THE FUTURE OF PRIVACY TECH

IN CONVERSATION WITH GILBERT HILL



Gilbert Hill is a privacy technologist who is speaking at the 2021 Summit. Most recently Gilbert was CEO and Advisor to Tapmydata, a start-up building consumer-grade tools for people to exercise data rights, with blockchain keeping score. What follows is an edited version of our podcast interview.

Can you tell us about how you came to be a privacy technologist?

I got into privacy by mistake. And I'm glad I didn't take a conventional route (if that exists) via law or academia. I studied archaeology and anthropology but I didn't want to stay in academia or work as a practical archaeologist so I took up a job on Citigroup's graduate trainee program, which was great insight into how a large, sometimes dysfunctional organisation worked over big distances and with thousands of (human) moving parts.

It was the time of the original dot-com boom. I found myself gravitating towards projects to build the bank's first digital channels, around web and email marketing which later became the building blocks of the data trade we now see. When that boom went bust, I started a web agency with a college friend.

We grew the business steadily and found ourselves doing more and more with data, and getting sucked into the world of behavioural marketing. From cargo cults and potlatch at university, I now found myself working with cookies and privacy-invasive technologies.

I didn't grasp the significance of this at first. Web cookies to me and my team were simply tools, small snippets of code that make the web work, in terms of personalisation. What we've seen with tech is how these tools took on a dual function, to create and track profiles of people as part of the multibillion-dollar business of behavioural advertising. The first crack appeared with the introduction of the EU cookie laws around five years ago.

These laws require website owners to inform users about what cookies they set, why and how the data is used. They were the starting point for me and others to learn about the more nefarious uses of tech in making us 'the product' in the free services we consume and, more recently, to manipulate our emotions as we've seen from films like The Great Hack.

They also, greatly added to by GDPR, single-handedly created an industry and opportunity in providing remedial work (for lawyers) and products for companies to deal with a risk many companies didn't know they had.

'The work of baking a baseline of privacy by design into key business processes and tech while re-acquainting people with their data and rights as citizens is only just beginning.'

We all got used to seeing data as an asset and created lakes of the stuff — these were now in danger of turning toxic. For me, this was an opportunity to automate some of this 'digital asbestos removal' and we created a software product to help companies manage their risk using cookie banners, which are now part of the street furniture of the web, so you can partly blame me for that.

This is only the beginning of the process though; it's all about companies getting their own house in order around a set of compliance obligations.

Meanwhile, the engine of data commerce roars away. Due to wearables and more recently the shift of a whole section of the population online means that most of the data in the world was created in the last two years, post-GDPR.

The work of baking a baseline of privacy by design into key business processes and tech while re-acquainting people with their data and rights as citizens is only just beginning, and that's what really interests me.

Anthropologist Daniel Miller has written about what he calls the 'cult of privacy' in light of Covid-19 and contact-tracing apps. He says, "We cannot be for or against privacy. It must be a question of the balance between care and surveillance." What are your thoughts on this?

Prior to lockdown, I was the bassist in a band gigging around London and the Southeast. The bass often seems to be the Cinderella in rock music, not centre stage, but what makes it noticeable is its absence. The music lacks body and drive, it's just a collection of different sonic frequencies and rhythms sitting on top of each other.

Privacy to me is similar. Often lumped together in organisations with security, it is treated as second fiddle. This is because while security is binary (bad guys hacked us, took my data), privacy is highly nuanced and contextual.

Because we've got used to trusting things like our bank details being treated appropriately as part of our daily lives online, we don't notice how the currency of our personal data and privacy is debased until it's basically non-existent, which is what we have now.

'The model is flawed. And the issue is not so much privacy per se as control. We have lost control of our data and agency online.'

Of course, we trade our privacy freely up to the point where we don't in real life too, and we've become highly skilled as social animals in the dance of when and how much to give up according to the context.

There's been a lot of attention recently around Harry and Meghan and their privacy. Megan made a really good point which I think sums up the current situation: if you have a picture of your child on your desk at work, a colleague might come up and say, what a lovely picture, is that your child, could I take a look? And that would generally be OK, because you put it in a semi-public domain. If that colleague then asked to have your phone and go through all your picture roll, you wouldn't be OK.

Meghan's point was made in the context of the paparazzi with long-distance lenses peering into her back garden, but the online world is a giant back garden with all the lenses pointing inwards. It's not so much the tech as the model which is flawed. For me the issue is not so much privacy per se as control. We have lost control of our data and agency online, and aren't even aware of the impact it may be having as we are categorised, monetised and traded by algorithms, the life opportunities we may be missing out on.



