Fraser Tweedale
foi+request-7565-3bb53558@righttoknow.org.au

September 8, 2021

General Counsel
Australian Taxation Office

Dear Australian Taxation Office,

Reference: 1-Q1HU99Q

On 10 August, 2021 you made an access refusal decision on my Freedom of Information request, reference **1-Q1HU99Q**, for the source code of the upcoming release of the myGovID Android application. Under s 54(2) of the Freedom of Information Act 1982, I am applying for an internal review of the decision. Below, I give the reasons why I disagree with the decision and discuss some additional factors that may not have been considered.

Section 47(1)(a) Trade secrets

The original decision stated:

> Source code has previously been found to be a trade secret for the purposes of the FOI Act, see Cordover and Australian Electoral Commission (Freedom of information) [2015] AATA 956 (11 December 2015).

The finding of fact in *Cordover and Australian Electoral Commission (Freedom of information)* [2015] AATA 956 (*Cordover*) was that because the AEC issues licenses on commercial terms to third parties to use EasyCount in compiled form, the EasyCode source code is a trade secret:

> 32. It is plain that the information must have commercial value and be used in or usable in trade. There was ample evidence from both Mr Lee and Mr Jones to the effect of the generation of income from being contracted to conduct elections using Easycount and also from licensing of it to other entities.
> 33. For the above reasons, the Tribunal is satisfied that the Easycount source code is a trade secret and is exempt from disclosure because of section 47(1)(a) of the FOI Act.

It is incorrect to infer that because *Cordover* found the EasyCount source code to be a trade secret, all source code developed and held by government agencies is a trade secret. *Cordover* affirms that:

> 26. Ultimately, whether or not information constitutes a trade secret is a question of fact to be determined in the circumstances of each case.

Therefore it is necessary to determine whether the source code of the myGovID Android application is a trade secret by applying the test given in *Guidelines* s5.200:

- the information is used in a trade or business
- the owner of the information must limit its dissemination or at least not encourage or permit its widespread publication
- if disclosed to a competitor, the information would be liable to cause real or significant harm to the owner of the information.

While it is clear that the second part of this test has been satisfied, the myGovID Android application fails the first and third parts of the test.

The myGovID system is not used in a trade or business. It does not generate revenue for the ATO nor directly relate to any particular income stream. It is a system for authenticating to a range of government services provided by the ATO and other government agencies.

In the *myGovID Terms of use - User* (https://www.mygovid.gov.au/mygovid-terms-of-use-user), the ATO affirms that the myGovID Android application, along with other parts of the myGovID system, is provided without charge.

> The myGovID system includes each of the myGovID service, the myGovID credential and the myGovID software. To the extent permitted by law, the ATO:
>
> - provides each of those elements of the myGovID system "as is" and without charge

For these reasons, the myGovID fails the first part of the test - *the information is used in a trade or business.*

The myGovID system also fails the third part of the trade secret test because there is no commercial competition in providing authentication mechanisms for government services, and because the myGovID service and applications are not used by the ATO in trade or business.

For these reasons, the myGovID Android application is not a trade secret and its source code is not exempt under s 47(1)(a).

Section 47(1)(b) Commercially valuable information

The original decision noted under heading *Trade Secrets* that:

> The ATO has invested a significant amount of information and time in developing the myGovID applications.

Guidelines s5.206 states:

> The time and money invested in generating information will not necessarily mean that it has commercial value. Information that is costly to produce will not necessarily have intrinsic commercial value.

The original decision states:

> The FOI Guidelines also provide a list of factors that may assist in deciding whether information has commercial value. I have taken these into account in reaching my decision.

However, there is no elaboration at all of the factors that were taken into account (be they from the *Guidelines* list or not) and how they weighed on the decision.

There are 5 factors in the *Guidelines*. The first factor is:

> whether the information is known only to the agency or person for whom it has value or, if it is known to others, to what extent that detracts from its intrinsic commercial value

This factor is enlivened only if it is established that the myGovID Android application source code has commercial value.

The second factor is:

> whether the information confers a competitive advantage on the agency or person to whom it relates — for example, if it lowers the cost of production or allows access to markets not available to competitors

The ATO provides the elements of the myGovID system without charge (see above). In relation to the myGovID Android client application, the ATO does not compete, in any commercial sense, with any other entity.

