Fraser Tweedale
frase@frase.id.au

January 10, 2022

Director of FOI Dispute Resolution
Office of the Australian Information Commissioner

To whom it may concern,

On July 13 2021 I made an FOI request to Services Australia, the scope of which was:

> 1. Source code of the myGov Code Generator iOS and Android apps, including build scripts, manifests, software license terms, and media assets (icons, audio files, etc).
> 2. Technical documentation describing the operation of the myGov Code Generator app, such as design documents, architecture diagrams, API documentation, security assessments, technical presentation slides, and similar documents.
>
> If it assists in the expeditious processing of my request, source code may be delivered as a "snapshot" or export of source repositories, in ZIP, "tarball" or similar format. However, the full development history is preferred.

The matter was given the reference **LEX 63435**. On 13 September 2021, Services Australia made an access refusal decision (letter attached). They identified 12 documents within the scope of my request, including source code, solution brief, use case documentation and API documentation. They decided that all 12 documents were conditionally exempt under section 47E(d) of the FOI Act, and that, for each document, release would be contrary to the public interest.

I applied for internal review of the decision on October 12 2021 (letter attached). The review matter was given the reference **LEX 64833**. On 11 November 2021 Services Australia conveyed a decision (attached) affirming the original decision. I am applying for Information Commissioner review of Services Australia's decision.

Services Australia's decision has two parts: first, the application of s47E(d) (information that would have a substantial adverse effect on the proper and efficient conduct of the operations of the agency); and second, the public interest test for conditional exemptions. However, the reasons given for the application of s47E(d) and the public interest factors against disclosure are, in substance, the same. Rather than addressing s47E(d) and the public interest test separately, I will address the substance of the reasons given for both.

myGov Code Generator, the program whose source code and technical documentation is the subject of my FOI request, is a mobile application with two related features:

1. a *one time password* code generator

2. an *enrolment* feature that initialises the one time password feature for use with myGov.

In summary, the application implements the *client side* or *user end* of one of the *multi-factor authentication* options for the myGov system.

I am a professional software engineer having worked in industry for more than 10 years. For the last 8 years I have worked a multinational software company developing authentication, identity management and public key infrastructure solutions.

I will now address the general reasons given in the internal review decisions dated 2021-11-11 (LEX 64833), as well as a couple of public interest factors.

Counterfeit applications (development)

The reasons given state:

> Disclosure of the information would significantly increase the risk of others creating counterfiet applications.

This risk must be considered alongside two other factors:

1. The latent risk of someone developing a counterfeit application. In the decision, Services Australia agrees that *the release of source code and technical documentation is not a prerequisite for the development of counterfeit applications*. The myGov Code Generator application is relatively simple and a skilled mobile application developer could, without access to source code, easily and taking little time develop a counterfeit.
2. A counterfeit application must be distributed before it has any impact on end users (and by deduction on the operation of the agency).

If we consider (1) development of a counterfeit without access to source code is easy and (2) successful distribution is hard, then it is not reasonable to conclude that disclosure of the source code *would significantly increase* the risk of counterfeit applications having a significant operational impact on the agency.

Services Australia contends that the disclosure of the source code would significantly increase the risk of others *creating counterfeit applications*, but that in itself does not automatically lead to a significant operational impact on the agency. The element of distribution is essential.

Counterfeit applications (distribution)

The decision states:

> In my view, the fact that the applications are distributed via "app stores" which list the publisher of the application does not mitigate the significant risks outlined above, given that the agency provides services to the most vulnerable members of the Australian community who have varying levels of technological literacy.

I disagree with this contention. Source code is not a prerequisite to developing a counterfeit app, and a motivated and skilled person could do so, and attempt to distribute the application. The prevailing "app store" distribution model

does provide both safeguards and recourse against counterfiet applications. To the extent that those safeguards may fail, because it is already possible, without source code, for a nefarious person to develop and attempt to distribute a counterfeit application, the availability of source code neither introduces nor substantially increases the risk for end users or the agency. The agency itself, if concerned about counterfeit applications, must implement measures to detect and take action against counterfeit applications in the "app store" distribution channels.

