Online Safety Amendment (Social Media Minimum Age): An Implementation Discussion

Written by Me
December 2, 2024

Table of Contents

Introduction

Nowadays, I restrict much of my online presence to *Survivor* thirst posting on Tumblr—have you *seen* Sol this season?—But like, I've been compelled share something of substance. And it's because of this social media age bill here in Australia.

I *could* go on and on about opposing it and whatever but honestly there's stronger, more coherent voices out there that can dictate their opposition much clearer than I. So, instead, for the first time in nine months, I thought I would use my ten year background in technology and try to understand what this bill might look like in the real world; I am, if anything, at least *somewhat* qualified in that regard.

This is going to be very free flowing and loose—also known as "rambley"—which will probably be boring to hear. I'll try to keep it interesting too, but I think the most interesting part of this is going to be the conclusions it draws anyway so if you're so inclined, skip to the end of the solution and conclusion like I often did while writing this and I'll see you at the end. But for those who stick around, there's some meat somewhere for you to chew on or find flaw with.

But like, why the hell am I writing about this? I write about almost anything I can think of and don't for a second consider putting it out there for people to read. Moreover, I could be on a beach somewhere, lying in the sun and listening to the beautiful lapping of waves. But for some reason, this has really caught me.

Why is that, though? Truthfully, I don't have an answer. Really, I *don't* know why. I do love writing, it's as much fun as it is torture, but there's got to be another reason right? I've been avoiding technology, or even talking about it, for nine months and suddenly this is what I want? It can't simply be "But I love to write!".

Part of it might be to do with the discourse I'm seeing. The discourse is so *widely* negative that I'm trying to really damper my similar feelings and dissuade them by actualising what I'm seeing. Or maybe it's because I'm *that* close to turning thirty—I'm like, for real, a week out—that I'm desperately trying to make something of myself while I'm still in my twenties. *Or* maybe it's because I've been watching Anthony Bourdain's glorious *No Reservations* way too much and hope to similarly eject myself into stardom by dumping on the industry that has treated me so well for the last ten years—as if to get back at it for something I can hardly comprehend or verbalise to others—while still desperately seeking its respect and admiration.

Well, whatever. I was compelled to write this; for whatever reason, I needed to get this out of my system and *bad*. So love it or hate it, it exists.

Enjoy.

Assumptions

What does the government actually want to achieve? That was really my first and only question. I had an entire document with that simple question sitting on my computer the first time I even heard about this thing, so let's answer it.

To put it simply, the government wants to prevent children aged below sixteen years of age from accessing social media platforms. Great, those words makes sense to me syntactically. We also know why. It's to curb bullying and mental health issues; which the government really seems to fail to understand from almost all angles.

How do we literally achieve that though, is the next question. There's all kinds of ways technologically, even many existing ones, so maybe if take a look at the bill we'll be able to make some assumptions to determine the kinds of technologies that may be appropriate; or maybe even the government will give us examples. So, essentially, I want to know what may dictate a choice or what the choices are.

Oh me, oh my, we've hit a road block already. The bill doesn't mention any technologies at all. What that means is we have to *infer* what kinds of technologies may be appropriate based on the content of the bill. So let's briefly skim the thing and see what assumptions we can make.

The bill indicates that a social media platform must not *"collect government-issued identification material"* [1] which includes the following:

1. *"identification documents issued by the Commonwealth, a State or a Territory, or by an authority or agency of the Commonwealth, a State"* [2]

2. *"a digital ID (within the meaning of the Digital ID Act 2024) issued by the Commonwealth, a State or a Territory, or by an authority or agency of the Commonwealth, a State or a Territory."* [3]

So we get a pretty flat security rule there for data collection, which we can use, and I think we also get an obfuscated hint in "digital ID". So let's ask ourselves:
Um, what is a digital ID and why does it matter? Coincidentally, we got a new act this year that tells us. The Digital ID Act 2024. It explains:

[1] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Page 7, Line 25 to 26, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r7284_aspassed/toc_pdf/24150b01.pdf;fileType=application/pdf

[2] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Page 8, Line 13 to 15, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r7284_aspassed/toc_pdf/24150b01.pdf;fileType=application/pdf

[3] Online Safety Amendment (Social Media Minimum Age) Bill 2024, Page 8, Line 17 to 20, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r7284_aspassed/toc_pdf/24150b01.pdf;fileType=application/pdf

> *"… a distinct electronic representation of the individual that enables the individual to be sufficiently distinguished when interacting online with services."* [4]

Very blah, right? Like, what does that actually entail? Well, like before, there's a tiny clue in there that we can use. We see this word "individual". Twice, in fact. You're probably likely to ignore this kind of word, but it pinged it my head and so I was curious about the express nature of an "individual". We can assume it means us as Australian citizens, but what exactly defines and describes an individual? Is it a collection of data or a single set of data? Oh, maybe it is. Let's follow that thread. So what kind of *information* or *data* defines an individual?

Oh, bingo. Digital ID Act 2024 back to the rescue. According to the act, an individual is ascribed two kinds of "attributes" which are referred to as:

> *"An attribute of an individual means information that is associated with the individual, and includes information that is derived from another attribute."* [5]

The two kinds of "attributes" are "attribute" and "restricted attribute" [6]. An "attribute" is defined as:

> *"name, address, date of birth, phone number, email, biometric information, racial or ethnic origin, political opinions"* [7]

A "restricted attribute" is defined as:

> *"health information, criminal record, identifiers (…), membership to professional or trade associations, membership to trade unions, tax file number, medicare number, health care number, drivers licence"* [8]

Nice, so that's our individual. Oh and hey, that's our relationship to digital ID as well. But before I put a stake in the ground, there's one thing that's not clear. A platform is

[4] Digital ID Act 2024, Page 10, Section 9, https://www.legislation.gov.au/C2024A00025/asmade/text

[5] Digital ID Act 2024, Page 15, Section 10, https://www.legislation.gov.au/C2024A00025/asmade/text

[6] Digital ID Act 2024, Page 10, Section 9, https://www.legislation.gov.au/C2024A00025/asmade/text

[7] Digital ID Act 2024, Page 15, Section 10, https://www.legislation.gov.au/C2024A00025/asmade/text

[8] Digital ID Act 2024, Page 15, Section 10, https://www.legislation.gov.au/C2024A00025/asmade/text

not able to *collect* information, but does that also mean they cannot *read* it? My naive initial reaction was no, they can't. But that is so, so naive. So we *have* to assume that platforms can *read* it. Which is a *huge* risk, because like do you know how easy it is for a team with *any* seniority to misconstrue a requirement like this and suddenly that information is *collected*? From personal experience, it's way more likely than you think. Like, *way* more likely. This is something I'll get back to later, so put a pin in this as a major, major, major, major risk.

