30 May 2018

Law Reform Commission
GPO Box 31
Sydney NSW 2001

Per email: nsw-lrc@justice.nsw.gov.au

Dear Commissioners

Re: Access to Digital Assets upon Death or Incapacity

The Society of Trust and Estate Practitioners (STEP) is pleased to provide the following preliminary submission in response to your review of:

- laws that affect access to a New South Wales person's digital assets after they die or become incapacitated;
- whether NSW should enact legislation about who may access a person's digital assets after they die or become incapacitated and in what circumstances; and
- what should be included in any such legislation.

Your primary point of contact is the chair of STEP Australia's Digital Assets Committee, Rod Genders [redacted]

The present members of the sub-committee with whom you will have contact for the time being are Rod Genders, Kimberley Martin and Adam Steen.

STEP are keen to work with you, and our committee is very willing to respond to questions.

Yours sincerely

[redacted]
Neil Wickenden

Chair of STEP Australia

[redacted]

[redacted]

https://stepaustralia.com www.step.org

[redacted]

Contents

Contents **3**

Preliminary Matters **4**

Summary of Recommendations **4**

Background & Expertise **5**

Fundamental Issues **5**

Identification of Digital Assets **8**

Discussion about 'Proper Law' and Estate Planning **9**

Recent International Reforms **11**

USA 11

Canada 12

Comparing USA and Canadian models 12

Privacy Protections for Electronic Communications after Death or Incapacity - CLOUD Act vs GDPR **14**

Policies and Terms of Service **16**

Laws Affecting Access to NSW Person's Digital Assets after Death **18**

Laws Affecting Access to NSW Person's Digital Assets on Incapacity **19**

Jurisdictional Issues **19**

Further Work with You **19**

Annexure A **19**

NOTES **22**

Preliminary Matters

1. We have had regard to your terms of reference. We understand at this stage that you are identifying issues and laws, and that one way forward for you may be the issue of a consultation paper. We are keen to participate further in the development of reform of the law governing this important area.

2. As the overwhelming majority of relevant laws in this area are state-based within Australia, and because our population is highly mobile and prone to interstate movement, STEP is strongly of the view that national model legislation is the best way forward. This is especially necessary given the international/global nature of the internet, and the difficulties which arise when attempting to define the 'proper law' of the contract between a local service user and a foreign Service Provider.

Summary of Recommendations

3. STEP recommends:

   (a) the creation of Australian uniform model legislation in this area, for ease of consistent adoption throughout Australian States & Territories;

   (b) preference being given to the Canadian uniform model legislation, as opposed to the USA model legislation, as it is more consistent with Australian values;

   (c) addressing the tension between the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") and the General Data Protection Regulation ("GDPR") (EU) 2016/679 by prioritising consumer rights, such as the inclusion of the right to be forgotten;

   (d) considering the introduction of Australian legislation which regulates the proper law of internet/cloud contracts as the law of the user's domicile to prevent the ability of End User License Agreements (EULA) to oust local laws and customs;

   (e) the introduction of Australian legislation preventing the ability of EULA to oust the ability of fiduciaries to step into the shoes of their principal; and

   (f) the introduction of Australian legislation mandating that the fiduciary must act in the outmost good faith and in the best interests of the principal.

Background & Expertise

4. The Society of Trust and Estate Practitioners (STEP) is the global professional association for practitioners who specialise in family inheritance and succession planning. The majority of STEP members in Australia are lawyers who specialise in trusts & equity, Wills, estates, guardianships and elder law. We also have members who are accountants or financial planners.

5. STEP works to improve public understanding of the issues families face in this area and promote education at high professional standards among our members.

6. STEP members help families plan for their futures, including estate planning; wealth devolution; guardianship, capacity & protection issues; delegations & directives; advising on issues concerning blended, same-sex and international families; protection of vulnerable individuals; family business succession; and philanthropic giving. Full STEP members, known as TEPs, are internationally recognised as experts in their field, with proven qualifications and experience.

7. Indeed, STEP's international Digital Assets Working Group was founded and led by a senior Australian solicitor, Rod Genders.

