2023 Submission to Electronic Transaction Act Consultation

Submitted at 4.30pm on 20 March 2023
Minted as NFT: https://mirror.xyz/badasl.eth/I-D9tFISPlcsbKzhG5_Mynu8BRSF5mYOMBhJhT7jVyc

Reference materials

Electronic Transactions Act Consultation: https://consultations.ag.gov.au/legal-system/eta/

Electronic Transactions Act 1999 (Cth):
http://classic.austlii.edu.au/au/legis/cth/consol_act/eta1999256/index.html#s5

Electronic Transactions Act Regulations 2020 (Cth):
http://classic.austlii.edu.au/au/legis/cth/num_reg/etr2020202000956381/

Submission

The standard ETA process gives people the right to withhold their consent for electronic communications.
As a consumer, have you ever experienced any of the following issues relating to giving your consent?
If your organisation represents a group of other individuals or entities, please answer based on their common experiences.
You may select more than one.
I have wanted to use paper transactions (and didn't give my consent) – but the other party used electronic tools anyway.
I have felt pressure to consent to use electronic tools, when I didn't really want to.
A government department didn't ask my consent before transacting electronically with me.
This hasn't been an issue for me, because I would generally prefer to use electronic tools over paper-based transactions if available.
This hasn't been an issue for me, because I've never thought about my right to give or withhold consent.
Other
Please expand by providing further background details about your answer/s above, e.g. what happened as a result of the issue/s, or why did you feel this way? Please use examples where possible and let us know which issue/s you're talking about.

Both myself and clients of Blockchain & Digital Assets Pty Ltd prefer to use electronic tools over paper-based communications and transactions.

However, the electronic signing of a blockchain transaction – often through a digital wallet such as Metamask – and the electronic communication that is the subject of the electronic signature are matters for clarification of application of the *Electronic Transaction Act 1999 (Cth)* (Act) as well as the State and Territory iterations.

One particular issue is whether, as part of obtaining consent, there should be a requirement upon the 'requestor' to convert the electronic communication into plain english language. Additional things to consider include:
- Maintaining an audit log of consents given
- The requestor digitally signing the consent request to enhance trust
- The requestor identifying themselves in such a way that links their DID to a real world identity
- Delegation of authority where a third party is approving consent on behalf of a user

Some would go further that there should be a requirement to clearly identify the risks of receiving the electronic communication or signing the electronic transaction where the plain english conversion does not make the risks prominent. Where messages are sent from one decentralised identity (DID) address to another, there can be risks that are similar to receiving scam emails or texts, where upon opening the message or clicking on a link (in this case, a non-fungible token) malicious software is installed on a device and/or the digital wallet.

As cyber-threats and cyber-attacks increase, so too does the policy question of whether security considerations should be 'built in' to pieces of law such as this Act.

Mere 'consent' is required by the Act and not 'informed consent', thus leaving a 'requestor' exposed to arguments that a transaction should be invalidated on grounds that the person gave consent without being informed sufficiently to understand the consequences of their consent. Further, that the 'requestor' is liable for consequential losses suffered by the person such that any prominent disclaimers or limitation of liability clauses are ineffective.

In an interconnected digital context, where a digital wallet controls access to value and information of a person, 'informed consent' becomes a necessary safeguard to mitigate against the potential compounded economic losses from and that can lead to leakage or interception of sensitive and personal information.

Whilst decentralised interaction models using DIDs allows multiple endpoints to be defined for a single wallet (so you don't need a single "wallet" per token to manage exposure to risk), it is worth noting early stage private market solutions such as Fireblocks. Fireblocks' software abstracts away the complexity of security for consumers in the way their proprietary software automatically creates a new wallet per new token and per new type of interaction so that risk is not consolidated in one digital wallet. Before such software is available for retail use, there will inevitably be points of uncertainty and thus inhibitors to business and community confidence in the use of these such forms of electronic transactions.

