Queensland Community Safety Bill 2024

Submission No:	11
Submitted by:	David Ingram
Publication:	Making the submission and your name public
Attachments:	See attachment
Submitter Comments:	

Queensland Community Safety Bill 2024

I wish to comment on the proposed changes to the PPRA that are contained in the above-mentioned Bill. My concern is that the burden of proof for delivery of electronic communication is unfairly pushed to the recipient.

An additional concern regards what constitutes a digital signature for the purpose for documents prepared by Police. This touches on a bigger issue of electronic signatures on documents, and the ambiguity present across multiple departments and legislation.

Electronic Communication

Putting the onus upon the recipient of an email or SMS is unfair and does not reflect the inherently unreliable nature of these communication systems. If electronic service is deemed to be made then this should only apply to a technology that both confirms receipt and reading of the message. Email and Rich Communication Services (RCS, souped up SMS) can provide this, but it is not the default. Spam filtering on email and phones could easily remove such an electronic message and the recipient would be none the wiser.

There is no provision in the Bill for the situation where there is positive confirmation that a message has not been delivered, such as a “bounce” message by email or undeliverable notification for SMS. The proposed 789E and 789F should expand the “unless contrary is proved” to include a requirement for timely check for error messages, as a recipient cannot prove a negative without access to the QPS email and SMS. 789E(1)(a)(i) “will be received by the person within a reasonable time” could be expanded here to be “will be received by the person within a reasonable time, and has not received any notification of unsuccessful delivery of electronic communication.”

The definition of a “unique electronic address” in Schedule 6 of the PPRA is quite ambiguous. What makes an address “unique”? Could someone nominate a shared email address (common in homes with older people that have a single address from their internet provider)? The provisions of electronic service seem pointless considering a person simply needs to not provide consent or nominate an address.

Clause 85 Insertion of new ch 23, pts 1AA and 1AB (Amendment of Police Powers and Responsibilities Act 2000)

789E Serving documents by electronic communication

(1) A police officer may serve a prescribed document on a person by electronic communication sent to a unique electronic address of the person if—

(a) the police officer reasonably believes, having regard to the circumstances—

(i) the electronic communication will be received by the person within a reasonable time; and

(ii) the electronic communication would be readily accessible by the person so as to make the document useable by subsequent reference; and

(iii) it is appropriate to do so in the circumstances given the purpose and effect of the document; and

(b) the police officer has made a reasonable effort to ensure the person understands the purpose and effect of the document; and

(c) the person has given consent under this part for service of the document by electronic communication; and

(d) the person's consent has not ceased to have effect under section 789J; and

(e) the person has nominated the person's unique electronic address for service by electronic communication.

789F When service by electronic communication is effected

(2) Unless the contrary is proved, for this Act and any other Act, the prescribed document or related document is taken to be personally served on the person on the day and at the time the document was sent by electronic communication to the person's nominated unique electronic address.

789L Evidentiary provision

For a proceeding under an Act, a certificate signed by the commissioner stating any of the following matters is evidence of what it states, unless the contrary is proved—

(a) a prescribed or related document is, or was, on a stated day sent by the police officer to a person's nominated unique electronic address;

(b) the police officer complied with sections 789E, 789G and 789K.

Electronic Signatures

If electronic signatures are to be used then there should be a consistent framework for these across all of government, and not a piecemeal approach. The Oath Act and guidelines are not fit for purpose from a cybersecurity perspective. Digital representations of "wet signatures" and typed names in emails do not satisfy the non-repudiation requirement. The 'technology neutral' position is unsatisfactory—this is a case where the Government should be setting technical guidelines to ensure the safe use of this technology. Why is it up to the Commissioner of Police to decide if a method is suitable? This should be determined by a person with expertise in the field of information management and cybersecurity, and be consistent across all of government (and ideally, across all Australian jurisdictions).

A certificate based signature is the only means of ensuring that 1) the document is signed by who it claims to be (authenticity) and 2) the document has not been altered since the signature was applied (integrity). The cost onus for PKI-based signatures is on the signer, as the recipient can easily validate the document and embedded certificate if the "root" Certificate Authority (CA) is made public[1] and downloaded by someone needing to check validity (if not included in the default set of CAs on their device).

Clause 85 Insertion of new ch 23, pts 1AA and 1AB (Amendment of Police Powers and Responsibilities Act 2000)

789M Approved method for electronically signing documents

(1) The commissioner may approve a method for electronically signing a document under section 789N.

(2) The commissioner must be satisfied, having regard to all the circumstances, that the method approved under this section is a reliable method for identifying a signatory of a document.

(3) Also, the commissioner must not approve a method prescribed under the Oaths Act 1867, section 13A as a method that is not an accepted method.

1 Queensland Health makes their root certificates available at http://pki.health.qld.gov.au/, but this does not support user authentication or signing at this time. Defence do support this, and are a good exemplar at https://crl.defence.gov.au/pki/.