The third factor is:

> whether a genuine 'arm's-length' buyer would be prepared to pay to obtain that information

Without disclosure of the myGovID source code, it is difficult to estimate the degree to which myGovID is similar to, or different from, other authentication systems. There are two possibilities:

1. myGovID is substantially different from publicly documented authentication systems. In this case, the Android application is coded to work specifically with the myGovID system, and will not interoperate with other systems without substantial modification. Therefore it is not reasonable to expect that an arm's length buyer would be prepared to pay to obtain the source code of the myGovID Android application.
2. myGovID is substantially similar to some existing authentication system, the protocol of which is publicly documented. In this case, software systems already exist for interacting with those authentication systems. It is very likely that these would include applications for the Android platform. Therefore in this case also, it is unreasonable to expect that an arm's length buyer would be prepared to pay to obtain the source code of the myGovID Android application.

The fourth factor is:

> whether the information is still current or out of date (out of date information may no longer have any value)

The source code of the specified release or build of the myGovID Android application that is the scope of my request is indeed current. But that is not evidence that it has commercial value.

The fifth factor is:

> whether disclosing the information would reduce the value of a business operation or commercial activity — reflected, perhaps, in a lower share price

The ATO provides the myGovID Android application without charge, via the Apple App Store and Google Play Store. The disclosure of its source code would not reduce the value of a business operation or commercial activity of the ATO.

Guidelines s 5.207 states:

> The second requirement of s 47(1)(b) — that it could reasonably be expected that disclosure of the information would destroy or

> diminish its value — must be established separately by satisfactory evidence. It should not be assumed that confidential commercial information will necessarily lose some of its value if it becomes more widely known.

The original decision did not provide any evidence in support of its determination that the commercial value of the myGovID Android application (if there is any) would, or could reasonably expected to be, be destroyed or diminished were its source code to be disclosed.

For the reasons given in this section, I argue that the myGovID Android application source code is not exempt under s 47(1)(b).

Third-party code

The original decision noted that:

> I further understand the source code contains or will contain components commercially licensed to the ATO.

I accept that the source code of any components commercially licensed to the ATO under terms that prohibit disclosure or redistribution, and which form part of the myGovID Android application, would be exempt.

It is likely that such components are separate from the rest of the source code, in the sense of being separate files, whether in compiled (binary) form or source code. Identifying and excluding them should be a simple matter.

Mere references to such components from other files would not make those other files exempt. Such references would merely disclose the existence and usage of particular commercially licensed components within the myGovID Android application - they would not disclose the implementations (content) of those components.

Section 47E(d) Public interest conditional exemptions — certain operations of agencies

Applicability of Section 47E(d)

In the original decision the ATO determined that:

> Releasing the source code would provide an authenticated version of the source code to the general public. This could be used to masquerade as myGovID, and allow malicious individuals to exploit any potential vulnerabilities in the system. I consider that this would, or could reasonably be expected to, prejudice or a

> have a substantial adverse effect on the security and effectiveness of the ATO's digital identification and verification operations.

There are two facets to this argument: *counterfeiting* (*masquerading*) and *exploitation of vulnerabilities*. I will address each separately. For both facets, I argue that disclosure could not reasonably be expected to have a substantial adverse effect on the security and effectiveness of the ATO's digital identification and verification operations. These arguments together constitute my argument that the myGovID Android application source code is not conditionally exempt under s 47E(d).

Counterfeiting

The "terms of use" of the myGovID system, including the Android application, stipulate:

> You may not:
>
> - decompile, reverse engineer, disassemble or attempt to derive the source code for the Software
> - create derivative works based the Software or modify it in any way
> - distribute copies of the Software or versions of it.

Even without access to source code, it is a straightforward matter for a person experienced in Android app development to develop a counterfeit application that could masquerade as the myGovID application. It is sufficient to study the appearance and behaviour of the compiled application, and extract its media assets (sounds, images, animations, etc), then build a program that is superficially similar in appearance and behaviour. An experienced engineer can deduce a great deal from the object code, text strings, and network activity of a program.

It is obvious that such activities violate the myGovID terms of use. Nevertheless, it is reasonable to expect that someone who has formed the intent to create and distribute a counterfeit application would not hesitate to violate the terms of use to gain an advantage.

For these reasons, access to the source code is not a prerequisite for creating a malicious Android application that masquerades as the myGovID application.

After creating a counterfeit application, the problem of distribution remains. That is, how will the malicious counterfeit application actually get installed on user devices?

The ATO distributes the Android myGovID application exclusively through the Google Play Store. Similarly, the iOS version of the myGovID application for Apple devices is distributed exclusively through the Apple App Store. The iOS version is not in the scope of my request, but it is useful to consider the advantages and disadvantages of the general "app store" distribution model.

"App stores" provide access to curated collections of applications for a particular device or family of devices, and a mechanism of secure distribution of those applications (possibly for a fee, though myGovID is provided without charge). The Apple App Store is managed by Apple, and the Google App Store is managed by Google.