The standard ETA process requires people to confirm consent from people before communicating or signing documents electronically.
In operating your business, have you ever experienced any of the following issues relating to getting consent from others?
If your organisation represents a group of other individuals or entities, please answer based on their common experiences.
You can select more than one.
I have wanted to communicate electronically with a government department, but they didn't consent so I needed to use paper methods.
Someone didn't consent to transact electronically, and this led to delays / postage costs / other issues.
Someone didn't consent to transact electronically, but they didn't have any good reason for doing so.
I wasn't sure at what point I needed to collect consent from the other person.
I couldn't think of an appropriate way to collect consent.
It wasn't clear whether the other person had consented or not.
This hasn't been an issue for me – I've always been sure that other people consent for me to transact electronically.
This hasn't been an issue for me – I've never thought about the need to collect consent.
Other
Please expand by providing further background details about your answer/s above, e.g. what happened as a result of the issue/s, or why did you feel this way? Please use examples where possible and let us know which issue/s you're talking about.

It would appear the objects of the Act should be updated to allow for a regulatory framework that recognises the importance of data minimisation and the associated role of tokenisation (token proofs and token attestations) and information security in protecting business and the community when engaging in electronic communications and transactions.

To the extent that non-government identity methods are used in an e-commerce solution, such as DID methods and verifiable credentials, proofs and attestations, then either the Act alone or more likely the Act and its periphery of laws produce uncertain outcomes and inhibit consumers and small businesses from benefiting from e-commerce efficiencies that are secure and privacy-enhancing*. The primary benefit of a decentralised approach to data sharing is that it emulates existing (physical) interactions and doesn't look to include unhelpful intermediaries, whilst increasing trust in those involved and the shared information. Consent management in decentralised interaction models are simpler as the customer is typically involved and consent shared directly between those involved.

Where it is not clear whether the other person had consented or not, the issues for clarification revolve around ‘identity’, ‘identity verification’, ‘just-in-time’ consent and related and necessary security considerations. The combination of these issues relate to one of the commonly cited reasons for not consenting, being the hesitancy to provide personal information where there are privacy-enhancing methods of ‘identity verification’ available that do not require the sharing of personal information (such as tokenisation of proofs and attestations, e.g. tokenised proof of being over 18 rather than all personal information that would be conveyed by a drivers’ licence or passport).

Traditional consent frameworks assume use of the existing -- centralised -- methods of identity verification to prove that a particular 'identity' is giving consent. For example, the requirement to create a MyGov account and use MyGov when interacting with Commonwealth entities carries a default assumption that the person using the MyGov account is the correct 'identity'. Equally, identity verification software providers typically default to government issued forms of identity and they are required to retain that information for a period of years stipulated by law, increasing their personal data management obligations, associated information security obligations and risk of cyber-attack or cyber-threats based on the data they hold.

Multiple factors of authentication are typically recommended by the provider upon account set-up to mitigate against the risk that an account is used by a person other than the named accountholder. However such security steps have not been proscribed by the law as a necessary part of the identity verification process each time consent is required, which further inhibits confidence to use electronic forms of communication and transactions. Furthermore, data retention laws with respect to identity verification providers have not been reviewed in the context of an increasingly digital world where cyber-attacks are on the rise and have the necessary and inconvenient consequence of identity fraud where full identity documents are typically required to satisfy ‘identity verification’ methods.

What is required by the Act when a signature is to be given to a non-Commonwealth entity (i.e. private actor) is that 'a method is used to identify the person and to indicate the person's intention in respect of the information communicated'. However, what does ‘identify the person’ mean? Does it permit mere proof of the person’s attributes such as being over 18 in order to electronically sign? Does it require the person to have legal capacity (and not incapacity) at the time of electronically signing? Does it require the identification of a legal person (human or legally recognised entity) so as to avoid artificial intelligence signing electronic transactions?

The policy question is whether, just for digital contexts or increasingly where paper forms are generated from digital contexts, the security and verification components of 'identity' and 'consent' need to be strengthened despite the context. Principles of security and privacy-enhancing verification should be embodied in at least the objects of the Act so that innovations around each can flourish with certain minimum safeguards.