8. The purpose of this Digital Assets Working Group was to raise awareness around issues involving fiduciary access to digital assets following death or incapacity.

9. Members of the working group included several of the world's foremost authorities in these areas of law reform for digital assets, including Donna Molzan QC[i], Kathleen Cunningham[ii] and Peter J M Lown QC,[iii] all of whom have been heavily involved in law reform initiatives relating to digital assets in Canada and elsewhere. This working group became STEP's international Digital Assets SIG (Special Interest Group) . It has members from Australia, UK, Canada, the USA and South Africa.[iv]

   In 2017 a team of researchers at Charles Sturt University and the University of Adelaide, under the direction of Professor Adam Steen and with assistance from Rod Genders *inter alia*, conducted the largest formal survey of Estate Planning in Australia ever conducted, where 1,000 adults revealed that 71 per cent knew very little about what would happen to their online content after they died or became disabled. Although more than 16 million Australians are active on Facebook, less than a third knew the American-based website owned all their content post-death. The report of the survey can be found at this link:

   https://researchoutput.csu.edu.au/ws/portalfiles/portal/19332794.

Fundamental Issues

10. When a person dies or becomes incapacitated, a fiduciary is needed to deal with the person's personal or financial affairs or make decisions for the person. These

fiduciaries are authorised to act under such instruments as a Will, a grant of probate or letters of administration, a power of attorney, a personal directive or a Court order granting guardianship or trusteeship. In these cases, the fiduciary is seen as "stepping into the shoes" of the person.

11. **Access upon disability/incapacity**. In order to manage an account holder's digital property, a fiduciary must be able to access it. To facilitate access, the account holder will need to disclose access information (such as usernames, account numbers, and passwords) or store that information where the fiduciary can access it. For some online accounts, this disclosure results in a violation of the EULA. The majority of popular Service Providers either prohibit account holders from disclosing their account access information or make account holders responsible to keep their access information private or secure.

    For example, Facebook's EULA provides that "*you will not share your password . . . , let anyone else access your account, or do anything else that might jeopardize the security of your account*." That EULA further provides that "[*i]f you violate the letter or spirit of this Statement . . . , [Facebook] can stop providing all or part of Facebook to you*." So, if an account holder were to provide their username and password to a fiduciary, then the account holder would violate Facebook's EULA and trigger Facebook's right to terminate the agreement, at which point the account holder might lose access to any digital property in the account.

    When Service Providers prohibit a fiduciary from learning an account holder's access information, they limit the account holder's ability to plan for the management of his or her digital property.

12. **Access upon death.** Many popular EULA state that they terminate at an account holder's death.

    For instance, Yahoo!'s EULA provides that *"[y]ou agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted*."

    If an account and its contents will no longer exist after an account holder's death, how can the account holder properly plan to have it managed for and distributed to his or her beneficiaries?

13. **Fiduciary risk.** When a fiduciary uses an account holder's username and password to access and manage the account's digital property, that fiduciary may risk criminal and/or civil liability under USA federal and state laws, even if such actions are authorised by Australian fiduciary laws. It is commonplace for an Australian trustee, executor or agent under an enduring power of attorney to have a legitimate interest in accessing and managing the digital assets of an incapacitated or deceased Australian user. However in so doing the fiduciary risks personal liability under USA laws by virtue of provisions in the EULAs of many popular service providers.

In Australia there are various laws that regulate computer trespass and the unauthorised access of data.[v] Offences generally cover hacking into password protected data (for example, an email address or Facebook account). In most cases, under the legislation, there is no additional requirement of an intention to commit another offence and no defence of "lawful excuse", so the scope of this offence is considerably wide.

14. **Service provider risk.** Part of the problem emanates from the 1986 USA Electronic Communications Privacy Act ("ECPA"), Title 2 of which is known as the Stored Communications Act ("SCA"). This prohibits public providers of electronic communication services ("ECS") or remote computing services ("RCS") from "*knowingly divulging to any person or entity the contents of a communication which is carried or maintained on that service …".*

    To date Service Providers have been cautious about disclosing information when the SCA applies, and reluctant to risk civil liability for disclosing private information. Their perspective is clear, given the huge volume of account holders, the high cost of litigation, and the lack of profit to be gained from those disclosures. Additionally the USA Federal Trade Commission ("FTC") prevents commercial entities "*from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce*."[vi] The FTC can prevent service providers and other commercial entities from violating their Privacy Policies.