Overwhelmingly, users of Android devices use the Google Play Store as the primary and default way to find and install applications on their device. It is possible for advanced users to install applications from other sources, but it is reasonably expected that such users know how to, and would, authenticate such packages.

The Google Play Store prominently displays the publisher of every application. This information comes from verified information about the owner of the account that publishes the application. In the Google Play Store, the publisher of the myGovID app is prominently identified as the Australian Taxation Office. A counterfeit application would prominently identify a different entity as its publisher.

Google Play Store Terms of Service prohibit applications that impersonate other applications. The Google Play Store application has a feature to report problematic applications, such as counterfeits. Google also allows developers to submit removal requests for applications that violate the Terms of Service, infringe on trademarks or copyright, or violate other laws. Google also takes proactive steps to remove counterfeit applications from the Google Play Store.

To summarise my arguments in this section:

- Source code is not a prerequisite to developing a counterfeit application.
- The "app store" distribution model provides significant safeguards and recourse against counterfeit applications. These safeguards are at work, and resource against counterfeit applications may have to be taken, whether or not the myGovID Android application source code is available to the public.

- End users will overwhelmingly download the myGovID application from app stores. It is reasonable expected that users who install it from other sources would be advanced users who would take steps to authenticate the application bundle before installing it.

For these reasons, I argue that with respect to the counterfeiting concern, releasing the source code of the myGovID Android application would not prejudice or have a substantial adverse on the security and effectiveness of the ATO's digital identification and verification operations.

Exploitation of vulnerabilities

Access to source code is not a prerequisite for finding potential security vulnerabilities in a software system. The cybersecurity industry deals with an endless stream of vulnerabilities in software, information systems and network protocols. Many vulnerabilities are discovered without any access to source code. Indeed, security researchers who had no access to the source code have discovered and disclosed weaknesses in the myGovID system and applications (https://thinkingcybersecurity.com/DigitalID/).

Access to source code could reveal potential vulnerabilities to persons motivated to exploit such vulnerabilities that would otherwise have been harder to discover. However, counterbalancing this is the fact that source code could reveal the same vulnerabilities to persons who would responsibly disclose those vulnerabilities so that they can be fixed or mitigated.

There are many ethical people with skills in software development and application security, and an interest in the security of the myGovID system. Public disclosure of the myGovID Android application source code would attract considerable attention and analysis by such people, who would responsibly disclose any vulnerabilities they discover to the ATO, ASD or other relevant agencies.

The ATO noted in correspondence dated 28 July 2021 that the ATO does perform (and/or commission) critical security analysis work related the the myGovID system. Therefore it is not reasonable to expect that there are castastrophic flaws in the myGovID system or the myGovID Android application awaiting discovery upon release of the source code.

For these reasons, I argue that with respect to exploitation of vulnerabilities, releasing the source code of the myGovID Android application could not reasonably be expected to have a substantial adverse effect on the security and effectiveness of the ATO's digital identification and verification

operations.

Public interest factors

If found to be conditionally exempt under s 47E(d), then it is necessary to weigh the public interest factors favouring and against disclosure and determine whether access is contrary to the public interest. Non-exhaustive lists of factors favouring and against disclosure are given in *Guidelines* s 6.19 and s 6.22, respectively.

The original decision stated:

> While there is some public interest in promoting the objects of the FOI Act, this in my opinion is outweighed by a stronger public interest in protecting the security of the ATO's digital identity services as a Commonwealth agency.

The only factor favouring release that was considered was 6.19(a), *promotes the objects of the FOI act.* The single factor against release was the security concern, which appears to lie in scope of 6.22(c) *could reasonably be expected to prejudice security....* The factor against was considered to outweight the factor in favour.

The release of the myGovID Android application source code engages several public interest factors favouring disclosure that were not weighed in the original decision. I discuss the factors favouring disclosure in the following subsections.

6.19(a) promotes the objects of the FOI Act

The original decision seems to agree that the release of the source code would promote the objects of the FOI Act, though it does not go into further detail. Two objects of particular relevance to this request are 3(2)(a):

> increasing public participation in Government processes...

and 3(3):

> ...increase recognition that information held by the Government is to be managed for public purposes, and is a national resource.

6.19(b) inform debate on a matter of public importance

The myGovID system is currently used for authentication to a number of government services operated by several agencies, including the ATO. For some services, myGovID is one of several authentication options, while for others (such as *Business Portal*) it is the only option. It is being adopted

by more services over time. It has been adopted by services used by a great many citizens, such as *myGov*.