Alright, it's stake in the ground time. So now, with our security rule and the definitions above, we've got another assumption spewing from the earth: A social media platform is not permitted to *collect* personal information from identification documents issued by a state or government body or from a digital ID.

Another thing I want to talk about is that the government clearly wants to build their own age verification solution. While they may approve other forms of age verification, the fact that they plan to build one of their says to me that they would *rather* platforms use theirs. But what would that look like, exactly? And what is it that we actually need for verification? Well, we need date of birth, that's for sure. But that doesn't answer where it comes from. In these platforms, you likely already have your date of birth set somewhere. But for their solution, where does it come from?

Frankly, it's clear the "digital ID" is again the key. It remarks storing a "date of birth", which is obviously something we absolutely need to use for age verification, but where does that live and what solution can we use? Does the government create something new literally called "digitalID"?

Well, it may come as a surprise to you, but it actually already exists and it's called myID—aptly renamed from "myGovID" days before the bill passed [9]. I'll go into later what myID actually is and how you use it, but for now all you need to know is that it is a *digital ID* service for identity and authorisation of government services. It does a lot of other stuff too but ignore that and try to just think of it as like "sign in with Facebook" or "connect with Google" but for a government service.

So my assumption for this is this: myID will be the government solution for age verification on social media platforms. Oh, and because myID is a digital ID, we can sneakily reframe our previous assumption to be: A social media platform is not permitted to *collect* personal information from identification documents issued by a state or government body or from myID.

Two quick other ones I want to make as well: What a social media platform is and who this is implemented for—who is the audience.

The bill itself dances around the definition of a social media platform like I do my personal life and could kind of include *anything* that has user involvement, but *we* know what a social media platform is so I don't want to play around with semantics. Facebook, Twitter, Youtube, Tumblr, Reddit, Bluesky—Those are social media platforms. We *know* what a social media platform is so let's no act all coy.

[9] myID, "myGovID is now myID", https://www.myid.gov.au/mygovid-now-myid

Additionally, I want to make another assumption that this is implemented equally for all Australians and with no variation. It may seem draconic, but we’re dealing with government mandates and while I might not agree with making the entire population do this, it *is* the simplest and likeliest. So, another joins the fray: This must equally apply to all users from Australia, regardless of age.

Fantastic, we’ve got some good assumption here. They are:

1. What a social media platform is: Facebook, Twitter, etc. We’re not playing games in this document, we know what they are.
2. What is required for age verification: Date of Birth.
3. myID will be the government based solution for age verification.
4. A social media platform is not allowed to collect the personal information stored within a digital ID, or in this case myID.
5. This must apply equally to all users from Australia, regardless of age.

For now, I think these are enough for what we want to explore. We may think of more later but let’s define them as we go as to not drag this on even more.

However, as I read these, I’m finding that I’m more interested in what a government age verification solution might look like over just like what the government wants to do overall. After all, we’ve already got some existing third party ones they may approve of, so what might a government one look like?

So let’s move forward thinking about that. We can still use the assumptions above because they still apply, but let’s say: We want to explore what a government age verification solution might look like.

Yippee! A direction! My parents would be proud.

Exploration

So we want to understand what a government age verification solution might look like. But we don't really know what kind of existing technologies are out there. Like we wanted some from the bill, but we didn't get any. We also don't use age verification solutions right now. So, let's do some exploring and ask questions like: Who is doing this elsewhere in the world? How do these solutions behave? What could it look like as a government based solution?

Facebook has a help page that outlines how age verification works their end, which they say they use "selfies", "phone numbers" and "date of birth" [10]. Although, "phone numbers" doesn't exactly seem available so let's pretend that doesn't exist.

The date of birth usage is obvious and something you've likely seen on many platforms, not just Facebook. If you enter an age lower than the platform allows, you're rejected from the registration process. To test it, I tried creating an account for an imaginary four year old and received a message from Facebook saying "We couldn't create your account. We were not able to sign you up for Facebook." [11]

The selfie verification is a little bit different, so we'll examine that. Facebook says they use technology from a company named Yoti [12]. Yoti develops all kinds of products and solutions, but what we're interested in is their "age verification" solution [13]. The process with Yoti is pretty simple: You take a selfie, the picture is run through algorithms to estimate your age (which, according to both Yoti and Facebook, uses anonymous images of human faces to compare against), they send the age result back to Facebook and then delete the image on Yoti and Facebook. If you're curious, these two videos from Yoti and Facebook are pretty helpful.

Instagram looks to have almost identical age verification methods as Facebook, so "selfies", "phone numbers" and "date of birth" [14] using Yoti and whatever else Facebook uses. Makes sense, both being owned by Meta. We won't explore this much further.

Google has numerous age verification methods. I found a help page titled "Access age-restricted content & features" wherein Google expresses they use the following methods: document verification using IDs (drivers licence, passport or national id),

[10] Facebook, "Confirming your age on Facebook", https://www.facebook.com/help/958848942357089

[11] Facebook, "Create a new account", https://en-gb.facebook.com/reg/?ty=tytrue

[12] Yoti, https://www.yoti.com/

[13] Yoti, "Age Verification", https://www.yoti.com/business/age-verification/

[14] Instagram, "Introducing New Ways to Verify Age on Instagram", https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram

selfie verification (which is similar to Yoti but uses OCRLabs, who have since rebranded to IDVerse [15]), credit card verification and phone number verification. All of these methods also request your date of birth as an extra layer [16].

I wasn't too interested in booking a demo with IDVerse to find out how everything worked, but I did find a talk by Terry Brennar, Head of Legal Risk & Compliance at IDVerse, who showed a few images of what IDVerse looks like to a user [17]. Check the footnotes if you're inclined, but if you watched the Yoti or Facebook videos, you get the idea of the Google version of selfie verification.

TikTok. Oh, TikTok. I have to be honest, this was pretty hard to find. My searchings originally led me to TikTok videos from creators explaining why they were banned and how they resolved the issue, but I eventually found what I was after.

TikTok seems to have more of a "report and appeal" style approach to age verification. From what I could find, the flow is basically: If a user is found to be underage (thirteen or under) by another user, they report them. An investigation is made and if this is found to be true, they are subsequently banned. However, if you still wish to use TikTok as a minor, you have to go through an appeals process.

The TikTok appeals process is kind of all over the place and actually made me laugh pretty hard while I was reading it, so let's briefly go through their options.