Centralised methods of identity and consent are evolving. Concurrent with the introduction of government digital identity frameworks, a drivers' licence may be reduced to a driving credential and not an identity document (but transitionally retained to have the status of an accepted identity document), and a passport may be reduced to a travel credential and not an identity document. See, for example, the NSW Digital ID (https://www.nsw.gov.au/nsw-government/projects-and-initiatives/nsw-digital-id) and NSW Digital Driver Licence (https://www.service.nsw.gov.au/campaign/nsw-digital-driver-licence), and the European Digital Identity (https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en).

In addition, decentralised methods of identity and consent are evolving. Thus the Act's objects and consent requirements should embody permissive and safeguarding principles that allow for flexibility from innovation in areas of identity, verification of identity, social recovery of identity (for non-government issued identities and reputation), and consent.

There are significant structural efficiencies and privacy benefits gained by both public and private sector using a common set of open-source standards for proving identity, trust and reputation. This is especially so when done in such a way that critical personal identifiable information (PII) does not need to remain stored on centralised servers. The current regulatory environment forces organisations to retain sensitive PII (drivers license etc.) which in turn creates honey pots of valuable data that are being hacked on a regular basis.

An electronic transactions regulatory framework that would contribute towards privacy-enhancing approaches to identity and consent management include:

1. Flexibility to support moves to models of identification that don't require centralised storage of sensitive information; and
2. Flexibility to move to a dynamic information sharing model where organisations request information in a standard way from a user on demand, and destroy it immediately after its use.

*Privacy-enhancing means a method that preserves a person's personally identifiable information and relies on the principles of data minimisation (don't collect more data than is necessary) and tokenisation of data (don't share the actual data such as the bank account, share a verifiable presentation (a token) that the bank account exists).

For more information on DIDs, and secure storage of verifiable credentials, see for example Verida: https://www.verida.io/ and Sezoo: https://www.sezoo.digital/.

What methods do you think are appropriate to make sure a person can access, and is comfortable with, electronic communication and signature tools?
You can choose more than one (e.g. if your answer depends on the transaction type)
There should be clear consent for every type of e-transaction.
There should be clear consent from each person I transact with.
People should use 'consent form' or something similar to confirm consent
If you have communicated electronically without complaint in the past, this should demonstrate consent.
If you provide an email or accept an e-signing link, this should demonstrate consent.
These days, it should be fair to assume that everyone is fine with electronic communications (unless they say otherwise).
I've never really thought about e-commerce consent.
Other
Please expand on your selections above

Further to responses above, there should be a risk-based approach to determining the consent requirements based on principles of data minimisation and tokenisation. The objects of the Act should allow for this flexibility of innovation in electronic communications and transactions with certain minimum safeguards for understanding ('informed consent') and security. Note that our mobile devices already provide access to multiple solutions that rely on cryptographic solutions, key management and the technology necessary for electronic communications, wallets etc.

What methods do you use to ensure a person can access, and is comfortable with, electronic communication and signature tools? (i.e. If you regularly send information/documents to other parties, or engage in e-signing.)
If your organisation represents a group of other individuals or entities, please answer based on their common experiences.

Esignature platforms are widely used but legal documents uploaded for electronic signature often do not include a clause that the parties' consent to sign electronically. Perhaps this is because if the person signs electronically then they have implied their consent to sign as such.

Tick or check boxes are also widely used for standard form contracts that allow a person to sign or agree to the particular terms and conditions, without creating a user account. Thus no 'person' is actually identified but proof of personhood may be established with tools such as CAPTCHA.

Each approach does not typically garner the person's intent in respect of the information communicated nor 'identify the person'. Clarification of application of the law is required. Moreso to prevent the inefficient use of resources for a class action suit that may arise from widespread economic loss directly or indirectly from the illegal use or interception of personal data collected in respect of compliance (or perceived compliance) with this Act.