Because it is very widely used and mandatory for some government services, transparency about the development, operation and security of the myGovID system, and its constituent components including the Android application, is a matter of public importance. Availability of the source code of the Android application will enhance public awareness and understanding and inform debate on this matter of public importance.

6.19(c) promote effective oversight of public expenditure

The original decision stated:

> The ATO has invested a significant amount of information and time in developing the myGovID applications.

It also stated:

> I further understand the source code contains or will contain components commercially licensed to the ATO.

Together, these suggest significant public expenditure has occurred and will continue to occur. Release of the source code of the myGovID Android application will promote oversight of this expenditure. In particular, access to the source code of the Android application will allow the public to assess, to some degree, matters such as:

- Is the quality of the implementation commensurate with the amount spent developing it?
- Were there lower-cost alternatives to the commercially licensed components used in the Android application?
- Was it necessary to develop an in-house solution at all, as opposed to using or licensing an existing software system (possibly with modifications).

6.19(i) advance the fair treatment of individuals and other entities in accordance with the law in their dealings with agencies

I am not aware of any law concerning the means of access to government services and restriction of access to particular technological devices (hardware or software). I therefore discuss this matter in the *spirit* of public interest factor 6.19(i), that is, *fair treatment of individuals*, and note that the list of public interest factors is *Guidelines* is non-exhaustive.

The ATO publishes myGovID client applications for the Android and Apple iOS operating systems used primarily for mobile phones and other portable computers. Android and Apple iOS devices are popular and together constitute a large portion of the market. However, some citizens do have other kinds of mobile devices, and I am one such person.

Furthermore, even for users of Android or Apple iOS devices, one can only access the myGovID application via the Google Play Store (for Android) or Apple App Store (for iOS). This requires registering an account and providing personal details to Apple or Google. These are foreign companies who act in the interests of their shareholders, not account holders.

I accept that the ATO cannot and should not attempt to create and distribute a myGovID client application for every esoteric device in the market. I also accept that it is reasonable for the ATO to use the Google Play Store and Apple App Store as primary distribution channels for the myGovID client applications. But consideration should be given to the individuals who do use other kinds of devices or who do not wish to become Google or Apple account holders and run proprietary, opaque software on their device just to access as Australian government service.

Releasing the source code of the myGovID Android application would advance the fair treatment of individuals by the ATO (and all services using the myGovID system for user authentication) in two significant ways.

First, the program can be adapted to other platforms. Or, with the understanding afforded by access to the source code, compatible programs can be written for other platforms. This involves skill, but it need only be done once for each platform, and the resulting artifact can be distributed to many users (including those without the necessary skills to "port" the program themselves). As a result, more people will be able to use the myGovID system to authenticate to those services that support or require it.

Second, users of Android devices will be able to access the myGovID Android application without needing to register an account with Google. As in the preceding point, skilled individuals can perform this work on behalf of the many, working around the lack of source code for the commercially licensed components as necessary.

6.19(k) contribute to innovation and the facilitation of research

Access to the source code of the myGovID Android application will facilitate research on the security of the application, and the myGovID system in general.

Access to the source code will also facilitate the kind of innovation described in the preceding subsection, that is: porting the application to additional mobile platforms, and/or creation of compatible programs, to allow more people to access services that support or require myGovID for authentication.

Access to the source code can facilitate innovation and development to improve the usability and accessibility of the application. For example:

- Improving the user experience for people with vision impairments or impairments that affect or prevent physical interaction with a mobile device.
- Translating or otherwise modifying the application to meet the needs of culturally and linguistically diverse cohorts of users.
- General improvements to the user experience, performance or security of the application.

If the ATO is so disposed, they can make it possible to incorporate improvements developed in the community back into the myGovID Android application (and/or other components of the myGovID system). This kind of software innovation can be collaborative rather than independent or adversarial.

Other factors

The "terms of use" of the myGovID system, including the Android application, include the following:

> You should ensure that the software does not interfere with your systems or devices.

Without access to the source code of the program, it is extremely difficult to evaluate the range of possible behaviours of all but the most trivial computer programs. Therefore it is nearly impossible for the public to comply with this condition without access to source code.

The Terms of use also include:

> You must ensure your use of the software complies with all applicable conditions of use, including third party software licensing conditions of use, relevant laws, including local laws in any relevant foreign country if you use the software outside Australia.

For the same reason, it is impossible to ensure that use of the software complies with local laws without access to source code.

For these reasons, it is important for legal protection and the security of one's device and digital information—matters very much in the public interest—that the source code of the myGovID Android application be released.

Sincerely,

Fraser Tweedale