

**Podcast with David Shrier
Founder & CEO, Distilled Identity**

***Note that transcripts may sometimes contain errors and that transcript timing notations do not match the posted podcast**

Jo Ann Barefoot:	00:00	We have a wonderful show today because my guest is David Shrier who is the CEO of Distilled Identity among many distinguished titles that you have. Welcome.
David Shrier:	00:13	Thank you, Jo Ann. It's great to be here.
Jo Ann Barefoot:	00:14	I'm so glad to have you with us today. I've been wanting to talk with you for a long time. I was at Harvard for a couple of years as a senior fellow, and I know you've been affiliated with the MIT media lab, which is an amazing institution. And you have done a lot of really cutting edge work, technology in general, certainly in finance, and also specifically in digital identity. So I'd like to start by asking you to talk about yourself. You're one of the guests where we could do the whole show talking about your CV.
David Shrier:	00:52	Well, I think it would be more interesting to talk about the substance of the work, but-
Jo Ann Barefoot:	00:57	Give us the highlights and also the journey that brought you here, a little of your background.
David Shrier:	01:42	Okay. Distilled Identity is an AI biometric software company. We help financial institutions and governments build better identity profiles to assist with things like financial inclusion, fraud, credit, risk. So we spun that out from MIT together with Alex Pentland, a professor at the MIT media lab and Alex Lipton, another professor who has been affiliated with Oxford and the EPFL. And so we're trying to solve the global identity crisis. I also keep a foot in academia, because I find it's a way to access the cutting edge of innovation and also engage with policymakers in a different kind of dialog then then you do as a software vendor. And so I still have a dual appointment at MIT and Oxford part time where I teach financial innovation.
Jo Ann Barefoot:	02:40	That's fantastic. So tell us more about how the software works, or the solution.

David Shrier: [02:43](#) Yeah, so we're trying to solve a few problems that relate to structural issues with how financial services, government, how everybody deals with identity. Go back in time. King Artaxerxes I issued a cuneiform tablet to the prophet Nehemiah so that he could travel under the protection of the king. And that was kind of our first let's call it identity document, and we haven't really updated the technology since.

David Shrier: [03:16](#) So we're still dealing with antiquated methods of identifying people with these physical tokens. So wouldn't it be great if we had something better, because those physical tokens are readily forged, readily hacked, represent a really inadequate solution. A lot of the ways that financial services companies today deal with identity is first name, middle initial, last name, and then they use fuzzy texts matching to match it up with lists of bad guys.

David Shrier: [03:44](#) Those systems have a false positive rate. They get it wrong 80 to 95% of the time. It's just not adequate to the task. You could try improving the data quality of the lists of bad guys. That helps a little bit, but really it doesn't solve the structural issue that using methods of identification that are ultimately based on that cuneiform tablet in the ancient Tigris Euphrates civilization doesn't really solve a what we needed to solve, which is to create an identity that actually describes you as you and adapts to how you deal with the real world, and so enter digital technology. Thanks to the rise of all these ubiquitous communications networks, mobile phone networks, 4G networks, wifi, internet of things, all these things that generate more and more and more signal about people, and thanks to better and better compute power and better AI, now we can create identities that are based on behavior and biometrics, and biometric behavior is a very, very cutting edge field rather than based on your first name, your middle initial, and your last name.

Jo Ann Barefoot: [04:48](#) Yeah. And where are we in that journey as far as if you can envision what a fully developed ... These systems never stop changing.

David Shrier: [05:02](#) Right.

Jo Ann Barefoot: [05:02](#) But if you could imagine your ideal of where we might be today compared to where we are, are we just at the very beginning?

