In:Confidence

Founding the New Era of Data Privacy

Insights from In:Confidence 2019

Powered by PRIVITAR

We're at a critical moment for data privacy

Whistle-blowers like Edward Snowden and Christopher Wylie – not to mention a succession of leaked Facebook memos – have given us a growing sense of how data can be used for control, and how difficult it is to protect individual privacy.

We've also woken up to a new economic model, surveillance capitalism, whose logic is driving organisations to violate privacy in invisible ways, and seek to coerce whole populations.

But at the same time we're seeing exactly how data, and collaboration around data, can be a net positive for humanity – from simplifying our lives to saving them. The data scientists working on those brighter futures need us to trust them with our information, at a time when that trust is in incredibly short supply.

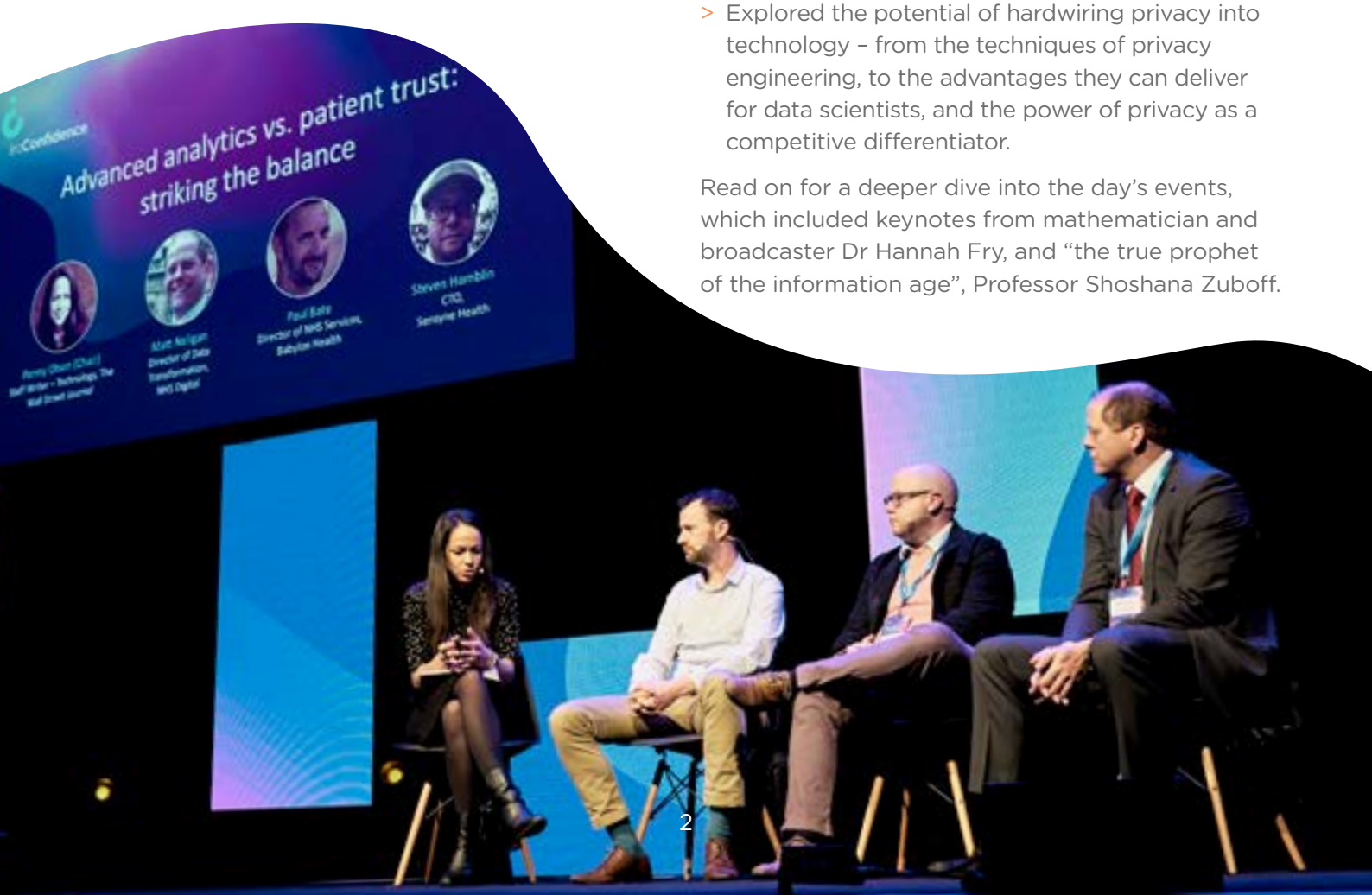
All this points to one central question: how do we protect privacy, without banning access to our greatest resource?