First of all, you can perform "Facial age estimation" verification through an undisclosed thirty party solution [18] or credit card verification which charges and refunds your account a very small amount in order to verify [19]. You can also request approval from a parent or guardian if they already have a verified TikTok account, whom may have also needed to verify using the previously mentioned methods of verification. Further, TikTok has a number of manual methods for appeal. One method is taking a picture of yourself, a piece of identification and another of you holding that same piece of identification and to send that to TikTok. So, basically, some sad sap at TikTok reviews your pictures and approves or denies your appeal based on what they see. Prone to problems, I suppose. What you can do as well, if you're underage and out of options, is do the same thing as above but instead with your parent or guardian. What is meant by that is to take a photograph with *"Your*

[15] IDVerse, "Age Verification", https://idverse.com/products/age-verification/

[16] Google, "Access age-restricted content & features" , https://support.google.com/accounts/answer/10071085?sjid=16739457453252018244-AP#zippy=

[17] Age Check Certification Scheme, "OCR & Doc Authentication, Terry Brenner, IDVerse", 0:56, https://youtu.be/iQXqy1PPxAg?t=56

[18] TikTok, "Facial age estimation (if aged 18 and over)", https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok#2

[19] TikTok, "Credit card authorisation (if aged 18 and over)", https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok#2

parent, guardian, or other trusted adult… looking at the camera and holding a piece of paper with the following items written clearly and legibly” [20].

So ultimately, and perhaps appropriately, TikTok is all over the place. But, hey, they do have a *kind* of age verification process, it’s just not upfront.

Because this was being touted as a “world first” solution, it got me wondering if that’s really true. Politicians sometimes tout this kind of thing and then an hour later someone online is posting about how it’s been done before. But in this case, and the media reporting on this should be a dead give away, there’s actually not a lot out there. Not a lot of approved laws, I mean.

However, there are a few a recent examples in a similar orbit to this that is may help gauge our situation here. In America, laws passed this year requiring pornographic websites to verify the ages of users. And while not social media platforms, we *can* apply the same lens.

So, according to a bill passed in Texas, a pornographic website must have an age verification system that verifies a:

> *“government-issued identification”* [21] or uses a *“commercially reasonable method that relies on public or private transactional data to verify the age of an individual”* [22].

In Louisiana, you can find similar sentiments:

> “*Require the person attempting to access the material to comply with a commercial age verification system that verifies in one or more of the following ways: Government-issued identification, Any commercially reasonable method that relies on public or private transactional data to verify the age of the person attempting to access the information is at least eighteen years of age or older.”* [23]

In both these the onus is on the platform. The platform must build or implement a way in which to verify a user age and if the platform doesn’t comply, they are fined. Or, from what I read, fight back in the courts or simply stop delivering content to those parts of the Americas.

[20] TikTok, “Photo with parent/guardian (if aged between 13 to 17)”, https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok#2

[21] H.B.ANo.A1181, Page 4, Line 1, https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB01181F.pdf#navpanes=0

[22] H.B.ANo.A1181, Page 4, Line 2 to 4, https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB01181F.pdf#navpanes=0

[23] HOUSE BILL NO. 142, Page 4, Line 10 to 16, https://www.legis.la.gov/legis/ViewDocument.aspx?d=1249878.

These to me read similar to the Australian Online Safety Amendment, but the onus is quite heavy on the platform themselves. There's no onus on the government body to create a solution and rather the focus is on handing out fines for non-compliance or completely banning a platform. Australia's bill, however, seems more hands on. I've said it like five times probably by now, but the government wants their hands to get dirty too. They want to create a digital ID, supply it and have social media platforms verify the age of their users with it. They want in too.

So, similar precedents but not exactly the same.

Okay, it's time. Let's chat about myID for a second because it's probably the best time for me to actually explain what the hell it is, especially if I'm so sure the government will use it as their digital ID in their age verification solution.

Well, it's pretty similar to something you've done probably hundreds of times before. I referred to it above, but you know how you can register with a website using Facebook? Or hit a "connect with Google" button to share your contacts Conveniently, it's quite similar. Although, only for government services.

myID acts as an identity and authorisation service for government services in Australia so you don't need individual accounts for each service. You're probably thinking, like I did, "Isn't that myGov?" Well, you're not wrong and this is where it gets confusing because it's a pretty typically bad government implementation. But we can really break it down into one, major factor: it's a digital ID.

To compare the two: myGov is a *portal*, whereas myID is a digital ID. myGov is a portal in a way that you can link your government services for access and use. myGov absolutely has your personal information on it, but myGov itself does not have documents or your tax file number or anything majorly sensitive on it; of course if someone had access to your myGov they could get all that sensitive information without a hitch, but myGov itself does not retain it, it's simply a gateway or portal to other services that do. myID, on the other hand, does—It has all your personal information and documents and the like. What myID also has is an identity strength feature. So, for example, some government services require a certain number of documents for verification and myID will have a strength attached to it which, if used, will determine if you meet certain government service criteria. Which is kind of whatever for this thing, but it's another *thing* it does. So really, it's kind of a big, heaping pile of a solution for identification, authorisation and verification.

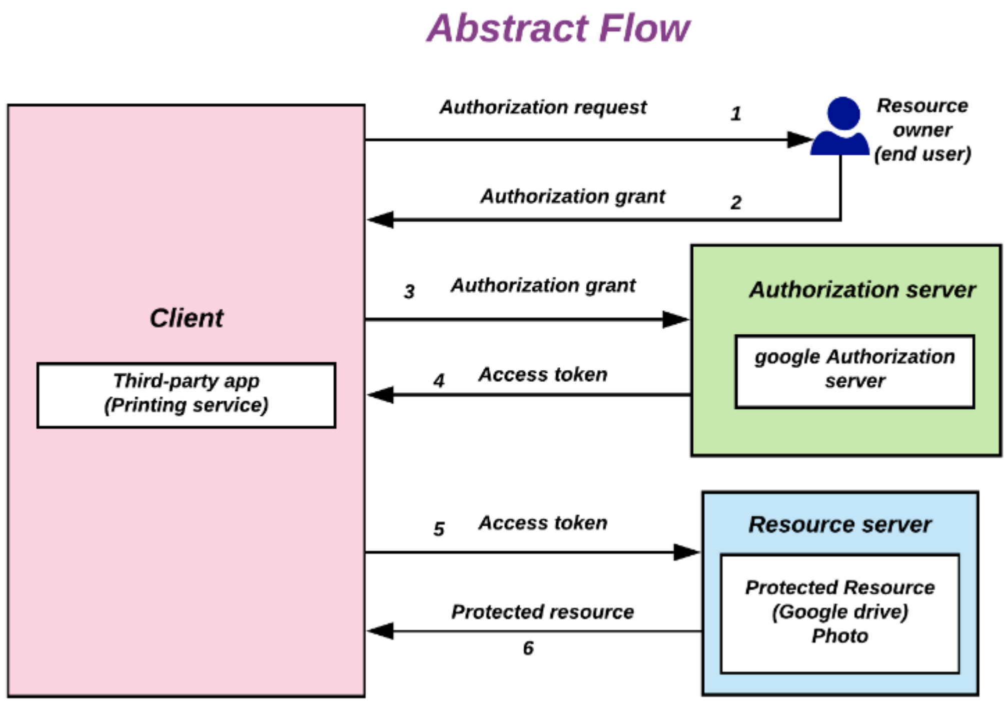
Also, as an aside, while myID and myGov may share the ability to login to the same platforms—myID can be used to sign into myGov, funnily enough—myID has way more services it can login to. One you may have heard of is The Medical Costs Finder Portal, which you may have also heard was a complete disaster. Anyway, this portal doesn't have any link to myGov but it does to myID, so it's kind of a strange relationship web you kind of expect from government solutions.

