Meet the woman who can protect your privacy in a world of hypertracing

As apps tracing Covid-19 spring up, there are fears for the safety of our private data. But Shafi Goldwasser may have the solution

By Harry de Quetteville 19 April 2020 • 7:00am

Premium

Silvio Micali, left, and Shafi Goldwasser, right, were awarded the prestigious AM Turing Award CREDIT: Getty

Exactly three months ago, though incredible to think now, Shafi Goldwasser huddled in crowded meetings with the globe's political, financial and technological leaders. It was the World Economic Forum at Davos, and social distancing was a concept of the future.

Amid the snow-capped peaks and fancy hotels, a densely-packed assortment of powerbrokers pressed the flesh, leaning close for whispered confidences at after-hours cocktail parties, as if contagion was not for the elite – as if Edgar Allen Poe's Masque of the Red Death was being played out in the Swiss Alps.

"I met so many people from all over the world," says Goldwasser, 61. "There was some discussion about this thing called Covid that's happening in China, but it really was not a big topic.

"To think all the world leaders and policymakers and companies were there, unaware, together. It's shocking, given what unfolded just a few weeks afterwards. It seems a lifetime ago."

Goldwasser is not a doctor. She is not an epidemiologist, or a vaccine researcher. She is an Israeli-American mathematician who was in Davos to talk about the power and pitfalls of big data.

And yet, today, her work too puts her on the frontline of containing Covid-19. At a moment when governments around the world are putting in place plans to monitor the movements of entire populations, her work could help them do so without prejudicing all our privacy. Shafi Goldwasser, you see, is one of the world's greatest cryptographers.

In 2012 she won the most prestigious prize in her field, the Turing Prize, named after the celebrated wartime codebreaker. Unlike Turing, however, she is not famous for breaking codes. It is the other way round. She has become a pre-eminent expert in encoding information to prevent it being hacked or stolen. In her twenties, she made a staggering series of breakthroughs by thinking in a way "that was very unconventional at the time".

The sum of those breakthroughs was the ability to do something which, even today, after decades of acclaim, she still describes as “magical”: to encode information so that it remains private and yet *still* analyse it to see what insights it can bring.
It sounds impossible. And indeed that “impossibility” has been the foundation of the internet to date: From Google Maps to Facebook Groups, benefits come at the cost of privacy. It is a trade off.

And many are now concerned with the launch of Covid-19 tracking apps, our sacrifice of privacy will become accelerated and entrenched. Around the world, 28 countries have launched such apps which they see as essential for contact-tracing, with another 11 known to be on the way. Some 13 of those states, according to analysis by Linklater’s law firm, are in Asia. But 11 of them are European, of which six are in the EU.
Google and Apple, which between them provide the software for all the globe’s smartphones, are working together to ensure that such apps run smoothly. The tech giants promise that they will adhere to stringent EU data privacy laws, but in the UK this week, the Information Commissioner’s Office (ICO) which punishes breaches of such rules, said it would take a softly-softly approach in the current pandemic.

It is, says Goldwasser, now director of the Simons Institute for the Theory of Computing in Berkeley and chief scientist at the cybersecurity start-up Duality Technologies, a defining moment for authorities’ use and abuse of individual privacy. Governments will either show that they can be trusted with “big data” gathered from the public, or to be tempted permanently to normalise mass snooping and surveillance.

“I think that there's definitely a chance that states or public agencies will see this as an opportunity to say that they have a right to data,” Goldwasser says. “It is the responsibility of scientists to make damn sure that doesn’t happen… so that we don’t release the genie from the bottle.”

Goldwasser’s part in that began in 1982, with a game of poker. She and her longtime research collaborator Silvio Micali began to work on a paradox of encryption: that it is very hard to encode the very simplest information, such as the result of the toss of a coin, which must be 50:50, heads or tails. In traditional, so-called "deterministic" codes, the encryption of "heads", say, would always look the same. So the code would not need to be cracked for an eavesdropper to learn that, in one sequence of 100 coin tosses, one side landed face up 35 times, the other 65.

Such "partial information" is particularly relevant in poker, where any detail at all, like a card’s suit or rank, is useful to an opponent. So in a celebrated paper, Goldwasser and Micali suggested a new way of encrypting single bits of information with a code that was random, not deterministic. The paper was called “Probabilistic Encryption” and it was the dawn of a new era for privacy.

“At the time, it was really an intellectual challenge,” she says, looking back. “How do you encrypt a single bit rather than a large number? It's very beautiful, intellectually. But at the time it sounded esoteric.”

That first breakthrough led, ultimately, to another: that by breaking complex instructions, like sophisticated computer programs, down into a sequence of basic operations on these simple “bits”, the programs could be run on encrypted data without the need to decipher that data.

In the case of Covid tracing apps, such “homomorphic encryption” would allow governments, say, to supply telecoms companies with lists of infected patients and ask for their recent whereabouts as well as the identities of people they’ve met – all in a limited, anonymous way. The telecom firm would never learn the names of the patients, and the government would only learn the location of affected people – not the entire population. “You only share what you want to share,” says Goldwasser. Yet the mass of data still yields the relevant insights.

On such advances today could rest the difference between benign surveillance and panopticon states.

“And,” Goldwasser says, “contact tracing is a very limited case.” At this point, the astonishingly precise mother of two sons in their 20s, who analyses questions in the manner of her greatest mathematical triumph – breaking each down into its simplest constituent parts – allows herself to get excited.

“There is tremendous importance in this concept,” she says. If sharing of complex data can be done in a way that guarantees privacy, then it could unleash unprecedented collaboration between individuals, companies, even states who currently don’t want to “because don’t want to leak secrets”.

Such sharing of countless data sets around the world, she insists, would drive extraordinary revelations and progress not just in health but in every field of human endeavour.

Taken together, in fact, Goldwasser’s work (which includes two other great leaps called the “simulation paradigm” and "zero-knowledge proofs") amounts to a four-decade defence of both privacy and progress.

“When I started I was entranced by the beauty of the mathematics, the idea that you can achieve things that don't seem to be achievable in the real world. That with a physical deck of cards, you need to turn one up to check what it is, but with digital means you can check without turning it up.

“But that was all a long time ago, before all this data was available. Now there are things we can do in health, finance, everything, that we can’t even imagine

can be done. Can mathematicians enable us to do it? By using cryptography my answer is, almost always, yes."

That was what she was trying to explain to the global leaders in Davos. And why, even as a new virus was beginning its destructive journey, she was quoted as saying that she foresaw "a safer world".

Time makes fools of us all, even minds as feted as hers. But she still sees a safer world, a world in which this pandemic provides an unique opportunity "to harvest information for the common good".

"If the public understands that there is this possibility out there to protect privacy and yet find out crucial information, then I think we will really make progress. We will be able to achieve a wish list of progress, through collaboration, we didn't think possible."