Deloitte.
Insights

INTERVIEW

New models for building digital trust:
An interview with MIT's Sandy Pentland

Jeffery Weirens, Michael Bondar, and Jennifer Lee

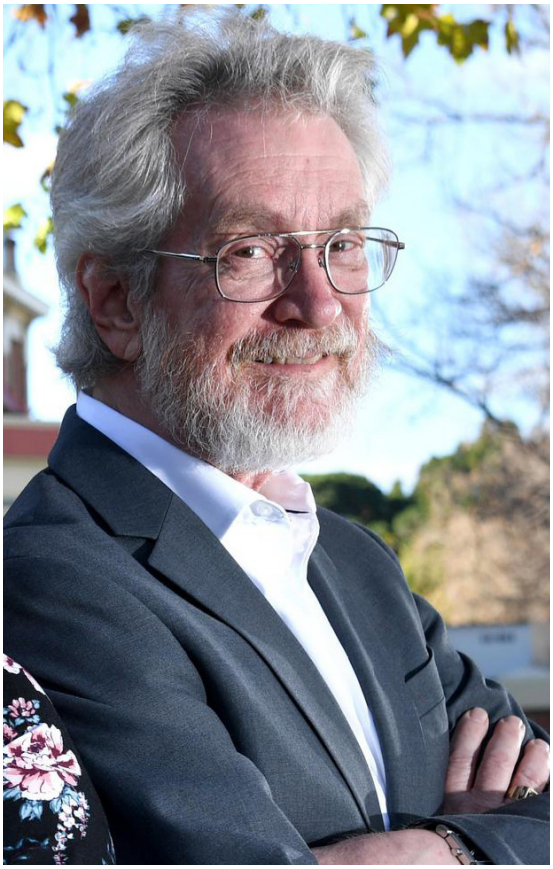
A DELOITTE FUTURE OF TRUST LEADERSHIP PUBLICATION

How can large organizations, facing increasingly complex disruptions, build digital trust with their stakeholders? Sandy Pentland reveals a significant shift in how organizations manage data to preserve digital trust.

DO YOU HAVE your customer's back when it comes to preserving their digital privacy? More importantly, do they believe you do? Recent research indicates most of us don't have much trust that our online privacy is being maintained or that our data is secure: A survey taken during the height of the COVID-19 pandemic indicated that more than 60% of remote workers polled were moderately or very concerned about the privacy protections available for their online tools.[1] Consumers are also anxious: Many are afraid to share health information online with their health care providers. At a time when more of customers' critical transactions are taking place on the internet, a lack of digital trust can cost business and society.

Like any form of trust, digital trust is based on relationships. It is "our willingness to be vulnerable to the actions of others because we believe they have good intentions and will behave well toward us."[2] How can organizations build digital trust with their stakeholders when company size, relative anonymity, and lack of face-to-face interaction may make it difficult to form the strong relationships so critical to building trust? Furthermore, how should an organization respond if a privacy breach occurs and customers or other stakeholders lose trust?

To learn more about these questions, leaders from Deloitte's Future of Trust team, Jeff Weirens, Michael Bondar, and Jennifer Lee, sat down with Alex "Sandy" Pentland, director of MIT's Connection Science lab who also works in close collaboration with the World Economic Forum on big data and personal data initiatives. Sandy has been studying the topic of data and trust for more than three decades. He understands what makes data ownership unique. He and his colleagues at MIT are at the forefront of developing new systems and frameworks to help nations and companies keep data safe and transparent and stakeholder trust intact.



Our discussion with Sandy reveals a significant shift in how organizations view data and their role in managing it to preserve digital trust. The following is a summary of this discussion.[3]

Digital trust relies on competence as well as intent

JEFF WEIRENS: Sandy, what is a common perception or misperception of digital trust?

SANDY PENTLAND: People are deeply confused about the difference between trust and reliability. Typically, when people are talking about digital systems, they're actually talking about reliability or competence. But that's not human trust. Human trust is understanding what a person's motivations are, and believing they've got your back. You can anticipate what they'll do. You know why they are acting the way they do.

This is something that is forgotten very often in constructing digital systems. Data is the clearest example. I'm going to deliver this service to you, and then without really making it clear, we're going to sell your data on the side. That's a violation of trust. A consequence is that if I don't understand your business model and what you are offering me and what the value is to you, I can't trust you. It's that transparency in value, the relationship, and the motivations that are often left on the floor when people talk about digital systems.