At In:Confidence 2019, some of the world's leading data practitioners, data-driven business leaders and technical decision-makers gathered to explore exactly this challenge – and its potential solutions.

At Printworks in London, this years' attendees:

- Heard how GDPR has triggered a wave of data regulation in nations worldwide – despite only 50% of GDPR-eligible companies claiming complete compliance.
- Debated the effectiveness and viability of greater data regulation – a measure now being called for by even Mark Zuckerberg himself.
- Explored the potential of hardwiring privacy into technology – from the techniques of privacy engineering, to the advantages they can deliver for data scientists, and the power of privacy as a competitive differentiator.

Read on for a deeper dive into the day's events, which included keynotes from mathematician and broadcaster Dr Hannah Fry, and "the true prophet of the information age", Professor Shoshana Zuboff.



The speakers

Dr Hannah Fry

Academic, Author & Speaker, UCL

Stewart Room

Partner & GDPR Leader, PwC UK

Peter Evans

Enterprise Editor The Sunday Times

Doug Gurr

Chairman, British Heart Foundation & UK Head, Amazon

Vivienne Artz

Chief Privacy Officer Refinitiv

Shane Lamont

Chief Technology Officer – Big Data and Cloud HSBC

Ed Vaizey

MP and former Minister for Culture & Digital Economy

Jason Perkins

Head of Data & Analytics Architecture, BT

Matt Neligan

Director of Data Transformation NHS Digital

Sherry Coutu CBE

Entrepreneur, CEO & Angel Investor

Parmy Olson

Staff Writer - Technology, Wall Street Journal

Natasha McCarthy

Head of Policy Royal Society

Dr Adrià Gascón

Turing Research Fellow

Rachel Coldicutt

CEO Doteveryone

Jason McFall

CTO Privitar

Paul Bate

Director of NHS Services Babylon Health

Ade Adewunmi

Data Transformation consultant

Neil Mullarkey

Actor, writer and comedian (compère)

Steven Hamblin

CTO Sensyne Health

Charlie Cabot

Research Lead Privitar

Shoshana Zuboff

Author and Scholar Harvard Business School

How easily privacy can be destroyed

Throughout the day our speakers showed just how easily data can be used – whether maliciously or accidentally – to compromise individual privacy.

Perhaps the starkest demonstration came when Privitar's Charlie Cabot successfully identified a single conference attendee from the geo-location trace produced by his smartphone.

It only took three data points – where the attendee had been the night before, and at two times earlier in the week – to identify the individual from a room of hundreds, potentially revealing not only where he'd been, but who he'd been with.

> In 95% of cases, it only takes four data points to identify an individual based on their geo-location trace.[1]

As we heard, this isn't the only way privacy can be compromised. In a talk that spanned New York taxis, Massachusetts hospitals and Cambridge Analytica, Research Scientist Dr Pierre-André Maugis revealed the different ways in which data reidentification and unintended data disclosure can combine to enable serious privacy harm.