- David Shrier: [05:11](#) So the technology has been in development for a couple of decades. My co-founder Alex Pentland created facial biometrics in late 1980s. The technology he created Eigenfaces is now, for example, how India's Aadhaar project identified 1.2 billion people.
- Jo Ann Barefoot: [05:29](#) Let me mention we did a show with Sanjay Jain, and we'll link to that in the show notes on our target.
- David Shrier: [05:33](#) Fantastic. Yeah. So the facial recognition in Aadhaar is based on Eigenfaces. So Sandy's been working on this stuff for quite a while, and Ivan Martinovic, one of our other collaborators created handset biometrics where basically how you hold your phone, and how you interact with it, and how hard you press on the screen and things like that, those are also unique signatures of who you are, because it has to do with your muscles and your ligaments and your tendons and how they work together, and the sensors on the phone are good enough that they can pick that up. And so when we combine all these techniques, we end up with something much, much better than any one of these by itself. So the academic work's been going on for decades. The commercial product is launching in March, so we will now actually have something going into people's hands.
- David Shrier: [06:19](#) We're going to do a big announcement next week, so stay tuned, where we're going to announce our first deployment with a significant government body that will help with refugee resettlement using biometric identity. And once you establish someone's identity using our techniques, you also can do things like build a credit score for them that can help them get a bank account and things like that. So we're very excited by it. But as I can tell you from this initial deployment, this is the first deployment of this biometrics 3.0 next generation technology. So very early days of adoption. Very I'd say late days of research and development, because it's had two decades of research behind it.
- Jo Ann Barefoot: [07:05](#) That's fantastic. I've run into you all over the world. I know you do a lot of work that, as you already mentioned, touches on the developing world problem. In the developing world, there are a lot of people who have no identity papers-
- David Shrier: [07:20](#) A billion people.

Jo Ann Barefoot: [07:21](#) A billion people.

David Shrier: [07:21](#) Mostly women and children.

Jo Ann Barefoot: [07:23](#) Exactly. Disproportionately women and children. And then in the developed world where we tend to have documents, as you just said, they're not secure anymore.

David Shrier: [07:35](#) Well, they've got bad or outdated data. The credit bureaus store a lot of antiquated information.

Jo Ann Barefoot: [07:40](#) Yeah. And a lot of things go wrong there, obviously. So with a system like this, we can envision the possibility of everyone having an identity. The UN has a goal that everyone in the world should have an identity.

David Shrier: [07:56](#) Yeah, that's right. SDG 16.9 says that everyone in the world will have a digital identity by 2030, and there's a wonderful nonprofit called ID 2020 which is trying to help promote standards around making that possible.

Jo Ann Barefoot: [08:10](#) Yeah. And of course everyone in the world at some point here is going to have a mobile phone, which is part of the ability to be able to create data about yourself.

David Shrier: [08:20](#) That's right.

Jo Ann Barefoot: [08:21](#) Regardless of whether you have papers or not.

David Shrier: [08:24](#) Yeah, so in Africa, for example, the poorest continent on the planet, there are 1.2 billion mobile phone lines, and by 2020, so a year and a half from now, roughly, we're going to have 500 million smartphones. So not just phones, but smartphones that can collect and analyze rich data about people to help drive inclusion.

Jo Ann Barefoot: [08:43](#) Right. And then this of course, becomes transformative in a lot of ways, including financial access, which in turn creates economic development. And so both governments and the private sector are really looking at these issues. How do you see it evolving? How are you going to sell what you're doing, for example? How are you going to get it into the hands of people?

- David Shrier: [09:10](#) Well, so first and foremost, we are looking at channel partners who can assist us with the deployment of this technology. So we are kind of like the Nvidia chip inside the Xbox. It's a critical technological component, but there's a richer system around it to actually deliver these financial services and government services and other services to people around the world. So having a very strong partner relationship strategy is integral to how we plan to get commercial adoption of what we're doing. And second of all, there's a requirement for a nuanced understanding of what policies can support this. So I'm running a training at Oxford with women's world banking in April, and we are funded by Visa, and we are helping 20 emerging economy regulators and policymakers understand how to drive financial inclusion for women in the developing worlds.
- David Shrier: [10:10](#) And so there's some interesting artifacts that come out of that. So for example, you would think, I just told you about smartphones, and they have all these sensors, and they can create identity and drive inclusion. But problem is in Bangladesh, men are four times more likely to have the smartphone than women. So if your goal is, for example, financial inclusion for women or identity inclusion for women, you need to address that issue that the smartphone may not be in the hands of your target demographic. And so we need to have a very thoughtful and nuanced deployment strategy and policy supporting it, but the opportunity's absolutely there.
- Jo Ann Barefoot: [10:47](#) Talk about the privacy and data security side of it then. That's the thing people worry about. We all know we can get good things from data being more widely used, but we worry about it getting in the wrong hands, whether that is the company, or having it sold, or having it manipulated by hackers, or having it stolen and so on. How are you guarding against that?
- David Shrier: [11:10](#) Yeah, so we spend a lot of time on data privacy. So we wrote a book about this actually called Trust Data. You can find it on the Amazon store, Sandy Pentland and I and another editor, Thomas Hardjono and-
- Jo Ann Barefoot: [11:23](#) We will link to that in the show notes, as well.
- David Shrier: [11:25](#) Great, thank you. And so federated data and decentralized or distributed data versus centralized data is one design principle.