If I may also add to the confusion, myID was up until recently called myGovID which did exactly the same thing. It just so happens that it was rebranded to myID about five days before this bill was brought to the public. (Think about that one, too, okay? I love coincidences, and this one is juicy right?)

So, what's the technology is behind myID? It clearly performs database operations of some kind to store data, but as far as authorisation is concerned? Well, the Australian government has a bad track record of using anything modern and I couldn't find anything transparent enough to remark upon what it actually is, but from how it behaves it's pretty similar to OAuth—Open Authorisation.

You might have heard of it before, but it's basically an authorisation solution that allows application to application interaction without you having to use your password or maintaining a session at all times of the day. It's a sophisticated, robust solution and is the technology behind pretty much every single "login using Facebook" or "connect with Google" prompt you've ever seen. What makes it robust is that it's user driven and scope driven, meaning an application cannot suddenly request more data that originally intended or without user consent. The scope, in fact, is built into the exchange that happens. So if the scope changes suddenly, for example if an application in the pair suddenly requested "location" out of nowhere, the "exchange" would need to be reauthorised by the user; which point the user can look at the new scope and say "That's not for me, I don't want to share my location" and that's it. Of course, platforms are sneaky and sometimes mask scope so that people will just confirm a scope without really realising what it does, but before that happens you have at least some confidence that the scope your allowing will not and cannot change. It's very technically transparent, at least. If it's great at anything, it's that.

Here's a really great example diagram taken from Wikipedia of a normal OAuth flow [24]. The example flow starts from a login to a third party printing service, to then authorising access to a photograph on Google Drive for printing:



[24] Wikipedia, "OAuth", Image source, https://en.wikipedia.org/wiki/OAuth

The scope in this example is likely something like “read access” for a single Google drive resource. What that means is that there’s no way the third party printing service can suddenly pull down the whole folder without you or Google knowing. It’s locked down to a relationship between the printing service and this resource.

myID, seemingly, behaves similarly [25]. But instead of a printing service requesting authorisation for Google Drive and a photograph, government services request your personal information and documents to serve you adequately.

Obviously, in a perfect world, myID is well implemented. But I’m making an assumption about what myID is under the hood and that it’s being used correctly. After all, it could be some weird proprietary awful nonsense.

So there’s a lot of methods out there, right? Biometric, date of birth, credit card, identity documents, and yet there’s probably more I haven’t even see yet.

What I think we can take away from this is that the government likely won’t be building a solution using identity documents or credit cards to specifically verify age. While they may have this data and use document verification for other kinds of government services, it’s likely too unscrupulous to use here for age. They may also use identity documents to verify who you are with myID itself during registration, but not with a social media platform. That seems risky, right? And if a social media platform does that already, then they’ve already got your info, so why duplicate.

That leaves us with using biometric recognition and some kind of verification process with date of birth. And, really, I think the feasibility of both is very likely. Why? Because myID already has finger print and facial recognition. And obviously a date of birth verification is what we’re really concerned about here and really the only way to validate age, so biometric methods will be tertiary.

So while *I* don’t trust it, I think what exists in myID is enough to ponder on what a solution might be. So, moving further along, we’ll consider a what the government age verification solution might be like including the use of date of birth, finger print recognition and/or facial recognition.

[25] myID, “How to use myID”, https://www.myid.gov.au/how-use-myid

Solution

If there's anything I've learned from my time in technology, it's that the simplest solution is often the best one. I mean that in terms of the solution itself, as well as what the solution is built with. And while I won't be deluding this with technical engineering jargon (code), I do think that we can come up with a relatively simple government age verification solution from what we've already discussed.

So what *have* we already discussed? Let's go over that again. What we assume is: myID will be the place that holds our date of birth, biometric and other data, we cannot allow social media platforms to collect information from myID, we would like to verify the age of users using their date of birth, potentially use biometric features as a supplementary feature, and this applies to all users from Australia.

As probably obviously neglected in the section above, I did not explore solutions that were mobile driven. I also did not explore solutions that could sit at the browser plugin level or even at the operating system level. The reason I didn't do this is because based on the time of this *bill*, I feel that that's not going to be achievable. A plugin? Perhaps, but operating system level interactions require a lot of time and red tape nonsense, so I can't see that happening any time soon. So, this is not only the simplest but also the fastest solution. And because it just seems too coincidental that myGovID was rebranded, I couldn't help but bite.

So, what I see the solution as is… (drum snare) Making use of myID, a digital ID, as a form of age verification for social media platforms.

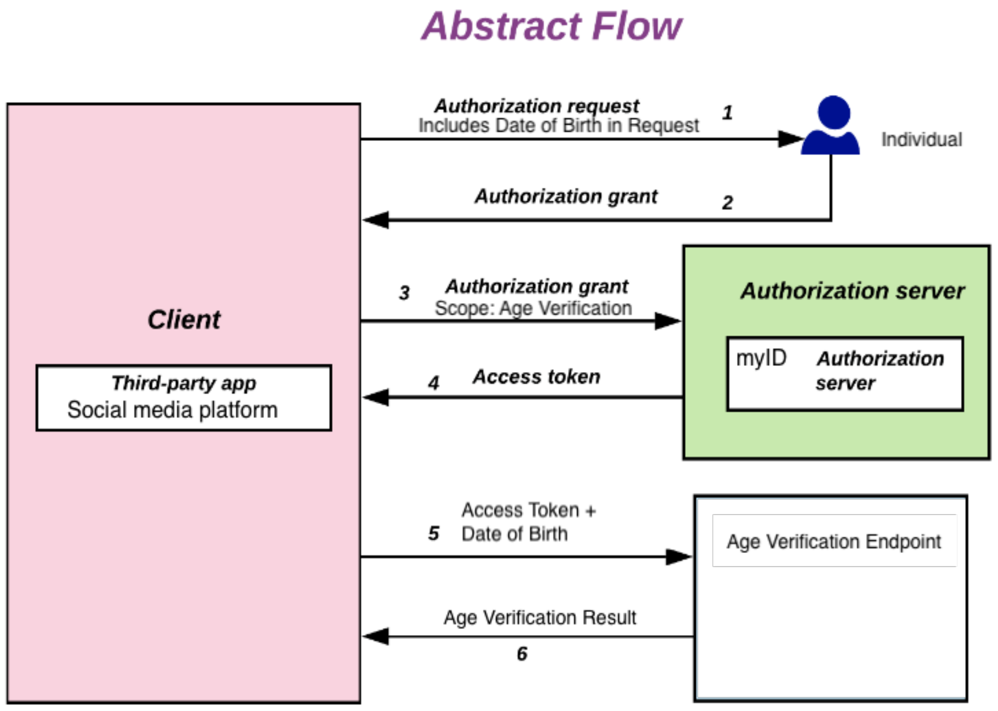
The question now is: How will this work? What kind of user flows do we need? What is the experience for a user verifying their age through myID? What kind of data might a social media platform request of myID, if any?