The dark side of the moon. Photo by Nasa on Unsplash.

The platforms, led by Facebook, have arguably also lost control of this even as they refuse to recognise their status as a publisher or a provider of a public service with a duty of care. This is why the current situation is so volatile and the movement which started with cookie laws is picking up pace. The fact we all click on cookie banners to make them go away isn't because we're OK, we're acquiescing to not playing a role in a system from which we're disenfranchised.

Before GDPR, companies assumed all the data collected about us was their property. There's an increasing awareness among the public that their data is theirs but there are challenges around 'where is my data', 'who has my data', 'how can I control who gets my data', and probably also, 'how can I be paid for my data?'. Can you talk about this?

When I started talking about all this, lots of people — generally with vested interests — insisted that people in general, and young people in particular, don't care about privacy and have no idea what happens to their data.

I wanted to prove this wrong, that it's a product of the online value exchange being totally out of whack — the value of services people receive from free stuff online is greatly exceeded by the money a few huge companies were making from them.

There was a similar dearth of information prior to GDPR about what was going on with our data. GDPR did change that because, for the first time, popular media was seeded with an effective campaign by governments to make people aware of their rights, and businesses of their responsibilities around data. I actually had that moment in a bus near Lewisham where I overheard two old ladies talking about data privacy.

"As an individual, it's very hard in practice to exercise your right to request and repatriate your data compared to how easy it is to lose it in the first place."

What was clear is the danger, when it all settled down, that companies would comfortably fall into the pattern of going through the motions of 'we have to tell you this because GDPR' and nothing would change. To a certain extent that's true, as that article by Daniel Miller points out. Despite its complexity GDPR is a blunt instrument, and an unfortunate product of this is it's harder for voluntary groups and small businesses to use data legitimately, while big platforms can achieve baseline compliance easily and, in the case of Google, even start to act like regulators themselves.

As an individual, it's very hard in practice to exercise your right to request and repatriate your data compared to how easy it is to lose it in the first place. So when I was approached by a start-up in Bristol called Tapmydata I was intrigued. They had built a piece of consumer-grade tech in the form of an app for people to exercise their rights. We got talking and eventually they asked me to lead the project.

Personal data vaults, VPNs, and 'clouds of me' had been around for some time but failed to capture my or the public's imagination. What I liked about Tapmydata is they had focused on one single task: requesting data from companies that had it and holding it securely on your phone when you had it back.

We quickly found that people did care about their data, loved the tech, and were curious about where their details had got to. We found the average user had 130 records held on them by companies, and they all had different, often very poignant, reasons for using the app. Many had been born under regimes where data was used as a tool of surveillance and repression.

Predictably, companies were less enthusiastic. They didn't want to relinquish control of the data they, in many cases, had paid for and viewed as their property. And I should stress we were all part of this. As a technologist, the default approach I had to building websites and apps had been to get all the data, do our best to hold it securely, and work out what to do with it later.

What we're seeing now is the logical conclusion: huge amounts of data and online attention concentrated in the hands of a few platforms, and a large sea of sketchy data that is increasingly a liability held by everyone else.

We started to make progress when we could show that the less info a company held, the less risk it represented, and the more they could repatriate questions from a privacy-aware public away from legal to customer and service teams the better the level of trust was. People didn't necessarily want to have all their data deleted and live in a cave. But they do want to have control and are increasingly starting to ask for a slice of the commercial action.

This all seems to be part of a slow uprising around taking back control of the internet since its utopian beginnings, with people wanting digital technologies – and data – to serve the public good rather than just private companies. What are your thoughts on this?

Whether it's new regulations like the Digital Markets Act in Europe, or the Data Dividend Project led by Andrew Yang in the US, there's a growing movement to re-emancipating citizens in terms of their data and its value.

I was at a conference recently where Professor Dame Wendy Hall described this as people becoming "pro-sumers". We don't just consume, we produce data too, and want our views and interests respected.

This is partly a reaction to where we are now with tech. If you look at the history and philosophy of tech and its neoliberal ethos, you'll see it has replaced many of the social structures and groups people had become familiar with, be that clubs, intermediaries, and now physical meetings and events.

In a world where so many things have become



Photo by Patrick Perkins on Unsplash.

commoditised, there is a real premium on trust. Companies like Apple and Ikea are at pains to show that their approach to data ethics and codes of customer contact go beyond compliance, as a brand value.

What's particularly interesting to me is the concept of data unions enshrined in the EU's Digital Markets Act which passed late last year. Data unions address one of the big challenges to changing the status quo around data, which is that individually our voice is small and our data isn't worth a whole lot.