All of these dynamics are forgotten when people make digital systems. And that's, in many ways, the fundamental error. A breakdown in this understanding is a pretty good approximation for the situations I've seen where issues of trust come up.

Data is a unique asset that should be managed differently to preserve trust

MICHAEL BONDAR: As individuals, it's second nature to us to strive to be trustworthy, constantly doing the right thing. Can you share examples of organizations that understand the value of being trustworthy with the data they manage?

SANDY: Data is now one of the fundamental means of production, and it needs institutions that are analogous to the institutions we have for money. Data ownership is not the same as for other goods: It's not fungible. It expires. It's mutually created. So the institutions that manage it have to be different. You need the banks and the credit unions that you have for money in the case of data, too—in other words, somebody who has your back. The whole point of GDPR [General Data Protection Regulation], for example, is that level of transparency about motivation.

Data ownership is not the same as for other goods: It's not fungible. It expires. It's mutually created.

There are different types of organizations that understand this. Consider Estonia: They put in place a blockchain system, a very-difficult-to-corrupt ledger, where you can see your data in all government interactions. I remember being in a restaurant with a high-ranking technology leader in the country, and we talked about medical data. He opened up his laptop in the restaurant and said, "Here is my medical record, and here are all of the people who have ever looked at my medical record. Here is the reason that they accessed it. And there's the authorization." And since they put that system in place, they have had zero examples of data fraud.

When the Estonian government did the same for their tax system, the collection of VAT taxes went up 15%. The government liked that. But citizen satisfaction went up far more. It's a trusted system,

because you can see everything that has happened and who disputed it or who didn't dispute it. There are no arguments anymore. You can see how the system works. The idea of becoming probably the most trusted government in the European Union in a period of less than a generation is pretty amazing.

In general, banks and telecommunication companies have a fair amount of digital trust, due in part to regulations. Because the regulators are monitoring them, it's pretty clear how they make money. Beyond that, within communities are financial cooperatives, many of which are B Corps or not-for-profits. These organizations are highly trusted because they interact with people physically and they are not there only to maximize profit. They help finance projects that the community cares about. They act as an interface to the financial system for the community. They have, I think, extraordinary levels of trust.

Changing digital trust mindsets: Distribute data and avoid honeypots

JENNIFER LEE: Sandy, what about organizations that have gotten it wrong? In your experience, what are some of the digital pitfalls that companies have embedded into their business model that hinder trust?

SANDY: It's been very disappointing what people have done in the pandemic. An example of this is widespread use of data lakes. Once you have a data lake, more data is exposed. We're likely to see this occurring more regularly. For example, there are likely going to be vaccine passports just like there used to be TB [tuberculosis] passports. People are going to try and make national registries and statewide registries to support these passports, and that's a major risk from a centralized data perspective.

Instead, an alternative approach similar to credit card systems works better. The way it works in the financial system is, I present my credit card to a merchant. That goes via the credit card company to the bank where I have my money. They validate it or not, and then "yes" or "no" comes back to the merchant. The merchant doesn't know how much I have in my bank, doesn't even know which bank it is. The credit card company knows which bank, but they don't know how much the purchase is, typically, and they don't know anything else about it, too, because all that other information is kept encrypted.

We could do that with vaccination records where you don't have these large honeypots of data that can be exploited. If you don't have a single data lake, if your data's distributed in the hands of the people who know the data best, because they had to collect it—for example, clinics or your hospital—then you don't get massive database leaks, because if data is stolen, it's separate from other data sources.

JENNIFER: That's really helpful. It's about building frameworks around the organization, not just the data teams, to protect and build trust with our consumers. In your view, once a breach occurs, how does an organization go about rebuilding trust?

SANDY: How do you rebuild trust? By accountability. If you can continually track where the data goes and detect things early, that's transparency, right? And then you follow it up with accountability. But also notice that if the data is distributed, you don't get the massive failures. You may get lots of smaller failures, but they're smaller, and they're attributable.

JEFF: I was just going to ask, on the flip side of the honeypot, some may say, we'll just build the right cybersecurity, the best cybersecurity. How do you ensure in a distributed model that each of those small pockets has state-of-the-art security around it?