15. **Examples of Difficulties in Dealing with Digital Assets.** A collection of examples of real life issues and case law in the area of digital assets is provided in Annexure A.

    Many of these examples occurred before the introduction of the GDPR and the Cloud Act, which may have affected the outcome in these examples, however we have provided them to showcase the issues and difficulties that Australians face in dealing with digital assets and why it is vital that legislation be introduced to assist them.

Identification of Digital Assets

16. Your terms of reference came with background information about access to digital assets, to which we will refer in this preliminary submission.

17. In the background information you have identified, in a general way, that a person's "digital assets" might include:

- Photographs
- Videos
- Emails
- Online banking accounts
- Cryptocurrency
- Domain names
- Blogs
- Online gaming accounts

18. The term 'Digital Assets' can be used to define as any item of text or media that has been formatted into a binary source over which a person has ownership rights (Van Niekerk, 2006). As such the scope of digital assets is quite extensive. Zhang and Gourley (2009) include digital documents, audible content, motion picture, and other relevant digital files. They further propose that digital assets may be stored on currently existing digital appliances or those that may be developed in the future. Johnston (2015) notes digital assets could include not only valuable things such as domain names, online businesses, or bitcoins, but more commonly data of sentimental value such as photographs and emails. Some of these things may be held in cloud storage or on third-party hosting sites. Ploss (2017) defines digital assets more broadly to include any account, document, information, record, photo that is accessible primarily by an individual's access via electronic device (which includes tablets, smart phones, computers) to the Internet. An extensive listing of the types of possible digital assets is provided by Ploss (2017) and includes[vii]:

(a) Email Accounts

(b) Social Media Accounts (such as Facebook, LinkedIn, Twitter)

(c) Blogs (created and maintained by the individual)

(d) Currency (such as Bitcoins)

(e) Photos and Video posted through web portals to the web

(f) Websites

(g) Online purchasing accounts such as Amazon, PayPal, and catalogue accounts

(h) Online store accounts (e.g. EBay, Sirius XM Radio, Pandora, and Spotify)

(i) Music (e.g. iTunes or Google)

(j) Video Sharing Accounts (e.g. YouTube)

(k) Electronic Libraries (such as Kindle, IBooks, Barnes & Noble)

(l) Gaming Accounts

(m) Sports Gambling Accounts (such as Draft Kings and Fan Duel)

(n) Electronic Medical Records (accessible through portals)

(o) Personal Computers, Smartphones and Tablets (which are the portal)[viii]

(p) Documents stored to the cloud (through Carbonite, Barracuda, ICloud and Microsoft)

(q) Movie Services (e.g. Netflix and Hulu)

(r) Reward Programs (such as Airline, Credit Card and Hotels)

(s) Contact Lists

(t) Calendars

(u) Text Messages

(v) Electronic Financial Accounts and Account Records

(w) Electronic magazine and newspapers subscriptions

(x) Online Bill Payments offered through banks (automatic payment of monthly bills)

(y) Online sales accounts (e.g. EBay, Craigslist).

Discussion about 'Proper Law' and Estate Planning

19. Laws regulating succession tend to be very localised, differing widely across the world. Due to the intangible and global nature of digital assets, it is not possible easily to determine the 'proper law' of a dealing with a digital asset. In most instances, several laws from different jurisdictions may apply to each digital asset.

20. The 'proper law' of a dealing with an asset is the substantive law applicable where a conflict of laws occurs. Further, choice of law rules determine under which jurisdiction or system of law a case should be heard.