Mark Zuckerberg has famously said each Facebook user's data is worth 1 dollar, each year. But that's largely because Facebook controls the value of that resource on its platform, with neither users nor advertisers getting visibility of the spread between cost and price, or even what data Facebook is playing with.

But together we're stronger. With data unions I can band together with others who share a belief system, or a group such as a charity, church or community and bargain collectively for our data and its value. For advertisers, this is attractive as it breaks the Facebook/Google stranglehold and they get more accurate data and consumer insights from groups at scale.

When you combine that with true data portability, which is built into the Digital Markets Act and US state legislation, there is suddenly framework and a choice for me as a citizen to choose to share my data free for the public good, for a price to the right organisation or not at all to others. Much like we've seen people vote with their feet recently to leave WhatsApp (owned by Facebook) for Signal and Telegram messaging services because of concerns around privacy and data.

I heard someone once say that "blockchain is a problem looking for a solution". How do you see blockchain and crypto playing a significant role in data privacy in the future?

And this is where blockchain comes in. I completely agree with you: I failed to see the relevance of much blockchain around the time it was being hyped a few years back. Most of the applications, complex supply lines, sourcing provenance of diamonds and priceless antiques, didn't play a role in my life!

But when I met the tech guys from Tapmydata, I had a change of heart. Currently a significant problem with data privacy is the businesses that hold our data essentially mark their own homework. They hold the record for how data is held, and whether rights are respected when someone asks about their data. Regulators' only window, or rather a rear-view mirror, is volume of public complaints when something goes wrong in terms of a data breach or privacy scandal like Cambridge Analytica.

The blockchain in this context can be used as

a inviolable, public statement of record. Using an analogy from anthropology, it's a 'tally stick' of transactions so when I ask a company for my data, a notch in the stick is made and when they respond, equally so. This creates an audit trail that can be interrogated by regulators, civil rights groups, and other interested third parties.

Where blockchain can also provide an elegant solution is smart contracts, which are basically automated agreements to do something: sell an asset, transfer some data, or in this case, rights. Combined with the structure of data unions, this means I can agree what can and can't be done with my data, forget about this, and have this flow though at scale into products which can be traded on data markets.

That's where the final part comes in. Blockchain and crypto currencies can provide the payment rails for decentralised data. We've seen how crypto payments have proven popular in countries and sections of society which are typically unbanked, and the phone as a tool by which people can get micro-payments as a source of income.

In the past 18 months, there has been an explosion of activity in DeFi, decentralised finance, where people use crypto-assets as collateral to borrow, lend out, or just plain speculate on. Despite the hype and some big flows of money, it's still a niche activity, with only 2 million active users worldwide.

Creating workable, ethical frameworks and decentralised markets around data could be a way for individuals, groups and families to access income and funds using their personal info, and keep control. And while not everyone has crypto, we all have our data and are waking up to its value, and its risk, and that's a whole new type of value exchange.

Before we go, is there anything you want to leave us with that we haven't covered?

COVID apps (like so much else over the past year, these weren't even a thing) became a concern and now seem to be returning as we slowly emerge from lockdown. There have been lots of comparisons used (and abused) by politicians here in the UK and elsewhere between COVID and a state of war.

One of the casualties of this was (justifiably) privacy, and we've seen great results from apps and other projects that looked to crowdsource data voluntarily. This has gone hand-in-hand with more mandatory data-gathering, and a big role for the private sector in test and trace.

What is legitimate in war may not be acceptable when it is over, or when a vaccine is available. The danger is many of these emergency powers granted to governments, and the tech they use as tools to wield them, doesn't show any sign of going away.

In particular, I was reading yesterday about Covid apps being mandatory for pubs and other places to force younger people to vaccinate, as if they're a source of disobedience and problems when they will in fact bear the long term impact of COVID's disruption. This reminds me of the arguments against GDPR back in the day and it's concerning, to say the least.

FURTHER READING

- An Artificial Revolution: On Power, Politics and AI by Ivana Bartoletti.
- The End of Trust (McSweeney's 54) – features an interview with Ed Snowden explaining blockchain to his lawyer.
- Privacy is Power: Why and How You Should Take Back Control of Your Data by Carissa Véliz.
- The Cryptocurrency Revolution: Finance in the Age of Bitcoin, Blockchains and Tokens by Rhian Lewis.

You can read some of Gilbert's blogs on subjects he covered in this interview on gilbertmhill.com and he's @gilberthill on Twitter.