Age-old forces, brand new privacy threats

> "We've bought the lie that if you have nothing to hide, you have nothing to fear. But if you have nothing to hide, you have nothing. The private is the source of my identity and self. My agency and freedom. These things are not meant to be taken without my knowledge."
>
> Professor Shoshana Zuboff, Author and Scholar, Harvard Business School and Harvard Law

If the means by which our privacy is being invaded are new, the motivations – economic and political advantage – are centuries old.

In her keynote, Harvard Professor Shoshana Zuboff explained the central thesis of her best-selling work, The Age of Surveillance Capitalism.

Zuboff charted the rise of this new strain of capitalism, from its birth in a financially desperate, turn-of-the-century Google, to its maturing as an increasingly pervasive economic and political logic.

She described how this logic claims our private data as a raw material, without our consent, with the aim of predicting, and ultimately controlling, human behaviour.

[1] https://www.nature.com/articles/srep01376

Balancing privacy with social good

But just as we're waking up to the forces and models challenging privacy, we're also gaining a deeper appreciation of the immense benefits of data to society and individuals.

This year's attendees heard how a major healthcare charity is investing in data science to enable earlier, better-targeted and more effective innovation.

One area of its research could accelerate heart attack diagnosis from 48 hours to just three, dramatically improving the survival rate of individuals who arrive in A&E presenting chest pains.

> "The NHS is sitting on one of the world's best health data ecosystems. But it's difficult for the NHS to turn it into meaningful value."
>
> Steve Hamblin, Chief Operating and Technology Officer, Sensyne Health

The panel discussion healthcare analytics vs patient trust, meanwhile, shone a light on the multiple models being used to enable privacy-preserving access to NHS data:

- Matt Neligan explained the checks and balances in place at NHS Digital before researchers are allowed access to NHS data – from the multi-stage evaluation of their proposed projects, to assessments of their data security infrastructure.
- Steve Hamblin revealed how Sensyne Health acts as a 'docking station' between NHS trusts and industry partners, processing NHS data itself. The partners receive the insights they need without direct access to patient records, while the trusts receive royalties from their innovations.

What else can be done to make patients happier about their records being put to use? Paul Bate of Babylon Health explained the importance of seeking consent in the context of specific, local services:

> "We can make it very clear that, with their consent, the data from patients' medical records will be used to improve future interactions with our AI and Babylon GP at Hand. It's much harder for the state to have that conversation with the individual, because there's not that natural bond of trust associated with a particular service."

Data regulation: is it the answer?

One common solution to protecting privacy – and increasing public trust - is greater regulation. But how effective a lever is it?

During the Data privacy in the age of the tech titans panel, Ed Vaizey MP welcomed Mark Zuckerberg's recent call for greater government regulation. His fellow panel members, however, showed greater scepticism.

Doteveryone's Rachel Coldicutt observed that Facebook seems much happier to talk about how it handles privacy and content in the wake of Senator Elizabeth Warren's calls for the breaking up of tech monopolies.

Ade Adewunmi of Big Think Analytics cited the leak of 524 million Facebook records the day before the event, suggesting that if Facebook can't effectively audit its own data, regulators have little hope of success.

She also noted, however, the victory of Proctor & Gamble's Chief Brand Officer in getting Facebook and Google to submit to auditing based on commercial drivers. "The only reason P&G is able to do this," she explained, "is because of the serious threat of withdrawing advertising funds."

Moving beyond the GDPR

The greatest recent advance in data privacy regulation has, of course, been the introduction of the GDPR.

But as Vivienne Artz – who sits on the European Advisory Board of the International Association of Privacy Professionals – explained, most companies still have a lot more work to do to make its principles a practical reality.

- Less than 50% of companies report being fully compliant with the GDPR
- Almost 20% say they'll never be fully compliant[2]

> "I liken the GDPR project to renovating a house," Artz explained. "In getting ready for GDPR, firms have repainted and repapered – sprucing up their organisations. But in order to really live privacy, they're going to have rebuild and make it a part of their operations."