21. An assessment of the 'proper law' of certain digital assets is provided for assistance:

(a) *digital assets (that are intangible) owned by an individual*: as intangible personal property, the 'proper law' is the law where the deceased was domiciled. Therefore, provided that the intangible digital asset is owned by the Willmaker or Donor, it is perfectly feasible to make provisions for intangible digital assets (such as photographs and videos) in a Will or Power of Attorney, and to deal with digital assets as part of the administration of an estate;

(b) *digital assets (that are tangible) owned by an individual*: as tangible personal property, capable of transfer by delivery, the 'proper law' is the law of the domicile of the deceased. Therefore, provided that the tangible digital asset is owned by the Willmaker or Donor, it is perfectly feasible to make

provisions for digital assets (such as phones and laptops) in a Will or Power of Attorney, and to deal with digital assets as part of the administration of an estate;

(c) *digital assets regulated by EULA*: if the digital asset is regulated by EULA (i.e. a photo uploaded to Facebook) or if it is a licensed asset (i.e. an eBook or iTunes music file), then the 'proper law' will, in most circumstances, be the 'proper law' stipulated in the EULA. A photo provides a useful example:

- if the photo is stored only on the deceased's iPad, it should be easy to access, and will most likely be distributed to beneficiaries (for example by USB) as part of the residuary estate or as part of a specific gift;
- however, if the photo is stored on Facebook, Flickr or other online storage accounts, access will be controlled by the relevant EULA, and will therefore be more difficult to include in the provisions of a Will; and

(d) *digital assets that are accounts regulated (or are linked) by a EULA*: as a bundle of contractual rights, the 'proper law' could be any of the following:

- the location of the Service Provider's headquarters;
- the location of the Service Provider's servers;
- the location of the account holder;
- the location of the communications equipment transmitting information between the provider and the user of the account; or
- the agreed "proper law" as set out in the contract, licence or terms of service agreement.

The above sources of determining 'proper law' can and will vary from time to time and from place to place. For this reason there is no definite or consistent identification of what is the 'proper law' of any digital asset.

22. The feasibility of provisions about accounts (such as social media accounts and emails) in a Will or Power of Attorney, and the ability to deal with accounts as part of the administration of an estate can, at this time, only be determined by a close examination of each of the above possibilities.

23. Lawyers who practise in estate planning assist their clients to prepare their assets for management (including access, control and devolution) for different phases of the client's life, including contingent provisions for their incapacity and death. As digital assets include some things that are property, the above definition of estate planning is applicable to dealing with digital assets. This is because a client may want their digital assets held, controlled, terminated or distributed in accordance with their wishes and directions, regardless of whether or not all digital assets are strictly speaking, probateable assets. Similarly clients also want the digital assets held, controlled and perhaps terminated or distributed, during incapacity.

24. Outside of accepted succession law principles and practices, the introduction of individual 'policies', 'EULAs' or 'terms of service agreements' for each Service Provider has created a labyrinth of parallel succession regimes, containing a completely different set of rules for each service that can only be found and (hopefully) understood by reading through many pages of 'fine-print' terms and conditions. The inconsistency in policies has made it more difficult for people (and their professional advisors) to understand, and apply in practice, a general approach on how digital assets fit within accepted principles of estate planning, how to attempt to deal with them and how to keep up with the fact that they are subject to frequent change. It has also made it very difficult for clients, who are attempting to make provision within their estate plan or who are administering an estate, because they have no idea what to do or where to find information.

25. Although there are strong legal arguments that a relevant fiduciary's powers must extend to accessing & controlling parts of a person's digital assets, with no formal legislative or judicial recognition of such powers in Australia, problems exist in compelling (foreign) Service Providers to recognise this.

Recent International Reforms

26. Legislative reforms that are intended to resolve some of the uncertainty are currently underway in various countries. You have identified for consideration the Uniform Law Conference of Canada's Uniform Access to Digital Assets by Fiduciaries Act (2016) and the American Uniform Law Commission's Revised Uniform Fiduciary Access to Digital Assets Act (2015).

USA

27. In 2012 in the USA, the Uniform Fiduciary Access to Digital Assets Act (UFADAA) was first proposed by the National Conference of Commissioners on Uniform State Laws (Uniform Commissioners). Several members of the STEP Digital Assets Working Group (STEP-DAWG) were official observers of the USA UFADAA initiative. Suzanne Brown Walsh[ix] was chair of the USA ULC's Revised Uniform Fiduciary Access to Digital Assets Act, and was also a member of STEP-DAWG.