Finally, if an entity develops a smart contract and deploys it to a permissionless blockchain so that it functions autonomously as it is coded to function upon receiving certain instructions, then the extent to which that entity is required to obtain consent from the consumer, 'identify the person' and ensure an 'indication of the person's intention in respect of the information communicated' is unclear. Based on the above examples, perhaps only proof of personhood is required and the intent of the person in respect of the information communicated is implied by their engaging in the ensuing conduct.

The requirement to collect consent makes it difficult to conduct electronic commerce in Australia
Strongly agree
Agree
Neither agree nor disagree
Disagree
Strongly disagree
Please expand on your selection

Per above responses, the collection of consent involves answering uncertain and evolving legal questions related to 'identity' and 'verification of identity' which is what increases the difficulty of collecting consent. This is particularly so if the small business or consumer seeks to adopt privacy-enhancing methods, such as DID and verifiable credentials, in managing consent while concurrently practicing the principle of data minimisation (don't collect more data than you need in relation to the consent/action).

Apply your answers to the statements below:

	Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
The consent requirement is necessary to prevent unjust outcomes.					
Consent is an important aspect of transacting electronically.					

Please expand on your selections

The key policy questions for this consultation are those of enhancing the 'future-fitness' of the Act. As more transactions are undertaken online and cyber-threats and cyber-attacks are on the rise, consent and identity continue to be important but must be better articulated with the principles of data minimisation, tokenisation and security in mind.

Consent is a loaded term that also implies the 'identity' of the person consenting has been verified. In paper-based consent, typically paper-based identity documents are presented that are either the original and official document produced by a government authority or are certified as a true and correct document by a justice of the peace or notary. Paper documents can be fraudulently produced, as can certifications.

The velocity of frauds able to be perpetuated in paper-based systems is much slower than the velocity of frauds that can occur in a digital and interconnected global economy.

Consent in decentralised solutions are typically simpler as the person needing to provide consent is typically involved in the transaction. Additionally, with a decentralised interaction model, the individual also has the capability of initiating secure communications using the same cryptographic solutions as that used to share verifiable credentials and in these contexts additional/specific solutions are not required.

Identity verification is an important aspect of some electronic transactions but not all. The electronic transactions for which full identity should be verified (and not just proof of personhood, for example) is the subject of contentious debate, but which has largely occurred in the context of detecting and pursing financial and tax crime in the context of token transactions for financial value on permissionless and global digital infrastructure that allows for pseudonymity. There has to be a level of abstraction and thus clarification between where full identity is required under this Act for the Act's own objects and purposes versus where full identity is required in other legislative contexts such as for anti-money laundering and counter-terrorism financing in relation to the legal validity of electronic transactions.

Finally, permissionless and global digital infrastructure is and will increasingly be used for token transactions for non-financial value -- trusted transactions -- because of the integrity of the ledger records in the context of increasingly false information generated by humans and artificial intelligence. The integrity and security of the permissionless and global digital infrastructure could be, and perhaps already is, trusted more than any one centralised actor (such as Google for emails or search engines for credible and peer-reviewed search results). Accordingly, the Act should be flexible enough to enable confidence in electronic communications and transactions as the innovation around trust and safeguards related to identity and verifications in respect of communications and transactions also evolve.

Is there anything further you would like to raise with the government about the ETA consent provisions?

The ability to revoke a consent should be possible and under the control of the appropriate party. The existing legislative framework does not cater for revocation of consent.

The opportunity to discuss this submission further with relevant stakeholders is welcome, along with the offer to invite businesses working on innovative solutions to demonstrate how clarifications in the application of the Act would promote safer innovation in electronic communications and transactions.

When signing a document or entering a contract, do you (or your organisation) use electronic signatures as your most-preferred option?
If your organisation represents a group of other individuals or entities, please answer based on their common experiences.
Yes

Do you think that it is difficult to determine whether an electronic signature will be valid for any given document?
Yes
No
Please expand on your response

Depends on the 'document'. See previous responses regarding smart contracts and whether there should be a requirement to convert into plain language in order to obtain a higher level of 'informed consent' rather than mere 'consent'.