My thinking in how it will work is exactly how it works today for government services: you authorise through myID and receive access to a platform. However, I *really* don't see social media platforms using a "register with us using a digital ID" approach. These platforms are selfish, after all, and they want as much information from you as you can possible provide, so what I think is likely to happen is that you use your digital ID as an additional step. Which, while likely ugly, I think is probably the simplest approach. Okay, so: You will register/login as normal, but be presented another step that verifies your age using your digital ID—myID.

Further, in my opinion, I don't think a social media platform should request any data at all. Instead, myID should simply have a process in which you authorise a platform with myID, reach out to an endpoint and the "protected resource" that is returned is simply the knowledge of whether a user is of age. Maybe even a simple "Yes" or "No". But that's not realistic, unfortunately. What happens in the case where the date of birth recorded on the platform is not the same as what is in myID?

So okay, you might be thinking I think we should give social media platforms access to the date of birth inside of myID, but I don't think so. I think that opens a can of worms we can't close. Instead, I think, as per our OAuth diagram above, when the platform calls the resource server to retrieve the protected resource, *the platform* should supply *their* recorded date of birth so myID can do a comparison. The reason this is my preferred solution is because we completely eliminate the need for myID to grant access to the data it has. The scope required may be something like "age verification" which allows the platform to perform an age verification request, but it does not allow data from myID to be retrieved by the platform during handshake. It's like you're connecting Facebook to Google to post to your profile but Google doesn't not know *anything* about you or your data. We just want the functionality to do so.

Okay, so let's edit our OAuth diagram from above to show that:



What's happening here is the following: A user authorises with a social media platform. A date of birth is requested during the platform authorisation process. After this authorisation, an age verification process triggers. To do this, we authorise a connection between the social media platform and myID with the scope of "age verification"; meaning, we intend to use this connection to perform an age verification check with myID. When this succeeds, we make a request to an "age verification" endpoint with the platform date of birth and await the result.

This works well, right? Nice and simple. Shweet, let's move on!

So we've got OAuth style connection design defined, but how does it fit into a user experience? To do that, we need to define some flows.

In my opinion, we'll need a flow for existing users and another flow for new users. But before we define these flows, we have to ask what these flows have in common? Well, both flows have myID as a prerequisite, for without which a user cannot verify their age; they might have other means, but we're focusing on the government solution. Similarly, each flow does share quite a lot of the same handshake, meaning I can't see why existing and new users need to supply differing amounts information. I also don't see why myID needs to have different endpoints that serves the two purposes. As long as a user has myID, they should be equal. So let's say that's true. Let's say the requirements between each flow are identical, they are just within different areas of a platform.

Righto, I feel like we have enough information to start defining these flows now, so let's start with a new user flow (or, a registration flow):

1. A user lands on a social media platform registration page.
2. That registration page asks for whatever data is relevant for the platform, *including* a date of birth.
3. On submit, the platform, being aware that the user is based in Australia, will perform an age verification check using a digital ID—myID—supplying the date of birth that the user previously entered.
4. If the verification check fails or is cancelled, the registration ends.
5. If the verification succeeds, the user is logged in and has access to the platform and all its features.

As for an existing flow, I could see a functional "disabling" of the account if the age verification check fails. That is, until the age verification check passes/passes again. In this case, an existing user flow may be like:

1. An existing user of a social media platform logs in using their email/username and password as they have in the past.
2. When authenticated, a prompt will appear in the form of (maybe) a modal or an alert which states "Your account may be disabled very soon due to new age verification laws in Australia. In order to prevent your account from being disabled, please verify your age."
3. If decided to do so, the user continues.
4. The first thing that is required is that if a user does not have a date of birth selected, they must enter one. Platforms likely already have this, but just in case. If they refuse, the account disabled. If they enter one, the flow continues.
5. The user then goes through the handshake with myID, using their date of birth on the platform, and once verified they can continue using the platform.
6. If the handshake fails or is cancelled, the account is disabled, locked or frozen until rectified or deleted.

Golly gee! Those sure are some flows. I'm pretty happy with those, so let's start to round out the solution with some other considerations.

Something I've been batting around my head with this is: Does myID become mandated for use across all government services before this happens? And, does myGov become obsolete in the process? After all, to have both creates friction.

So, in my opinion, the answer is yes. But the reality of the situation is that we'll end up having two government logins for no reason. It won't make sense and people will hate it, but we'll have myGov for core government services and this single myID for social media platforms and fringe government services we hardly use. But hey, this is my solution right? So we'll mandate it. Every government service must move to this digital ID solution in myID.

So, does a teenager make an account with myID themselves? It serves me to wonder if they'll have the knowledge. But, let's say they do. When they turn fifteen, which is the minimum age for a myID registration by the way [26], a parent and/or guarding supports them in creating a myID account. And so by the time they're legally permitted to register for a social media platform, they'll already have a myID account setup and ready to go. If they don't, they'll obviously need to create one before they can experience any of the flows mentioned above.

Another consideration is to bring up transparency within myID to see which social media platforms are already authorised. The platforms will obviously show the link because they've been using OAuth forever, they'll also likely have the ability to add or revoke the authorisation from their end too, but I can see the need for myID to have a list and log of activity of all the connections you have made. Nothing is inappropriately stored to be security conscious, but maybe a simple list exists so that a platform can be revoked at any time; this would then trigger the need to reauthorise within the platform and is up to the user to reauthorise or ignore it.

Probably another factor, based on this, will be reauthorisation throughout normal user behaviour. I'm not implying that a user will have to keep authorising their age, but likely if a user signs out or something with their browser changes, I could see a background reauthorisation happening to ensure the user is still of age. All through OAuth too, so the only time the user knows this is happening is when it breaks or their age is lowered through some strange means.

Oh, maybe the reauthorisation is for if the user changes their date of birth on the social media platform. Like sure, go ahead, but you'll need to reauthorise that this is true and valid. Why? So that there's no funky disconnect between the date of birth they have and the one myID has; meaning someone could connect for the first time and then change their age later on. I did originally think of disabling the date of birth field so maybe that's an option too, but also more work for a platform.