So Equifax was a big pile of centralized data, makes a really attractive target for a hacker. It's better if you can leave that data at the edge. And instead of bringing the algorithm, bring the data together in a big pile and running algorithm on it, you leave the data decentralized and you bring the algorithm to the data. So there's an open source code project called the OPAL project, O-P-A-L, and that's promoting this model of these algorithms going to the data rather than the data going into the algorithm. And the related project is the one that we put together based on the book. So there's an open source code project called the Trust Data project, which you can find at trust.mit.edu, and that's actually building this decentralized personal identity and personal data architecture that federates the information and puts the algorithm out to the data rather than the other way around.

David Shrier: [12:29](#)

And so that is much more cyber resilient and cyber secure. You need to do other things as well. You need to encrypt the data, you need to create the right permissioning, you create the right governance surrounded. But these are solvable problems. We have the technology to dramatically improve security and control of data for the individual, personal data. What we lack in some countries is political will. So Europe had the political will to pass GDPR, the general data protection regulation, and a lot of the thinking that came out of the World Economic Forum Working Group on Privacy that Sandy chaired was integrated into the creation of the GDPR. So Sandy, myself, and another advisor to my company, Eve [Demanchoy 00:13:12] still work with the European Parliament, the European Commission on these questions of personal data, distributed data, decentralized data, and personal privacy. So we have an exemplar of what good could look like.

David Shrier: [13:28](#)

A lot of companies complain about it. Facebook lobbied heavily against it for years and insisted it was technologically possible. And lo and behold, once GDPR became law of the land, Facebook discovered that it is very possible. I know data. My first job out of college was a database programmer, and I can tell you, it's inconvenient perhaps, but it's certainly not impossible to create that kind of personal control for the consumer around their own data rather than having it be in the hands of Mark Zuckerberg. And so that's an opportunity. In the US, we have not put as strong a set of controls around personal data for the individual. It's still largely in the providence of these

larger corporations that have centralized or data assets, and as the saying goes, if you're not paying for the product, you are the product.

Jo Ann Barefoot: [14:21](#) Yeah. So we are in New York. We both spoke today at the FINRA FinTech conference, and-

David Shrier: [14:29](#) I loved your joke about Mark Zuckerberg. Yeah.

Jo Ann Barefoot: [14:33](#) I won't tell it right here and now, but I'm glad you liked it. The conference here is on RegTech, and we are both on FINRA's FinTech advisory committee, which has been a great experience. FINRA's doing a lot of really hard thinking about all of these issues. We have a very eclectic listener base, but a lot of our listeners are financial companies, FinTech companies, banks, as well as regulators. If we bring this down to the ... What should they be thinking about and what should they be doing in these issues? What should people be looking for and starting to do?

David Shrier: [15:22](#) First and foremost, they need to raise awareness. There are a lot of risks associated with improper handling of personal data and identity data, so the collapse in Facebook's stock price is exhibit A for the cost of not having a heightened awareness and ethical implementation of good data governance and good identity governance. This does not mean shut everything down. You will also cost the business money if you overreach and overregulate. So I have seen some organizations that respond to GDPR for example by refusing to do anything, and that is also bad. This requires sophistication and nuance. So first you need to get really well educated. If you don't have a chief privacy officer, you need one, and you need to empower them. It cannot just be innovation theater. It cannot just be privacy theater. It can't just be someone you stand up there and do a press release and say, "Look, we appointed someone privacy officer," and then they have no power to actually help you evolve a thoughtful privacy strategy.

