LETTERS on LIBERTY

DEFENDING THE DIGITAL SELF

Tracey Follows

LETTERS on LIBERTY

Welcome to *Letters on Liberty* from the Academy of Ideas. *Letters on Liberty* is a modest attempt to reinvigorate the public sphere and argue for a freer society.

academyofideas.org.uk/letters

ideas
academy of

Since its foundation in 2000, the Academy of Ideas has hosted thousands of public debates, festivals, forums and salons where people from all walks of life come together to debate often-controversial topics and to challenge contemporary knee-jerk orthodoxies. We always hold on to one defining principle: free speech allowed.

academyofideas.org.uk

What are Letters on Liberty?

It's not always easy to defend freedom. Public life may have been locked down recently, but it has been in bad health for some time.

Open debate has been suffocated by today's censorious climate and there is little cultural support for freedom as a foundational value. What we need is rowdy, good-natured disagreement and people prepared to experiment with what freedom might mean today.

We stand on the shoulders of giants, but we shouldn't be complacent. We can't simply rely on the thinkers of the past to work out what liberty means today, and how to argue for it.

Drawing on the tradition of radical pamphlets from the seventeenth century onwards - designed to be argued over in the pub as much as parliament - *Letters on Liberty* promises to make you think twice. Each *Letter* stakes a claim for how to forge a freer society in the here and now.

We hope that, armed with these *Letters*, you take on the challenge of fighting for liberty.

Academy of Ideas team

DEFENDING THE DIGITAL SELF

In January 2022, Hollywood actress Reese Witherspoon took to Twitter to ask people if they were planning for the advent of 'digital identity'. 'In the (near) future, every person will have a parallel digital identity. Avatars, crypto wallets, digital goods will be the norm', she concluded.[i] Over 50,000 people liked that tweet, and nearly 25,000 retweeted it. The comments seemed split down the middle. One half supported the statement, advocating crypto currencies and living our lives as digitally enhanced beings, while the other half was appalled that such an inhuman reality might lie before us.

There is a new societal division on the horizon: between those keen to jump into an immersive digital entertainment environment (that has come to be known as the 'Metaverse') and those who are terrified of outsourcing their identity to digital platforms that could control everything in one's life via an ecosystem of apps.

I could answer Witherspoon's question in the affirmative, for I have been thinking and planning for digital identity for quite a long time. I had noticed that our identities were becoming less integrated. No longer were we existing purely as physical beings in

the physical world, but we had started to take on personas in social networks, online forums and even within productivity tools at work. We often used a different picture of ourselves in each of these domains, sometimes we used a cartoon character or a celebrity in place of our own portrait. And as this digital information grew, and the technology platforms we were using grew with it, those manifestations of our identities became more and more distributed across the internet.

The distributed self

In effect, our digital self has become fragmented - little bits of it exist here and there. Our qualifications and employment data reside on LinkedIn; Facebook is where our social life with friends and family is catalogued; and the rest of it is displaced among Tinder, Instagram, Spotify, Fitbit and Uber. We leave traces of ourselves whenever we use a technology platform that requires some personal information to make life convenient, and to provide a digital service we need.

It wasn't until I found myself locked out of my own Facebook account in 2016 that I fully realised the implications of this data spread.

I had been receiving messages from Facebook suggesting I update my status to let my friends know what I'd been up to. But rather than referring to me by my name, the platform kept addressing me as 'Byron Loweth'. My account had clearly been compromised, so I tried to change my login details.

> *We're in severe and urgent danger of losing our own identity in the digital realm.*

What happened next was something I never expected. When I scanned in my passport as my official authenticating documentation, I was denied access - Facebook didn't recognise me. Regardless of my social feed containing photos of me, my friends, my family, my previous and existing employers, even my address and location, I was, apparently, not provably me. To this day, I no longer have a Facebook account - it remains in limbo waiting for me to become machine-readable.

If I cannot prove that I am who I say I am, even with government-issued documentation, who is it that gets to verify or authenticate me? How can I prove that I exist? Who is really in control of my identity? Is it me, the government, or - as many of us are starting to suspect - the technology platforms who hold so much of our personal data?

Without us noticing, global technology platforms have taken on many of the roles and remits that traditionally sit with national governments. We're in severe and urgent danger of losing our own identity in the digital realm.

Conversely, national governments have tried to embrace technological solutions to governing populations who demand the ease, convenience and free-of-charge services they have come to expect from Amazon and Google. As a result, what we are living through is the transformation of traditional nations into digital nations.