28. The intention of UFADAA was to spell out the rights of fiduciaries with respect to users' digital assets. In 2014 Delaware enacted a law regarding digital asset privacy that is substantially similar to the originally promulgated UFADAA. A coalition of internet based businesses and privacy advocates offered its own more limited version of digital asset legislation which was enacted in 2015 in Virginia.

29. In 2016, the USA Uniform Commissioners adopted a Revised UFADAA (RUFADAA). Under RUFADAA, fiduciaries are allowed to manage a deceased's digital assets, but it restricts a fiduciary's access to electronic communications of

the deceased unless the deceased expressly consented to such access in a Will, trust agreement, power of attorney, or other legal record (Jean and Woods, 2017). As of the date of this submission, 35 US jurisdictions have enacted the RUFADAA. A further nine US jurisdictions have introduced bills to enact RUFADAA.

30. The RUFADAA definition of 'digital assets' only includes electronic records in which the individual has a property right or interest. Amongst other things, Section 2 (10) of RUFADAA provides a definition of digital assets (consistent with the definition in the earlier UFADAA) and Section 3 defines fiduciaries who can access to an individual's digital assetsx. RUFADAA provides that where an individual's instructions address the ability of family members or fiduciaries to access their digital assets upon their death or incapacity, these instructions are prioritised over service access agreements. However, if the individual's instructions do not explicitly grant fiduciary access to their digital assets, then fiduciaries can only access a record of the individual's electronic communications but not their content. Where there are no instructions, the terms of the service agreement will be followed.

Canada

31. In August 2016, The Uniform Law Conference of Canada adopted the Uniform Access to Digital Assets by Fiduciaries Act (2016) (the "Canadian Model Act") that draws on the 2014 United States UFADAA (precursor to RUFADAA). The disposition of digital assets is controlled by provincial law in Canada, just as it is controlled by state law in the United States and Australia.

32. The Canadian Model Act defines a "digital asset" as "a record that is created, recorded, transmitted or stored in digital or other intangible form by electronic, magnetic or optical means or by any other similar means." This definition is similar that which has been used in Australia (See Steen et.al. 2017) and includes any type of electronically stored information and content uploaded on a website. Unlike RUFADAA, the Canadian Model Act does not define the terms "information" or "record."

Comparing USA and Canadian models

33. In both the Canadian Model Act and RUFADAA, the term "fiduciary" is defined to include personal representatives, guardians, attorneys appointed under a Power of Attorney for Property, and trustees appointed to hold a digital asset in trust (Esterbauer 2017).

34. While RUFADAA addresses provisions of American privacy legislation Canadian law does not treat fiduciary access to digital assets as a "disclosure" of personal information. Hence, under Canadian law, the impact on privacy legislation by fiduciary access to digital assets is relatively limited.

35. Unlike RUFADAA, the Canadian Model Act does not authorise custodians of digital assets to choose the fiduciary's level of access to the digital asset. Instead the Canadian Model Act states that a fiduciary's right of access is subject to the terms of the instrument appointing the fiduciary, being the Power of Attorney for Property, Last Will and Testament, or Court Order.

36. Further, unlike RUFADAA, the Canadian Model Act has a "last-in-time" priority system. The most recent instruction concerning the fiduciary's right to access a digital asset takes priority over any earlier instrument. For example, an account holder with a pre-existing Last Will and Testament, who chooses to appoint a Facebook legacy contact is restricting their executor's right to access their Facebook account after death pursuant to the Will.[xi]

37. In our submission, the Canadian model is preferable to the USA model.

Privacy Protections for Electronic Communications after Death or Incapacity - CLOUD Act vs GDPR

CLOUD Act

38. On 23rd March 2018, the USA Government passed the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") which amended the USA Stored Communications Act ("SCA"), which establishes procedures permitting the USA government to seek data from service providers of electronic communication services, such as email, or remote computing services, including cloud computing (collectively, "providers").