Before we pat ourselves on the back, there's one major flaw in this that I can see being abused quite easily. I thought about this flaw while I was writing my initial draft and I even originally wrote it as an assumption, but I'll put it here instead because it fits nicer here in the solution part of the discussion.

So, we can authorise a social media platform account with myID. Great. However, what's stopping us from authorising another account for that platform and just giving it to my friend? What if I don't care about my data and use myID freely and so I just make a bunch of accounts and hand them out to all my friends? Nothing, currently. So, I'm going to do the governments job again and fix a flaw.

This is an easy one to fix too, but might be kind of controversial. The solution is really simply: You can only have one kind of social media platform account

[26] myID, "How to set up myID", https://www.myid.gov.au/how-set-myid

authorised per myID account. Although I think this is kind of cheating, I do think it's something the government is likely to adhere to. They obviously don't know much about social media as it is and the idea that someone might have more than one account is probably incomprehensible, unless a senator out there is cheating on their spouse or something, so this kind of functionality will be imposed. I don't see a problem with authorising and revoking again and again and again with many different accounts, perhaps with a limit or delay, but multiple simultaneous authorisations with one social media platform will likely be forbidden.

I'm too tired to think of anything else, so I'm happy with what we have. Let's summarise what we've got, look at some risks and then retire for the night.

Hey, wait a minute… did we just create the solution *for* the government?

Ah, crap. Sorry, didn't mean to do that. But you see how easy that was, right? Even if I'm avoiding doing any actual engineering, it's not a very hard solution to produce and something you could do with a very small team and very easily. Not only is it simple, but it's also quite secure and free of data exchange. OAuth is doing a lot of the heavy lifting, rightfully so, and much of the interaction between a social media platform and myID is user driven, so it's a solid idea.

However, I do see this being way more complicated as delivered through the government. I could whip up something like this over the weekend because I'm not burdened by red tape or contracts, so I'm assuming this won't be as easy as what I've done here. It could be and we could all be surprise, but likely not.

So let's summarise our solution so the government has to give us credit: In order to protect children under the age of sixteen, we propose a solution whereby myID acts as an OAuth authorisation service that provides an "age verification" scope and resource for social media platforms. When a social media platform is authorised by the user, an age verification process begins with the option of using myID. On a success, the platform allows access to the platform and on failure the platform access is disabled. For parity the platform will supply a date of birth to myID during this verification and only one account may be authorised at a time.

Gosh, how clever are we.

Risks and Challenges

I’ve been babbling on about this implementation for so long that it’s time we actually look at the impact of this thing. We can talk implementation all day but what’s the actual reality of this? We kind of already know the impact existing solutions have had (“We’re dealing with it right now, dude!”), but what impact with this one have? And, will there be further changes as a result?

So, how do we bypass this whole process? That’s the first thing I think of when designing something like this: How can I break it forever?

It’s simple, really. I can register with iCloud and turn on Private Relay—setting my country somewhere without age restrictions—and I’m done. Easy, right? I just avoided the age verification. I mention iCloud first because it’s more user friendly to setup and likely is already turn on for iCloud users, but obviously you can use a VPN too and do the same thing as I might with Private Relay. Boom. Bypassed. That means I can use social media platforms before the age of sixteen.

What else can we do? Well, choosing platforms that don’t have age verification is another one. I can basically get my friends together and hop between platforms until we get kicked out or asked to verify our age. That’s any easy one. Oh, and you know, what if I had a friend overseas? I could ask to create an account or purchase one from someone and use that because it won’t get age verified. Nice.

But what about myID? Can I specifically fudge that at all? Well, I just mentioned account purchasing so I imagine that’s a feasible route too. Like, of course myID touts being fairly secure and you need official documents to register, but I’m still thinking about someone creating numerous myID accounts under multiple names, giving them to teenagers and them just registering social media accounts under false names. That, I think, is likely possible and very likely punishable too. Particularly to the person selling the accounts. This kind of scenario, however, is the reason I specified that you can only have one social media account authorisation per platform, because I can really see someone taking advantage of the system like this by having an account and authorise like fifty social media accounts for their siblings and friends. Fortunately, the solution protects against this and so one user cannot have an insane number of accounts authorised with their myID, but as far as forgery is concerned you really can help that as much. If a person has your documents and data, there’s nothing stopping them from registering myID in your name and authorising with however many social media platforms.

Alternatively, I do think there is a more softer socially engineered version of the above that isn’t all stealing and selling. Like, you just might have a “cool” parent. That’s all it takes. And the cool parent is just fine with their child being on social media platforms before they’re sixteen so they let them use their myID account or they register a myID account just for the child to use. So, they’ve just bypassed this entire thing without anything fancy. I think this one in particularly is pretty likely, especially if a parent, guarding or even sibling doesn’t really have the desire to use social media but the child does. This even more especially likely given parents will receive no punishment, according to the bill [27].

So yeah, for now, those are some good social engineering options, no?

Another easy oversight is like, international students. I don't know exactly if you need a myID to deal with your visas and other documents, but I could see international students sliding by with this. They're not technically official citizens, so my feeling is that the government will only impose this on them if they're made a permanent resident. I think there's a lot of challenges surrounding this and so there's a good chance the government just lets this slide for them. Which is fair, like they didn't come to this country to get age verified by another government only to return home and still have this weird link on your account for no reason.

I also think social engineering challenges may be present here again when you think about the mingling of international students and local students. Like, it's totally possible for local students to just make friends with an international student and ask them to register an account for them and start using a platform as we see it today. In fact, if I was still a student and I wanted to use a specific platform, that's probably the route I would take because Australian internet connections are so slow that adding a network layer like a VPN is a death wish. So there's another circumvention too.

One big thing we *have* to discuss as well is namely around education and safety.

What I've been seeing a lot of people suggesting, instead of this whole fiasco, is implementing educational programs to teach young people what to avoid and how to disseminate information online, because right now they're not taught anything like that. I was fortunate to grow up in the whole "don't believe anything you read or see online" space, so it's *so* engrained in me that it's a personal character flaw. But when you're not brought up without that backbone, social media can really scare you. Like, you can come across things that aren't real and they'll frighten you to your core because you don't really know if they're real or not or if the person you're talking to is who they say they are. And even though I have a predisclosed flaw that prevents me from taking anything seriously, I can still get swept up in whatever I see.

So while the government thinks this is a good thing, I think they fail to realise that leaving this as the only solution is not really good enough. You also have to teach young people how to be more critical online, how to protect themselves and their friends. Just because you change the law to be sixteen and leave it at that, it doesn't necessarily mean young people will have the immediate cognitive emotional development required to get out of social media unscathed. After all, we've seen adults and even seniors collapse under the weight of social media because they didn't know how to handle it or made some silly, easily resolved mistake. Social media sucks for sure, but it's become a part of life. So knowing how to protect yourself and others is an important step.

