Imagine if we walked around the real world with a small screen floating above our heads. That screen would update with a different set of information depending on who looked at you. It would always be above you displaying at least your name, the date of your birth, and the neighborhood where you live. Imagine being in a crowd at a protest, or a concert. Anyone's, everyone's details would be there. And of course, if the police looked that screen would fill with all sorts of additional information about you and the people you associate with.

Dystopian? Even if we don't consciously think about it, anonymity is important to us in our everyday lives. Or if that scenario isn't scary enough, what if you were a Hong Kong pro-democracy protester? Or a political correspondent in the middle of a war? What if you were fleeing from domestic violence? Hiding in witness protection? There are plenty of reasons why individuals value their privacy—privacy that is protected by public anonymity.

Yet, in the online world, many (wrongly) believe that a system of real names would create accountability—they would love a system of screens above everyone's heads.

The Australian government is on a bit of a crusade against the big bad internet, pushing through draconian measures in the name of protecting the vulnerable. Yet, the measures too-often wind up actually harming those they proclaim to protect.

The most recent shiny idea that was floated from the government is that in order to bring accountability to domestic violence and sexual abuse, and reduce their occurence, social media users should be required to submit 100 points of ID to digital platforms. This is a new spin, but similar measures have previously been floated as a means to reduce other types of cyber harm (bullying, spread of misinfo, defamation). Once again this reignited a discussion about mandating a "real name policy" which would mean everyone has to use their full name across social media. Well, there's a lot wrong here which we can unpack.

But before we get into the details here, let us get out of the way that ANONYMITY IS ABSOLUTELY ESSENTIAL for the free and open internet to function. We cannot glorify the Arab Spring protests and the might that social media has given to social movements at critical points in time, and then immediately turn around and remove every component which made those movements possible. Of course that is indeed what governments, and many of those in power want, because that is precisely the sort of movement-building capability they don't want individuals to wield. Studies have shown that anonymity is central in enabling individuals to speak up and speak out.

We also have to recognize that the internet is a different place than it used to be, and it continues to change and evolve. Our online footprints are ever more permanent and visible. Traditionally those who benefited from anonymity were dissidents, human rights activists, journalists, and members of vulnerable communities. Yet, increasingly, pseudonyms are embraced by the general public as a way to maintain a private life alongside a public one online. And, in fact, some data has suggested that those who use pseudonyms leave better, more researched, and nuanced comments.

We shouldn't give more personal data to social media, they can't be trusted

With the amount of sticking it to the "internet giants" that the current government is occupied with, trusting them with 100 points of identification is an unexpected policy flip. This idea is uniquely Australian, because while a lot of governments have considered mandatory IDs, it has always been through some version of a token authentication and never by actually giving the social media company personal documents. In instances of remote authentication, all that a social media provider receives is a response from the ID provider verifying a core piece of informationation—typically either that you are a person or perhaps even that you are of age (not what age you are, it just says "yep, this person is over 18"). And even then, such proposals are under scrutiny and receive criticism.

It was almost surreal to watch the news media report on one of the biggest breaches in Facebook history and simultaneously hear the government discuss giving Facebook and other companies actual copies of personal documents. Setting aside the social impacts that we've outlined above, just the risk of identity theft if those documents were leaked is incredible. The fact that the discussion is around 100 points of documentation—as opposed to even something like a copy of a driver's license—seems beyond disproportionate.

Anonymity is a (contested) building block of the free and open internet

In his 2015 report to the United Nations General Assembly, David Kaye, former Special Rapporteur on Freedom of Expression, studied the use of encryption and anonymity in digital communications. The report concluded that encryption and anonymity act as key enablers for individuals to exercise their rights to freedom of opinion and expression in the digital age and, as such, deserve strong protection.

"Strong encryption and anonymity are fundamental for the protection of human rights in the digital age and are critical to individuals who face persecution because of their sexual orientation or gender identity. Anonymity has been a crucial tool for women and sexual minorities for self-expression, connecting, and mobilizing and the use of anonymity online supports the most vulnerable groups."

In spite of its nature of sheltering marginalized voices, anonymity is constantly under fire and the subject of court deliberations. Australia has had its own struggle with what data about us online is subject to the Privacy Principles and which is not. Australia's laws only protect "personal information", which is defined by whether a person is identified or identifiable from the data. And even though the Office of the Australian Information Commissioner (OAIC) often cites IP addresses as protected, in 2017 the Federal Court made a landmark decision to strictly limit what constitutes "personal information". This decision means that certain data held by Telstra, including IP addresses, URLs (websites) visited and geolocation data, are not protected by Australian privacy law.

Real name policies lead to real world harms

We note that the government's 100 ID points proposal doesn't necessarily require a real name policy, however, tying identity documents to any identity increases the likelihood of that information being linked. Digital platforms continue to hemorrhage our personal data in massive leaks (with impunity), and the end effect not only risks de-anonymizing individuals, but also leaking additional private information like addresses, phone numbers, birthdays… every piece of information stored on the identification documents which were submitted. **The proposal essentially doubles down on creating risk and vulnerabilities for individuals.**

Those who use or want to use pseudonyms, are not a small minority. Almost half of the population belongs to a social group that can benefit from pseudonyms. The most cited examples are victim-survivors of domestic violence who are hiding from their abuser—and it's a strong example because there is a shocking amount of people victim to domestic violence in Australia. But the category is a lot broader and includes children and teens exploring their identities, journalists, political dissidents and activists… the list is long.

It's worth noting that not everyone uses a name that is different to the one that appears on their birth certificate in order to *hide* who they are. For some, it is about being able to actualise their identity. For example, forcing trans, non-binary and gender non conforming people to use their deadname online would not only cause harm, it also wouldn't be an accurate reflection of who that person is—pretty counterintuitive to the pupported goal of a real names policy!

Some of the cost to those complying with a real name policy are:

- harassment, both online and offline,
- discrimination in employment, provision of services, etc.
- actual physical danger of bullying, hate crime, etc.
- arrest, imprisonment, or execution in some jurisdictions,
- economic harm such as job loss, loss of professional reputation, reduction of job opportunity, etc.
- social costs of not being able to interact with friends and colleagues,
- possible (temporary) loss of access to their data if their account is suspended or terminated.

We are extremely concerned that the government is attempting to solve one problem without actually weighing the large scale negative impacts of such policy changes across the population.

Good public policy doesn't rely on a single take and anecdotal evidence, or the personal gripes of someone currently in power. Australians deserve a regulatory approach that is fit for purpose in the interconnected world we live in—and that should start with an update to the Privacy Act, not half cooked ideas about giving digital platforms copies of our most sensitive identification documents.