The digital state

Estonia is a good example of a seemingly successful digitised nation. In 1994, anticipating the digital revolution, the country created a new set of principles for an Estonian Information Policy. By 2002, the country offered citizens a digital signature via an e-identity.[ii] The changes paved the way for a suite of e-public services, even including e-residency giving foreigners the opportunity to set up a company in Estonia to run digitally (and therefore globally). As a geographically small nation, Estonia realised its digital

potential was infinite.[iii] Perhaps one day they will rebrand it Estonia.com.

> *Most people would rather be a citizen of Google than the United States, because Google or Facebook are more responsive to them as a constituent.*

Estonia has become the digitised trailblazer other nations want to follow. In November 2021, at a Digital Nations Ministerial Summit, the UK government took part in a discussion on the theme of 'digital government in open societies'. The Department for Digital, Culture, Media and Sport (DCMS) reported that 'digital technologies play a crucial role in allowing our governments to meet the needs of our citizens whether in relation to delivering healthcare, social support, information or education'.[iv]

Alongside prioritising the creation of the right culture to foster artificial intelligence and manage change, DCMS acknowledged that digital-identity solutions can unlock economic benefits for both the public and private sector. Ministers claimed digital identity was 'key to transforming the delivery, efficiency and accessibility of public services', stressing that it could 'play an important role in enhancing security, as well as promoting inclusion'.[v]

As the transformation from nation to digital nation continues, more and more capabilities are moving from land to cloud, with far-reaching consequences for citizens. As more and more public services are delivered digitally, there will be increased need to authenticate us in the digital realm. US investor Adam Townsend goes further, suggesting that tech platforms are a substitute for the nation state itself: 'Amazon can no longer be thought of as a company, it's a country.'[vi] He makes the point that most people would rather be a citizen of Google than the United States, because Google or Facebook are more responsive to them as a constituent.

If one can't be recognised as the same person on land as online, we are forcibly condemning people to live split personalities, and split lives.

When the internet was launched, there was famously no identity layer - you never knew who was on the other end of your communication.[vii] In fact, you could still be a cat or a dog online, and no-one would ever really know.[viii] Today, it feels that a digital identity is inevitable, not least due to the emergence of the digital nation. In fact, in a world of digitised public services, a digital identity is perhaps essential.

The sovereign self

A far more valuable question to pose is *which* approach, and *what* system, will be the most desirable for the protection of our privacy, autonomy and the civil liberties of all?

We must answer this question practically as well as philosophically - having control over one's own identity is of paramount importance. As Roger Scruton articulated so well, the idea of treating personal identity as something illusory is unworkable. Scruton argues that if we are unable to identify a person as the same entity at different times, it is impossible to accurately ascribe to them their rights, duties and responsibilities.

He goes further, claiming that without personal identity as immoveable fact, we would not even be able to ascribe an emotion to an individual: 'Emotions such as love, anger, admiration, envy and remorse... would vanish... and with them would vanish the purpose of our life on earth.'[ix] Our ability to identify and authenticate ourselves as a known self, independent from others, is what allows us to interact honestly and sincerely with other people as part of a community. We might call this the sovereign self.

The digital native

A new generation doesn't seem to worry that they will leave behind their self-sovereignty in the digital world. Born into the middle of this digitally transforming age, they are more at ease with the notion of having a self that is more like a digital copy. As Damara Inglês, a self-confessed 'fashion tech cyborg', put it:

> *'As digital natives we have always lived in between two parallel realities, with a physical body that is designed by nature, and a virtual identity that is made of pixels: copied, pasted, shared and reposted.'*[x]

This chimes with Witherspoon's belief that every person will have a parallel digital identity. I'm not so sure that's quite right.

It is perfectly possible for us to have one identity that straddles the physical and virtual worlds - in fact it is incredibly important that it does. No one wants to see a young generation suffering from identity crises any more than they already do. If one can't be recognised as the same person on land as online, we are forcibly condemning people to live split personalities and therefore split lives. It's imperative that you can choose to be 'you', wherever you are, and can express yourself in the way you wish.

But if that's the case, how do we protect our own privacy, and exert our self-sovereignty, in a digitised world that is now thoroughly dependent on technology platforms?

How do we become machine-readable without giving ourselves over to the machines?