[27] For some reason I can't find this anymore but I did read this somewhere. I apologise if this is no longer the case.

Another weird oversight is like, thinking bullying doesn't exist after you turn sixteen. I was quite lucky in high school in that we didn't really have bullying *that* much, people just kicked the shit out of each other if they disagreed and moved on, but I always heard from friends or peers in other schools who said the bullying got so bad towards graduation that they almost killed themselves—not at sixteen, older. Like bullying totally will continue before and after this, unfortunately, so it's not as much of a solution to that as we think it is. I will say, though, young people are getting more aware of this kind of thing so maybe in time this naturally prevents that. But permanently? We'll have to wait and see.

I also think we might see a different kind of bullying because of this. Like, I think we'll start to see a bit of separation with regards to young people who actively ignore this law and use social media platforms anyway and those who do wait and use the mandated age verification solutions. Like, imagine you're a good young person and you wait the whole time—You wait until you're sixteen. But when you turn sixteen, you find out that your friends and peers have been on social media for *years* longer than you and haven't included you at all and *that's* where they've been bullying you—talking about you behind your back. That's an awful, heart breaking thing. And, potentially, really scary. Maybe your friends will be really cool and guide you through it all nice and sweetly, but maybe they won't either.

A lot of this stuff I'm talking about is very socially hyperbolic and we have no real way of backing it up, but I am interested in the technological repercussions from such a thing. Like, how far do we go to protect the young people? Like, say what I'm talking about above does come into play and bullying, suicide, sexual assault and the like continue unreported. What happens then, you know? Parents are obviously frustrated that it isn't working as promised, so what happens?

For starters, I think we'll see features on these platforms blocked or we'll get more streamlined, dumbed down versions of them. For example, maybe young people under eighteen don't see any advertisements at all. That's kind of an okay one and something I wish was for everyone, but let's ignore that for now. So maybe this moves onto other feature, like young people under eighteen don't see community features, they don't see public posts, they can't participate in public things or register for events. The only thing you *can* do is interact with an immediate circle of friends and family and nobody else. It locks things down, but does it help?

Cool, okay, say it does help—removing advertisements and community interactions helps. But what happens if you start being bullied by your close circle of friends or even by a relative outside your family home? How can you prevent that kind of thing from happening and how can you monitor your child's social media to make sure it's not happening or they aren't doing it themselves? After all, parental fatigue is a huge factor, according to the amendment. Parents clearly don't want to be swimming in this changing landscape of social media, they want a strong footing to be able to disseminate it all. But like when your children turns sixteen, it's going to all rush in at once and be really quite overwhelming. New platforms, so many messages. This will be hypocritical of me to say, but in this respect I'm actually on the side of the parents because isn't this simply more technological fatigue?

The next clear step is actively monitoring activity. I can see an end where conversations and the like are logged and stored in myID or the social media platform whereby if there’s a dispute about bullying or if a parent wants total access to their child's social media, they just go through myID to view it all or even as a kind of backdoor to browse the platform unfettered. But then that’s a huge privacy concern there too, like doesn’t that imply that the government can also use this backdoor?

Another addition may be creating parental controls within myID. Perhaps even a step where a parent has to approve the social media platform authorisation before their child can authorise themselves so the parent knows *exactly* what the child is using. Which sounds reasonable from a technical perspective, to be frank, but I wonder if this is again too much technological fatigue for a parent?

But these added solutions may not be easily enforced. Social media platforms really really love showing users their new features, so it’s likely they will push back on this much more than they have with this blanket ban. And installing all these backdoors for government or parental access—Surely they would hate that too?

So that’s enough of that. Let’s be more technical. What’s wrong with my solution? It’s pretty simple, clearly, but what is it doing wrong?

The use of myID is a big one. It really could be a huge red herring and I’ve just decided that it’s a digital ID they want to use for this and this whole discussion is blown out of the water. I’ve elected to think of it as the solution because of convenience and the fact that it is considered a digital ID already, but the honest truth is that I have no idea if that’s really the case. Given the confusion I have myself surrounding myGov and myID, I wouldn’t be surprised if the government decided to start from scratch with a solution that we’ve never heard of. And really, that’s entirely a possibility. The risk there is much clearer in that we have no idea what it would entail or would that would be. The behaviour might not be at all *like* OAuth and be some totally new proprietary technology that hasn’t even been designed yet.

I keep hammering this “proprietary” word too because the government, while being frightful of third party solutions, is *so* frightened of open source solutions and protocols. Not only have they not implemented them correctly in the past, but they’re so afraid that a laymen will find a back door that they don’t trust them. So the concern here is that while I can buff up this whole thing and think of myID as an OAuth solution, I have no idea if that is true. And they might not even use myID at all. And given the government’s track record, by next year we’ll have myGov, myID and myDigitalID or something that confused everything all the more.

Let’s also talk about the idea of *read* access. So I basically died on the street realising my original naive mistake with this, which you can lambast me for if you desire, but the government has not specified if a social media platform can *read* any of the information from identity documents or a digital ID.

It probably seems obvious with regards to identity documents because if a company is building something themselves they absolutely have to read these documents to verify them, but do you *really* need to give platforms access to myID for this? This to me is not just an oversight but a smoking gun for potentially a major data breach down the line. And it’s not for reasons you think.

Of course there's a chance that a bad faith actor can create a fake application and start fishing people’s personal data. *Of course* they can. So what can we do about that? There’s not *much* you can do exactly, social engineering is a funny thing like that, but what you can do is make every single platform who wants to use this government age verification solution go through a rigorous approval process. This happens with platforms like Facebook already (I go into this next, so stay tuned) and basically a team over there looks through your solution and verifies it’s okay for production; you're not harming anyone, the technical solution is sound and secure and reasonable, etc. You also have to supply a *lot* of business documentation to prove that you are a legitimate business, or if you're a sole trader the documentation or contracts you received to do so. It’s all really stringent, which is a good thing but that doesn’t mean you can just fake it anyway and an inspector at Facebook is having an off day and lets you through. But this *does* help.

My fear with this idea though is that government employee positions are so like, volatile. You *need* this to be a department within the government because you cannot trust a third party with this. But that’s an issue because while one year we could have a team of twenty employees reviewing and inspecting solutions for approval, the next election cycle we could see the entire department gutted and replaced with a single person who becomes overworked and easily manipulated.