What verification or identity methods do you think are appropriate for the electronic signature tools you use?
If your organisation represents a group of other individuals or entities, please answer based on their common experiences.
Please refer to responses to earlier questions in relation to data minimisation, tokenisation and security which go towards collecting on the data required (which may not be full identity documents), and thus enabling innovation and flexibility of choice for consumers and businesses to adopt fit-for-purpose and privacy-enhancing methods of verification of credentials or identity.

How might this change based on what document you're signing?

The Act should strive to uphold principles of data minimisation, where tokenisation assist to achieve this principle. This principle could be broadly applicable to all types of documents being signed electronically.

Generally, the ETA allows paper-commerce to take place electronically. However, other legislation or the ETR can override these provisions and affect the validity of e-commerce options.
With that in mind – have you ever needed to search to see whether an e-commerce activity was affected by specific legislation or regulations?
If your organisation represents a group of other individuals or entities, please answer based on their common experiences.
Yes
No
How did you conduct this search?
You may select more than one.
By reviewing the legislation directly.
By reviewing the ETR.
Elsewhere online, like on a government or consumer website.
By seeking professional advice.
On physical materials, like pamphlets or books.
I have never needed to search for an ETA exemption.
I did not know about the existence of ETA exemptions until now.

How did you find the search process?
Very easy
Easy
Neither difficult nor easy
Difficult
Very Difficult
If you found it difficult or complicated, why?
Not difficult in the sense I am a trained lawyer, but not easy in the sense that it takes more time than it should to answer such basic questions.

What do you think would make the process easier?

Consumers and small businesses would be assisted by a mapping exercise that clearly shows what electronic activities map to what laws (Cth and State/territory) and where the areas of legal uncertainty remain any why.

Which exemption/s did you find affecting your e-commerce activity? How did this effect you?
Signing and witnessing of wills and deeds.

Do you or your organisation save important records (including communications and documents) electronically or physically?
If your organisation represents a group of other individuals or entities, please answer based on their common experiences.
Electronically (like on the desktop, on the cloud, or on file management programs)
Physical paper records
We record documents in both electronic and physical form
It depends on the record or document.
Please expand on your response

Electronically

Do you think that it is difficult to determine whether a record is allowed to be kept in electronic form?

No

Is there any further feedback you or your organisation would like to provide on record-keeping under the ETA?

In order to keep documents in purely electronic form, the organisation should be required to undertake a cyber security audit each year to reach assurance over:
1. Information security such as passwords and permissions to core systems and data
2. Vulnerabilities to cyber-threat or cyber-attack and recommended mitigating measures
3. Ease of retrieval of back-up information and exposure period in the event of information loss.

The government will look to publish resources which encourage greater use of e-commerce in accordance with the ETA. What information or content do you think would best help users navigate the legal requirements of Australia's e-commerce framework?

As referred to earlier, clarification of application of the law in the examples provided would assist the Act's usability and areas for reform to make it more future fit.

A mapping exercise would be helpful that clearly shows what electronic activities map to what laws (Cth and State/territory) and where the areas of legal uncertainty remain any why.

Finally, a list of cyber auditing firms that could reliably perform cyber security audits would be of great assistance to small businesses.

Do you have any suggestions about the form or style of this information?
This style has been very easy to engage with.

Do you consent to make your submission public?
Note: your submission may be made public unless you request it not be made public or the Attorney-General's Department considers it should not be made public. That will usually only occur for reasons associated with fairness. Submissions that are made public may include redactions made as the Attorney-General's Department considers appropriate.
(Required)
I agree to my submission being made public under my name
I agree to my submission being made public anonymously
I do not want my submission to be made public

With thanks to Chris Were at Verida and Jo Spencer at Sezoo for their valuable contributions to this submission.