I agree that many users or potential users of the myGov Code Generator application have varying levels of technical literacy. Installation of applications *outside* the default "app store" for a supported platform is an advanced operation. People with lower levels of technical literacy will, overwhelmingly, only install applications via the "app store" for their platform, and therefore be protected by the safeguards of this distribution model and by whatever additional measures Services Australia has in place to ensure the absense of counterfeit applications in these channels.

For these reasons, with respect to counterfeit applications, even if access to source code makes it easier to *develop* counterfeit applications, it would not reasonably be expected to have a serious or significant effect on the operations of Services Australia.

Circumvention of security

The agency's reasons state:

> Disclosure would also allow nefarious actors to circumvent security features and potentially gain unauthorised access to third party information.

The reasons given lack technical detail and seem to appeal to *security by obscurity*; that is, that information about a system must be restricted to ensure the security of the system. In the domain of software systems and security, *security by obscurity* is a fallacy. It is widely accepted that the specifications of network protocols, and especially protocols and algorithms relating to security (authentication, privacy and integrity), should be public to permit analysis and support interoperability. It is also accepted that publishing the source code of software implementations does not, in general, prejudice the security of a program or information system. Indeed this is the Government's own advice through the Digital Transformation Agency[1].

The possiblity of attacks against the myGov service itself cannot be used to justify the refusal to disclose the source code of the myGov Code Generator application itself, which is a small component of the system that is installed and operated by end users. Insofar as the source code or technical documentation of the application contains information about the myGov network Application Programming Interface (API), such information can already be attained by observing the network traffic between the application (or other myGov client programs, including web browsers) and the myGov servers. Access to the source code is not a prerequisite to discovering and exploiting vulnerabilities.

[1] https://www.dta.gov.au/blogs/making-source-code-open

I consider that there is nothing special about the myGov Code Generator application that means that the disclosure of its source code or technical documentation could reasonably be expected to have a serious or significant effect on the operations of the agency, with respect to security, risk of unauthorised access or availability.

Privacy obligations

The agency's reasons insofar as they relate to privacy are lacking in technical detail. A possible interpretation is that because the myGov Code Generator application enrolment feature involves "logging in" to the myGov service, that a counterfeit application could be used to violate the privacy of persons who were deceived into using it. I have already dealt with the agency's contentions about counterfeit applications in detail.

Public interest factor: oversight of public expenditure

The decision maker did not consider that release of the source code would promote effective oversight of public expenditure. The decision states:

> I find that the release of the source code would not contribute to this in any significant way. I find that the published product and the expenditure used to create that product are more relevant to this point, and that much of this information is already available in the public domain.

Whilst the quality of the final product—the compiled application as distributed to and used by end users—provides some insight into whether public money has been spent well, there are some important questions that can only be answered by access to the source code, such as:

- have best practices been followed in the implementation?
- has the agency implemented subroutines or features themselves when an existing "library" routine or platform feature would have sufficed? That is, has public money been spent "reinventing the wheel"?

Public interest factor: fair treatment of individuals and innovation

The decision states:

> In your submission you contend that the release of the source code would advance the fair treatment of individuals and other entities in accordance with the law in their dealings with agencies. Your submission also contends that release of the source code may facilitate further accessibility of the application, allowing members of the public to more easily engage with the agency. However, given the significant security and privacy risks I have identified above, I do not find that creating any copy or imitation application would reasonable be considered to advance the fair treatment of members of the public engaging with the agency.

This argument relates to *derived works*, for example "ports" of the application to another platform, or modified versions that improving accessibility for cohorts

with particular needs. The argument is hard to follow but seems to contend that any and all derived works necessarily constitute or increase security and privacy risks, thereby negating any benefits of the derived work. I do not agree with this conclusion. In particular, if the derived work is distributed in source form or if the source of a derived work is available, the modifications from the original version are transparent and it would be possible to verify that the derived work does not present an elevated risk—or that it does, and should be avoided.

Closing

Thank you for considering my submissions. If the OAIC decides to undertake a review, I would be happy to provide further submissions or adduce expert testimony upon request.

Sincerely,

Fraser Tweedale

encl: Decision letter for initial request (**LEX 63435**)

encl: Internal review application letter

encl: Internal review decision letter (**LEX 64833**)