prevention and identity validation, extra interest is felt because a network that throws good, legitimate users into high relief - rather than following the traditional approach of trying to catch malicious actors - represents a new direction in this competitive, high-stakes industry.

Providerless technology has the potential to improve online experience for both consumers and companies, and to simplify efforts to make sure users' privacy is consistently respected and protected. That's an improvement in trust across the board. Paradoxically, providerless achieves this by removing trust from the equation. Where anonymity and privacy are incorporated into the very structure of a network, trust between parties becomes unnecessary. If no sensitive data is being shared, companies no longer have to worry about whether a particular organization deserves to be a "trusted partner."

Leveraging a Framework of Trust

It is the trust factor, more than anything, that has caused large global companies to start exploring providerless and what it can do for them. It is the trust factor that has transformed providerless options, in the last year or so, from being an interesting experiment to becoming a significant trend with traction and the potential to change how things are done.

When companies can trust good users through a providerless network, they can provide the kind of service that itself engenders trust, both in terms of experience and approach to privacy. Providerless technology offers the ability to do this without having to trust any other company or third party in the process. It's easy to see why some companies are thinking that this sounds better for their business, better for their users, and even best practice, too.

Thank you to all our authors:

Cameron D'Ambrosi
OWI

Mélisande Mual
The Paypers

Uri Arad
Identiq

Karisse Hendrick
Chargelytics

Noam Naveh
Fraud Strategy

Ran Canetti
University of Boston

Ran Achituv
Entrée Capital

Raphael Lawson
The Hut Group

References:

[1] Arkose Labs, Fraud & Abuse Report, Q4 2019

[2] Payment Card Fraud 2018, The Nilson Report

[3] The E-Commerce Conundrum: Balancing False Declines and Fraud Prevention, Aite

[4] https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement

[5] PWC, Consumer Intelligence Series, Protect.me

[6] https://www.weforum.org/whitepapers/the-next-generation-of-data-sharing-in-financial-services-using-privacy-enhancing-techniques-to-unlock-new-value

[7] IBM, Survey: Consumer Attitudes Towards Data Privacy, 2019

[8] Accenture: The Bottom Line on Business Trust

[9] "Researchers spotlight the lie of 'anonymous' data" by Natasha Lomas, TechCrunch, July 24 2019 https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/

[10] https://www.idtheftcenter.org/2019-data-breaches/

[11] https://knowidentity.com/

Additional References

Protecting Privacy in Practice, The Royal Society

Is Privacy Privacy?, Berkman Klein Center

2019 True Cost of Fraud Study E-commerce/Retail Report, Lexis Nexis Risk Solutions

The Changing Face of Data Security, 2019 Thales Data Threat Report – Global Edition

2019 National Retail Security Survey, NRF

Slipping through the cracks: How synthetic identities are beating your defenses, ID Analytics

Online Payment Fraud: Emerging Threats, Key Vertical Strategies & Market Forecasts 2017-2022, Juniper

Identity Fraud Study 2019, Javelin

The Prius Approach, Harvard Business Review

EMEA Fraud Report 2019, Forrester and Experian

The E-Commerce Conundrum: Balancing False Declines and Fraud Prevention, Aite

Data Risk in the Third-Party Ecosystem, Ponemon Institute

2019 Edelman Trust Barometer

About Identiq

Identiq is a completely anonymous identity verification network that allows its members to validate new users, and vouch for ones they already know, without sharing any customer data or identifiable information whatsoever.

Identiq is a providerless solution, enabling peer-to-peer collaboration. Legitimate users have real, rich history online - while they or some of their details may be new to one merchant, they will be familiar to and trusted by many more.

Drawing on this shared knowledge enables companies to fight fraud more effectively and identify good users more accurately, reducing false positives, increasing approval rates, creating a better user experience. Absolute end-user privacy means companies can even start validating data points that were challenging in the past, like credit card ownership.

To find out how your business can leverage truly anonymous providerless technology to validate identities more accurately and improve customer experience, get in touch.

Find Out More