And even if we have all this kind of stuff, we have to still deal with development teams. Yeah, that’s right, I’m going to attack developers. What’s that? Hey! Hey, stay back! Don’t hurt me! Please! Okay, okay, look. *Look.* I’ve been around technology for awhile now and you start to see patterns. One of the patterns I’ve seen is that requirements gathering is almost always wrong. No matter what kind of requirement you have, even if it’s like “Change this to purple!”, *something* is going to go wrong—maybe not today, maybe not tomorrow, but like a month later someone will invariable ask “Why did you choose *this* purple?”. There’s a lot of companies out there that have dedicated teams to gather requirements and take months to do so, but once the solution is made and hits the public there’s always a massive flaw that nobody thought of; it’s why the industry technology is so expedience focused now, so you can fix and change stuff really easily. Government work is always like this. But something really sinister in this is like… human beings. Everyone tries to do good work, but sometimes you slip up. And sometimes, when you see a requirement that says “you cannot *collect* data” you misinterpret it during your technical exploration phase because the data is *readable* and so you build an entire solution that rests on needing to collect data. And then that solution goes into production and suddenly you’re breaking the law without realising it. This might seem like I’m speaking from experience, and I am. But like, for way more negligible stuff I mentioned previously: *the colour purple*.

So even though this is what the law states, that doesn’t mean it will always be reality. Humans slip up all the time and it’s only a matter of time, really. Which is why I was really hoping the law would read “you cannot *collect* or *read…”*. I even predicated my entire solution on it because that’s how ridiculous the idea is, especially for a government solution. Like of course it makes sense for interoperational government services, but for a social media platform?

Give me a break.

This leads into one final thing to consider and I'll send you on your way. And that's when OAuth is implemented lazily or frustratingly, it can be quite damaging.

You remember the Cambridge Analytica leak? The authorisation system in Facebook wasn't as tight as it is now and basically gave you an open scope to harvest like hundreds of thousands of Facebook users and their data for your discerning purposes. This was a huge, huge deal and it fundamentally changed the way Facebook operates and interacts with third party developers.

Things changed for the better, but I have to say that even with all this, you could still get a lot of information from Facebook users if you were determined. Like, some endpoints you could just call to get user profiles with any scope applied. Further, and I didn't experience this personally because the company I worked for at the time was great about explicit data consent and stuff, but some other companies were obfuscating the kinds of scope that were being authorised by the user and using flowery language like "[platform] *may* request your email to use in…" or "[platform] will not use your email for…" but then using it for something sinister anyway.

So what frightens me with an implementation like this is that the government may provide a "default" scope of access to social media platforms that contains a lot of your personal data for absolutely no reason. I really, really hope this is not the case because it would be such an awful, awful thing and incredibly short sighted.

Conclusion

So what was this whole thing about? I wrote the first draft of this over a weekend to quickly try to understand a possible implementation and the risks. But why?

I think I was mostly curious about what a government age verification solution might look like. I've seen other stuff before, but would a government one be the same? What would be different about it? And I did learn a lot. I obviously didn't know about myID and I still don't really know much about it now, but knowing what is feasible has given me a kind of confidence for what we might see in the future. Will any of this actually happen? Maybe, maybe the government will surprise us and show us there's a safe way to approach it. Who knows. Ultimately, though, if the government solution *is* like the above, it's not *as big* of a deal as I thought it was. If it's a really small interaction that really doesn't expose much of anything, then that's *okay*. Would I use it? Probably not. Would I tell others to? Probably not again. After all, I don't trust having all that information in a digital ID that *can* connect to a non-government based third party, but I wouldn't go crazy to avoid it either. I would just not use it, really. Truthfully, all the risk lies entirely within myID but even so this method of interaction is so low friction that the risk is also low. Anything more complex I would be very wary of, though, because like why does it need to be?

So where do we go from here? What's the next? I'm personally not much of a heavy social media user and so the impact for me will likely to disconnect from the one I use if this is how it is, but what about the average person? People online detest this with appropriate levels of disgust, but what about the average person?

I personally think that quite a number of people don't really care about this. Specifically, I think a certain generation may not care at all and in fact willingly authorise a digital ID with a social media platform without thinking at all; perhaps even getting angry that the whole process is really quite ugly. But for younger people, aside from the most obvious impact, I do think there will be a lot of avoidance. And it will only further increase when the government and parents realise that this is not *exactly* as much as a fix as they realise—it opens up a lot, and I mean a lot, of new avenues that may be good but also may be horrifying. So lots of VPN usage, lots of other work arounds. Young people are smart, they'll figure it out. The punishment really lies on the end of the platforms, after all, and so if there's any good from any of this it's that platforms might actually start to care about their under age users. Will it be in the right way? We'll just have wait and to see.

And, you know, unfortunately, this whole circus can be summed up that way: We'll just have to wait and see. We'll just have to wait and see.

References

Online Safety Amendment (Social Media Minimum Age) Bill 2024, https://parlinfo.aph.gov.au/parlInfo/download/legislation/bills/r7284_aspassed/toc_pdf/24150b01.pdf;fileType=application/pdf

Digital ID Act 2024 https://www.legislation.gov.au/C2024A00025/asmade/text

myID, “myGovID is now myID”, https://www.myid.gov.au/mygovid-now-myid

Facebook, “Confirming your age on Facebook”, https://www.facebook.com/help/958848942357089

Facebook, “Create a new account”, https://en-gb.facebook.com/reg/?ty=tytrue

Yoti, https://www.yoti.com/

Yoti, “Age Verification”, https://www.yoti.com/business/age-verification/

Youtube, Yoti, “How to use Yoti facial age estimation online”, https://youtube.com/watch?v=Xr-JtYhXj0c

Facebook, “Age Verification”, https://about.fb.com/news/video/age-verification/

Instagram, “Introducing New Ways to Verify Age on Instagram”, https://about.instagram.com/blog/announcements/new-ways-to-verify-age-on-instagram

IDVerse, “Age Verification”, https://idverse.com/products/age-verification/

Google, “Access age-restricted content & features” , https://support.google.com/accounts/answer/10071085?sjid=16739457453252018244-AP#zippy=

Youtube, Age Check Certification Scheme, “OCR & Doc Authentication, Terry Brenner, IDVerse”, 0:56, https://youtu.be/iQXqy1PPxAg?t=56

TikTok, “Facial age estimation (if aged 18 and over)”, https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok#2

TikTok, “Credit card authorisation (if aged 18 and over)”, https://support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok#2

Tiktok, “Underage Appeals On Tiktok”, support.tiktok.com/en/safety-hc/account-and-user-safety/underage-appeals-on-tiktok#2

H.B.ANo.A1181,https://capitol.texas.gov/tlodocs/88R/billtext/pdf/HB01181F.pdf#navpanes=0

HOUSE BILL NO. 142, https://www.legis.la.gov/legis/ViewDocument.aspx?d=1249878

Wikipedia, “OAuth”, Image source, https://en.wikipedia.org/wiki/OAuth

myID, “How to use myID”, https://www.myid.gov.au/how-use-myid

myID, “How to set up myID”, https://www.myid.gov.au/how-set-myid