SANDY: Take, for example, the military. They figured out as early as 1500 that putting everything behind a single firewall was a bad idea.[4] We want to have defense-in-depth, so that if you lose the occasional battle—and you will—you don't lose everything. And, in addition, you get more accountability because with these distributed data pockets, you know who made a mistake. The result is that you will get much better security, because there's more visibility into what happens. You need to have that reputational feedback to each of the elements of the organization.

You also have to understand that you will lose. Bad guys will come up with newer exploits. People will make mistakes. All sorts of things will happen, but you have to minimize your losses and plug them immediately. The most frustrating thing about a lot of data breaches is detecting the problem six months later when they become a big surprise.

The most frustrating thing about a lot of data breaches is detecting the problem six months later when they become a big surprise.

Another interesting consequence is that the people in a local distributed system who collect the data are able to identify issues sooner. Let's take the COVID-19 example. The health clinic that collects testing data has a much better sense of what the data is, of what it should look like, than somebody in the state capital or the national capital, and should be able to spot anomalies sooner, because they know their population. They know the sort of normal rhythms. And it's at a finer grain. So you have the potential for, essentially, more eyes on the problem and more familiar eyes on the problem.

What do distributed data systems mean for tech business models?

MICHAEL: Sandy, as you've been on this journey, how have you seen the reaction and response from some of those big data houses today, technology companies, for example? What's their view around the kind of model you're proposing? And what risks does that expose them to?

SANDY: It's a real change of business for most organizations. As an example, we recently helped a large investment management firm that serves retirement accounts whose assets are held by cooperating banks. We helped them manage these accounts without sharing personal data, and, as a consequence, their system is much, much safer. In a similar way, imagine that you as a consumer had data holders that acted as a fiduciary for you. In this case, when a social media platform asks you for your data, they deal with your data co-op rather than dealing with you directly.

A social media platform, investment firm, or an online retailer doesn't get to see all the data in this model. They just want to know about the critical bits of information that let them execute their value chain. They also have less liability because they don't own the data, even though they can access insights from the data.

The data partner could be a community-based organization, a "data trust" or "data cooperative." It doesn't kill the tech business at all; it's just a different way of doing business. One of the things it does do, though, is that it breaks a lot of the data monopoly power. If you had lots and lots of data held by lots and lots of hands, and just share insights among them, then businesses can spin up sharing agreements much more quickly than trying to acquire consumer data directly.

Increasing distributed systems builds digital trust at business and government levels

JENNIFER: Sandy, I want to shift our discussion to preserving or building digital trust over the next one to three years. What technologies will emerge as organizations seek to improve trust with stakeholders?

SANDY: Beyond the emergence of data trusts to help people manage their data, the innovation that I think is the most compelling is the emergence of these distributed ledger systems to handle all digital transactions: medical, money, you name it. Singapore is developing a system called UBIN.[5] The intent is to have a uniform, continually auditable system for logistics chains and payments. This impacts, essentially, most of the big banks and telcos in the Indo-Pacific area. China has a parallel system for its Belt and Road Initiative. It's big and has already been piloted on a scale of 150 million people.

Tax authorities are beginning to notice these ledger systems for trade. You can't today capture all the cross-border taxes across countries, because they're handled on a whole variety of proprietary systems. What would happen if all that trade were done on a single encrypted system, but now you could say all cross-border trade of type X pays Y percentage? The tax authorities really like it, because it's not taxing their own citizens, at least not obviously. There's something like a trillion dollars a year in lost taxes that could potentially be recovered.

Our research team at MIT helped Switzerland set up the Swiss Trust Chain system with Swiss Post (Switzerland's national postal system) and Swisscom (the country's telecom carrier). It supports all digital transactions. The uniformity, continual audit, and ubiquity of these systems make them transformative in terms of cost, security, and, as I said, auditability.

These ledger systems help the government with taxes and control. They help companies with cost, and knowing their logistics chains. And the fact that instead of having a patchwork of separate systems, you have separate permissions on the same system ensuring security, privacy, and completeness. That Singapore and China are deploying these systems in the Indo-Pacific area means we're anticipating that three years from now, 10–20% of the world's trade could be on systems like this.

JEFF: We covered a lot of waterfront here. Any final thoughts or advice that companies should be thinking about?

SANDY: This idea of a company having a satellite of fiduciary organizations ("data trusts") that manage the data rather than trying to own data directly. This changes the mindset from having the data to having the data insights. We then have local data organizations everywhere. They hold the data for citizens, they have the risk, and they get audited. What that creates is a commercial

relationship where they share insights with companies, we share offers back for their members, and that's the way we do business.