[2] https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf

The need for privacy engineering

In an impassioned address, PwC's Stewart Room also spoke to the need for organisations to build privacy principles and rights into their technology and data layers.

Calling out the increasing normalisation of surveillance and propaganda, and the very real possibility of dystopian futures, Room cited privacy alongside climate change, terrorism and increasing inequality as one of the greatest challenges of our age.

> "I believe it's the community that's closest to the data that can deliver the most meaningful change, at the fastest pace. Whether that's a young engineer, working on the code, or someone like me, speaking up for privacy in the boardroom."

Stewart Room, Partner & GDPR Leader, PwC

Privacy engineering in practice

We also heard from the companies already working to build privacy into their own operations, including two giants of their industries, BT and HSBC.

How BT is creating a foundation for a data-rich world

As its Head of Data and Analytics Architecture, Jason Perkins, explained, BT is on a journey to become a more human-centric, insight-driven, service-led organisation – to enhance both operational efficiency and customer experience. And that means making greater use of its 27 petabytes of data.

Perkins revealed how the company has followed privacy-by-design principles to create an architecture that supports data democratisation. One key component is its data policy engine, which ensures users can only access the data they need, after the right anonymisation techniques have been applied.

How HSBC is balancing data access and data privacy

Does a marketing analyst need your national security number? What about a financial crime analyst? And how do you control who sees what data, when you're a global organisation with multiple businesses and 10-15 million different database fields.

> "We want to improve customer service and products through analytics. But we also need to make sure we have appropriate controls – so, for example, a friend of yours who works in our company can't find out what you earn."
>
> Shane Lamont, Chief Technology Officer – Big Data and Cloud HSBC

As Shame Lamont revealed, these are just some of the questions HSBC is asking as it works to balance data access and customer privacy. He also discussed how context-aware data views provide a potential solution, and even shared a step-by-step recipe for creating a minimum viable product.

More private – and more useful

As counter-intuitive as it may seem, getting to grips with privacy engineering techniques can actually make life easier for your data scientists.

Privitar Chief Technology Officer, Jason McFall, set out three key ways improving privacy can improve efficiency:

1. Faster access to data.
Protecting privacy means effectively tracking what data you have, and where and how it can be used – and that means it's much more readily available to data scientists.

2. Easier data science.
It's very hard to reliably de-identify rich, multi-dimensional data like geo-location traces. But if you create a feature extraction layer above this data containing a set of approved functions – for example, to calculate commute times – you can protect privacy, while saving data scientists the legwork of cleaning and organising data themselves.

3. More accurate machine learning.
When you keep training AI on the same dataset, it starts to learn too much from the specifics of that particular data, and its general accuracy gets worse. But take steps to protect privacy – such as generalising some values – and you actually get more accurate general results.

> "We need to find that alignment – where improvements in privacy also make it easier to get things done."
>
> Jason McFall, Chief Technology Officer, Privitar

The future: Differentiating through data privacy

As our understanding of data abuses – and their consequences – continues to grow, the need for greater data privacy should no longer be ignored.

It's now possible to deliver data privacy at scale. And there's every reason to do so.

It improves the availability, efficiency and accuracy of data science.

It helps businesses act as respectful data custodians, earning customer trust.

And – as increasingly evidenced by Apple's strategic positioning – it's fast becoming an extremely high-profile point of competitive differentiation.

In:Confidence 2019: Explore the sessions

Couldn't attend In:Confidence 2019? Or simply want to revisit key sessions? Explore more of the day's highlights here https://www.privitar.com/inconfidence19-recap.

We're Privitar

We help organisations engineer privacy-preserving data operations, using advanced data privacy techniques that protect sensitive information while retaining data utility. Our software accelerates and automates privacy-safe data provisioning, helping our customers get more business value from their data, generate data-driven insights, and drive innovation.

Contact us:

e: info@privitar.com
t: +44 203 282 7136
w: www.privitar.com