David Shrier: [16:25](#) Rather privacy is an opportunity, because as more consumers gain control of their personal data through things like PSD2, open banking, in the US, there are analogous moves towards API driven access to financial information. There's an opportunity for a new generation of personal data custodians, and it should have been Facebook, but Facebook has now lost

so much trust in the public eyes that it's not going to be Facebook, so someone else is going to be that trusted advisor and guide to the individual consumer over how to manage their personal data and how to make money off of it even. People will make money off their own data at their choice, and that's going to be a good thing, but they're going to need a trusted advisor do to get there. So that's a big white space that represents hundreds of billions of dollars in potential revenue, and smart companies that get savvy about this space sooner rather than later are going to be able to exploit that opportunity.

David Shrier: [17:25](#) I do recommend reading our book Trust Data. That'll get you really smart really fast. We have a new edition coming out in the fall from MIT Press, and then begin investing in the area. So investing in both the cyber security and protection of personal data assets, but also investing in the innovation potential of helping consumers capitalize on their personal data assets. People can live healthier lives with their physical health, they can live healthier lives with their mental health, they can live healthier lives with their financial health if they have more control and understanding around this personal data.

Jo Ann Barefoot: [18:01](#) So you seem optimistic, and we talked about this on the panel today, people think about these data and privacy issues as sort of a zero sum game. Either we have to give up our privacy to be able to live in the digital world, or we hold our privacy and then we don't get to have all the goodies that we want. And what I think I'm hearing you saying is that-

David Shrier: [18:25](#) There's a third way.

Jo Ann Barefoot: [18:25](#) Yeah. So say it again. So the technology itself is going to start solving these problems for us by giving people more ability to control.

David Shrier: [18:36](#) Not only ability to control, but once you've gathered your personal data in your personal data store, once you've begun collecting that information yourself instead of having some third party data bureau collect that information about you, then you can run analytics. Software can help interpret that data in a way that can help you understand, am I managing my spending well? Am I going to meet my financial goals? Am I exercising enough? So a lot of people use the step counter on their phone to help

them try and get 10,000 steps a day to just get a little more physical activity. That's personal data. If you think of that concept of the step counter and then you multiply it by thousands of data points about how we're living our lives, that can help us have a much more productive life in a much healthier life.

Jo Ann Barefoot: [19:29](#)

And as that happens, tie that back into the custodian idea. So how would your custodian advisor help you?

David Shrier: [19:40](#)

Yeah, so a few ways. First and foremost, although the ideal is that you have total control over your personal data in a personal data store that is somehow attached to you, if you lose your phone, does that mean you've lost all of your personal data? So we probably are going to have some kind of cloud, maybe blockchain based, but let's say storage somewhere that's not just on your phone. In that case, you want to trust whoever it is that it's helping manage that data for you. And furthermore, it's not going to be cost effective for you to run around and get all the different incentives and business deals cut and everything so that you can get \$10 a month for certain parts of your personal data that you don't mind monetizing. But someone who can accumulate a lot of people together will have the negotiating power to be able to help strike good deals for you. So if you think about-

Jo Ann Barefoot: [20:33](#)

So go back a step. You said the company that's helping manage or the entity that's helping manage your data for you.

David Shrier: [20:39](#)

Yeah.

Jo Ann Barefoot: [20:41](#)

If you're the consumer, what does that look like?

David Shrier: [20:45](#)

Conceptually, you can think of it as having your own agent, having someone who will be acting on your behalf to get you the deals that you want to get you the deals that you desire around what happens with your ... I want to get it. Let me give you a discrete example. I want to get a mortgage. So normally applying for a mortgage requires filling out a ton of forms and putting a lot of very personal information out there, and then it goes off into a black hole. Imagine instead you have all that data automatically accumulated and compiled for you, so you don't have the inconvenience of gathering all the paperwork for your

mortgage. And this personal data broker could help you by putting out a bid and for-