So, all of a sudden, organizations are insulated from brand risk of data loss or mismanagement, and from the problems of data breaches. The digital trust problem migrates, then, to the local organizations, not the company. And that mindset to not holding data directly but having these local, trusted proxies providing insights is a big shift.

JEFF: Thank you, Sandy. This has been great, and we look forward to continuing to discuss these topics with you in the future.

Mr. Pentland's participation in this article is solely for educational purposes based on his knowledge of the subject, and the views expressed by him are solely his own.

Endnotes

1. Cisco, *Protecting data privacy to maintain digital trust: The importance of protecting data privacy during the pandemic and beyond*, June 2020.
2. Sandra J. Sucher and Shalene Gupta, *Broken trust*, *Harvard Business Review*, August 2, 2019.
3. This is an edited and condensed transcript of the discussion on February 5, 2021, among Sandy Pentland, Jeff Weirens, Michael Bondar, and Jennifer Lee.
4. Pañeda Ruiz and José Manuel, *Evolution of siege techniques: From the Catholic monarchs to Vauban*, MilitaryArchitecture.com, accessed March 10, 2021, pp. 5–7.
5. Monetary Authority of Singapore, "Project Ubin: Central bank digital money using distributed ledger technology," accessed March 10, 2021.

Acknowledgments

The authors would like to thank **Ann Perrin**, **Brenna Sniderman**, **Nicole Nodi**, **Negina Rood**, **Aditi Rao**, and **Natasha Buckley** for their contributions to this article.

About the authors

Jeffery Weirens | jweirens@deloitte.com

Jeff Weirens is the Leader of Deloitte's Global Financial Advisory Business and serves on Deloitte's Global Executive. For more than 30 years, he has advised clients on many of the world's most iconic acquisitions and divestitures while growing and transforming Deloitte's consulting and advisory businesses. He has served in multiple leadership roles including Deloitte Consulting's Management Committee, the Energy, Resources and Industrials industry, and the Mergers, Acquisitions, and Restructuring practice. He is a trusted advisor to senior client executive teams and Boards of Directors and is the executive sponsor of Deloitte's Future of Trust initiative, including TrustIQ.

Michael Bondar | mbondar@deloitte.com

Michael Bondar is a principal with Deloitte Consulting LLP. He began his career leading business process transformation and ERP implementation programs across a variety of industries with clients spanning the globe. After spending time as an IT executive at a leading software company, Bondar returned to Deloitte to lead the firm's Global Innovation group with focus on development, scaling, and commercialization of the firm's most innovative technology-based solutions. Today, he is leading Deloitte's Future of Trust offering, bringing forward a suite of solutions intended to help clients measure, manage, and improve levels of trust within and outside of their organizations.

Jennifer Lee | jenniferlee@deloitte.ca

Jennifer Lee is the Global Managing Partner for Global Financial Advisory (GFA) clients & industries, focusing on developing and delivering Deloitte's global advisory go-to-market strategy. She oversees the growth of a multibillion dollar practice. Most recently, she led Deloitte's Global COVID-19 response and the global Deloitte COVID-19 leadership team. She is also the Canadian Managing Partner for developing the critical issue-based growth platforms for Deloitte Canada and Chile. She is focused on investing in leading edge practices to address the key issues facing our clients. Lee was named Manulife Mentor of the Year by Ascend Canada and was also named one of Global Consulting Magazine's top female leaders in Consulting in 2019.

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry center contacts

Jeffery Weirens
Global Financial Advisory leader | Principal
+1 612 397 4382 | jweirens@deloitte.com

Michael Bondar
Global Innovation leader | Principal | Deloitte Consulting LLP
+1 404 220 1992 | mbondar@deloitte.com

Jennifer T. Lee
Managing partner, Growth Platforms Value Creation Services | Global Financial Advisory Clients & Markets leader | Deloitte LLP
+1 416 874 3344 | jenniferlee@deloitte.ca

Deloitte.
Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.

Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Aditi Rao, Rupesh Bhat, Aparna Prusty, and Nairita Gangopadhyay

Creative: Sonya Vasilieff and Swagata Samanta

Promotion: Alexandra Kawecki

Cover artwork: John Jay Cabuay

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.