There is hope. Along with a new generation of maturing people comes a new generation of maturing tech - cryptographic technology now allows governments or companies to issue verifiable credentials. This means you could hold data about your qualifications, job, bank account or passport stored in a way that preserves authenticity and privacy. Only you, the user, should get to choose where, with whom and when you share these 'credentials',[xi] which function as proof of your digital identity and sit in your digital wallet.[xii]

Lists of policies and specifications called 'Trust Frameworks' are being developed in the US and the UK, and other countries are setting out the guidelines and standards for the system to work in a privacy-preserving way.[xiii] Governments and companies that are working to this decentralised model - as it's

become known - promote the primary benefit as being self-sovereignty.

Digital attributes

These credentials, when shared with others, become your 'attributes'. Think of them as what makes you, you. I stressed this point during a panel debate I participated in alongside the DCMS, Microsoft and Lord Holmes of Richmond last year. I suggested that we should think about the future 'self' as no longer physically fixed around an integrated whole, but as layers of digitisation that offer some fluidity and creativity. How do we become machine-readable without giving ourselves over to the machines? Only through creating and deploying layers of attributes that only we own.

The physical world and the virtual world are merging, and it can no longer be a choice between our bodily self *or* our digitised twin: we must convert ourselves into a database of informational attributes that can be as easily understood in the virtual realm as they are in the physical world.

These attributes will not result in a digital identity as much as a *digitised* identity. Attributes will be mixed

and remixed to suit whatever circumstance we find ourselves in. If we need to prove our age or address in a banking context, we will use only the attributes that describe those dimensions of us. If we need to prove our qualifications, or skills, we can disclose only the attributes relating to those aspects of who we are. We will become a fluctuating and flexible database of information - biological, locational, psychological, physical, emotional - accessible on a request-only basis.

In a fully digitised or virtual world, it won't be behavioural data as much as biometric data that is of value to these companies - and the digitised state, too.

This is the way that we might maintain our self-sovereignty in a digitally transforming world. It's the only way we can make sense of it, and ourselves within it.

Becoming digital

During the first two decades of this century, tech platforms extracted tonnes of personal data from you. They took a social graph plotting all your friends, a map of the locations you visited, a list of your top websites and the goods you browse, all the music you love, all the dates you went on, all your reputational feedback from peers, your heart rate, your sleep patterns, what you ate and how fast you walked. As we are all too aware, these platforms have captured and harnessed much of our behavioural data. In many cases we have willingly given this information away.

Even for the ever-increasing number of people working from home, there seems no escape. During the pandemic it became clear that some employers were using keystroke monitoring - cameras, screenshots and even recording audio of workers in their homes - to track them via their devices.[xiv]

The difference is that in a fully digitised or virtual world, it won't be behavioural data as much as biometric data that is of value to these companies - and the digitised state, too. Several years ago, Apple admitted that it systematically recorded and monitored Siri conversations, and that those recordings included

personal conversations between doctors and their patients.[xv]

While some of us are worrying about handing over images of our faces to be digitally searched, merged or even stolen, others are being paid to volunteer their faces for the deep-fake industry, helping to create avatars, digital super-models or virtual customer-service agents. It's not just our faces up for grabs, but each individual feature - our eyes, our veins, our voices, even our expressions. It's all going to be available for analysis and tracking.

We are on the cusp of a great transformation in society, the economy and potentially of our own sovereignty - our sense of self.

What this means is that machines may have the potential to read your identity, health status or emotional state via your biological signals to match advertising and promotional messages to you. Your frown while you are working at your virtual desk, or your squint while socialising in a virtual game, could be extracted for its commercial value - even without you realising.

The *Financial Times* reported on Facebook's (now Meta's) hopes to harvest data on the tiniest of human

expressions to virtually hyper-target advertising, sponsorship and point of sale.[xvi] With 'virtual stores' becoming common in the future Metaverse, we'll not only be able to buy real-world goods digitally, or digital-only goods with electronic money, we'll also be buying digital goods with digital currencies.

> *While data may be the new oil, self-sovereignty is the real prize.*

Whether we end up with central-bank digital currencies or a marketplace of numerous crypto currencies used to buy, sell and exchange things of value, everything will be digitised - and we'll become digitised, too. What we must not allow is our digitised selves to become owned by the technology platforms that have extracted our personal data for the last 20 years. I do not want Meta to be able to deny my digital payments for digital goods in the Metaverse, in the way they denied me access to my own social feed in the past. I do not want Meta or any other tech platform to be harvesting my biological data in a digital form. I do not want them to be harvesting my thoughts or memories, either.