- David Shrier: [21:39](#) And so for a 10 minute window of time, 10 different financial firms could assess that information about you and offer you terms in that mortgage, offer you terms in that mortgage, and then once you decide which firm you're going to do banking business with, you rescind the information from the other nine firms. That kind of what's called data governance or that control over what happens with your personal data is something that could be possible and could be mediated by this kind of data custodian or data agent who's acting on your behalf.
- Jo Ann Barefoot: [22:11](#) So you will have given permission to this entity to do this for you-
- David Shrier: [22:16](#) To act on your behalf.
- Jo Ann Barefoot: [22:17](#) To get all your information and protect you.
- David Shrier: [22:20](#) That's right.
- Jo Ann Barefoot: [22:21](#) And what do you see as the business model for these custodians? Because people worry about that, if they're going to ... Is it going to be a fee-based system, or is it going to have a different way of-
- David Shrier: [22:33](#) it could be fee based, it could be transaction based. Some of the entities that are looking at doing this, because this is not a unique idea. Many people have thought of this, and a number of people are pursuing it. Asset management firms, they are your trusted custodian for your financial assets. They could be your trusted custodian for your personal data assets, and they either can get paid on a per transaction or commission basis, which aligns their incentives one way, or they could get paid on a notional value of the overall asset, and that gets them paid another way. So there are some asset management firms that get paid 1% of all the assets that they manage on your behalf per year. And so your personal data assets could be similarly valued, and then they could get paid on that. And then whether they sell once, never, or several times, depending on what you tell them to do, they're getting paid to protect, secure, and empower your data, and you're getting the benefits of that.

- Jo Ann Barefoot: [23:30](#) So I know we're going to run short on time. Let's turn to the regulatory challenges surrounding all this.
- David Shrier: [23:35](#) And they are many.
- Jo Ann Barefoot: [23:36](#) They are many. And one of the things that's fascinating in listening to you is you were talking earlier about simultaneously entrepreneurial, innovative solutions in the private sector being maybe mirrored or-
- David Shrier: [23:51](#) Supported by, yeah.
- Jo Ann Barefoot: [23:53](#) Marrying up with new thinking and from the policy side on what should be the architecture. So if you were going to design the right regulatory framework for this and or have some advice for policy makers grappling with it, what would you suggest?
- David Shrier: [24:18](#) The policy typically lags practice, and that's healthy. You need to experiment around the edges and figure out a direction before policy can then empower, shape, and grow that direction. And so first do no harm, right? The Hippocratic oath of financial policy. Secondly, be thoughtful about a systems approach to implementing policies to support this, because there can be many unintended consequences if you're not careful. And thirdly, provide guide rails that provoke things like financial inclusion while at the same time empowering economic activity and commerce. I have a 60 page white paper that I've written together with some folks from the Office of Financial Research at US Treasury that goes into more detail on how to construct optimal policy for financial innovation.
- Jo Ann Barefoot: [25:16](#) Can we link to that in the show notes?
- David Shrier: [25:18](#) It's in our book, *Frontiers of Financial Technology*, so it's a chapter in the book, and absolutely, please link to it. That would be great. So we've put a lot more thought to paper, but high level, you look at the ecommerce principles that were adopted in the US in the late nineties under the Clinton administration, and those actually are enlightened financial policy. They promoted innovation in the e-commerce sector, they enabled the growth of an entire industry, and they still provided protection for consumers. And so we did not overregulate the way some did with, for example, my favorite example is the

New York state bit license, which caused New York City to not be a major FinTech hub for awhile.

David Shrier: [26:01](#) And on the other hand, it didn't under-regulate to such a degree that you kind of ended up having a lot of harm to consumers. So it found that third way, that path of both promoting innovation and also protecting consumers. And so we hope for the same thing around identity, and we see it being experimented with around GDPR, and something else will come in the US, and hopefully that'll be even better.

Jo Ann Barefoot: [26:27](#) I wish we had more time. Where can people get information about Distilled Identity?

David Shrier: [26:32](#) Distilledidentity.com is our website, and we do have the ability to get in touch with that with us through that. I blog regularly on LinkedIn and also now at forbes.com, and we have a series of books out, and so definitely Trust Data is a must read.

Jo Ann Barefoot: [26:48](#) Absolutely. David Shrier, thank you so much for being on the show today. It's been fantastic.

David Shrier: [26:53](#) It's been a pleasure, Jo Ann, and thank you for the opportunity.