We are on the cusp of a great transformation in society, the economy and potentially of our own sovereignty - our sense of self. But we must not

become distracted by all the exciting promises of the Metaverse. Instead, we must stay focused on the processes and policies relating to identification and verification in the virtual world.

The best route forward is a Digital Bill of Rights, that takes account of a changing world and recognises that the social contract needs updating to a techno-societal contract. Anything that can be digitised can be disappeared, and that includes our rights. When the Freedom Convoy protest refused to leave the streets of Ottawa in February 2022, the Canadian Government froze protesters bank accounts and their digital crypto wallets. GoFundMe blocked $10million in donations to the truckers' group, too.[xvii] The Canadian government, supported by private technology platforms, decided that these particular protesters held the wrong political opinions, and hence revoked their access to digital payment services.

We cannot become resigned to such flagrant abuses of power by governments or big tech. Following what's happened to the truckers, it's now clear that disablement of the digital services we enjoy as a digital self cannot simply be meted out as punishment. We need to ensure we have privacy online, knowledge of how our data is collected and used, true ownership of our own personal data and the right to portability.

We must protect our free speech in digital environments, but we must equally protect our free self, too. In both cases we need additional protection from those who would either diminish us digitally or profit from the computing power they exert over us. We must fight for the digital self and refuse to accept digital slavery, acutely aware that while data may be the new oil, self-sovereignty is the real prize.
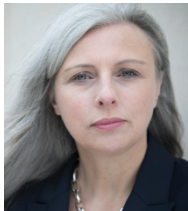
References

[i] Witherspoon, Reese, Twitter, 11 January 2022

[ii] Running, Thomas K, 'The ultimate guide to Estonian e-residency, banking and taxes', *Nomad Gate*, 11 February 2021

[iii] Orton-Jones, Charles, 'The inside story of building a digital nation', Chartered Management Institute, 24 June 2019

[iv] 'Digital Nations Ministerial Statement', Department for Digital, Culture, Media & Sport, 18 November 2021

[v] Ibid

[vi] Follows, Tracey, *The Future of You: can your identity survive 21st-century technology?*, Elliott & Thompson, 2021

[vii] Cameron, Kim, 'The Laws of Identity', identityblog.com, 2005

[viii] Victor, Daniel, 'I'm not a cat says lawyer having zoom difficulties', *New York Times*, 9 February 2021

ix Scruton, Roger, *An Intelligent Person's Guide to Philosophy*, Duckworth, 1996

x Inglês, Damara, speaking at a London College of Fashion event in 2020, as quoted in Follows, Tracey, *The Future of You: can your identity survive 21st-century technology?*, Elliott & Thompson, 2021

xi Hardman, Daniel, 'A gentle introduction to verifiable credentials', *everynym*, 24 October 2019

xii Follows, Tracey, 'Think digital wallet not digital identity', *Forbes*, 23 July 2021

xiii 'UK digital identity and attributes trust framework', Department for Digital, Culture, Media & Sport, 8 September 2021

xiv Abril, Danielle and Harwell, Drew, 'Keystroke tracking, screenshots and facial recognition: the boss may be watching long after the pandemic ends', *Washington Post*, 24 September 2021

xv Hern, Alex, 'Apple Contractors regularly hear confidential details on Siri recordings', *Guardian,* 26 July 2019

xvi Murphy, Hannah, 'Facebook patents reveal how it intends to cash in on metaverse', *Financial Times*, 18 January 2022

xvii Loh, Matthew, 'Canada says it will freeze the bank accounts of "Freedom Convoy" truckers who continue their anti-vaccine mandate blockades', *Business Insider*, 15 February 2022

Author

Tracey Follows is a futurist and
the founder CEO of Futuremade,
a futures consultancy. She is the
author of *The Future of You: can
your identity survive 21st-century
technology?* and host of *The Future of
You* podcast, where she invites
renowned academics, authors and innovators to
discuss the future of identity in a digital world.
Tracey is a member of the Association of Professional
Futurists, World Futures Studies Federation, a fellow
of the RSA and an associate fellow of the World
Academy of Art & Science. Find out more at
www.traceyfollows.com

Illustrations
Jan Bowman is an artist and author of *This is
Birmingham.* See her work at janbow.com

Letters on Liberty identity
Alex Dale

Pamphlet and website design
Martyn Perks

LETTERS
on LIBERTY

academyofideas.org.uk/letters