39. The CLOUD Act amended the mandatory disclosure provisions under the SCA to apply extraterritorially. Before the CLOUD Act, it was unclear whether the SCA could be applied to reach data that was stored outside the USA. The Supreme Court was set to resolve this issue in *United States v. Microsoft Corp*, where Microsoft had refused to comply with a federal warrant issued against it, demanding production of an individual's email records in 2013. Microsoft challenged the warrant, arguing that the government could not compel the production of the records because the underlying data was stored in Ireland and the SCA did not apply extraterritorially. In response, the government argued that the SCA did apply extraterritorially because the SCA reached all records in the recipient's custody or control, no matter where the materials are located. On 17 April, the case was disposed of as moot, in light of the CLOUD Act.

40. The CLOUD Act amended the disclosure provisions to clarify that the provisions apply extraterritorially. In doing so, it enshrined the government's position in the Microsoft case. Specifically, it stated that providers must disclose all requested records within the provider's "possession, custody, or control" whether or not the information sought is "located within or outside of the United States." This amendment permits the USA authorities to seek data from providers—regardless of where the data is stored—so long as the data is within the provider's "possession, custody, or control." The broad definition of "control" adopted by USA courts provides USA authorities with broad access to data from providers based or operating in the USA.

41. The CLOUD Act has a significant impact on international data sharing. Australian governments, companies and individuals should be aware that the USA government can now directly seek a warrant for data within the "possession, custody, or control" of providers that are based or operate in the United States, irrespective of where the data is stored.

GDPR

42. Becoming enforceable on 25th May 2018, the General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU.

43. Three of the most important regulations involve the right to be forgotten (as it is commonly known), consumers needing to opt-in in order for their data to be used, and heavy penalties should any of the regulations be breached.

44. The right to be forgotten has to do with the permanence of the internet and how data never dies, meaning everything online usually remains online. The right to be forgotten allows people to demand that personal data be removed.

45. Opting-in concerns the ability of companies like Facebook and Google to share personal data with marketers and others. Under GDPR, users must consent to the usage of their data before the companies can begin selling their information.

46. The fines for corporate misbehaviour are substantial: Either 4% of global turnover or €20 million, whichever is higher. The EU has shown its willingness to fine large companies for violation of EU law.

47. Overall, the EU is taking a far different approach compared to USA. Whereas the latter's laws have many provisions that favour the state, the EU has instead opted to have a more consumer-focused legislative philosophy.

48. There are tensions between USA and European Union laws, predominantly caused by the conflict of USA enforcement efforts and the EU's focus on the right to data privacy. We mention this, not to comment on the merits of the matter, but because governments and companies based outside of the USA must formulate laws and policies about how the CLOUD Act will impact their respective entities' data.

Relevance to Australia

49. It is worth noting that both American model legislation (UFADAA and RUFADAA) were created BEFORE their Clarifying Lawful Overseas Use of Data Act (or CLOUD Act)[xii] and before the European General Data Protection Regulation (GDPR).[xiii] Australia therefore has the opportunity of further addressing tensions relating to privacy and data sovereignty issues which have been raised in other jurisdictions.

50. In Australia the areas of law relating to your terms of enquiry are very largely state-based. While we recognise that the NSW Law Reform Commission does not have a mandate to address law reform in other jurisdictions, it is our fundamental position that it would highly desirable if your work resulted in model (uniform) laws which could be easily adopted by other Australian States and Territories.

51. We are mindful of the increasing globalisation of trade and commerce, and are keen to address and minimise the potential difficulties which could arise from substantially different policies, laws and protocols between Australian jurisdictions. This approach of uniform model legislation has been drafted in both USA and Canada (discussed below) and is in the process of being adopted by those countries' states and provinces.

Policies and Terms of Service

52. Under the Terms of Reference, you are to consider policies and terms of service agreements of social media companies and other digital service providers.

53. We anticipate that you will receive submissions from a number of major providers, and that you will be able to identify the major providers' policies in terms of service agreements.

54. Where we may be able to assist is in dealing with the concrete issues that arise from the variety of policies and terms of service agreements that you identify.

55. We invite consideration to some of the issues catalysed by End User License Agreements (EULA) and Terms of Service (TOS) Agreements typically mandated by service providers:

    (a) **Inequality of bargaining position**; it might be said that end-users are often placed in a "take-it-or-leave-it" position, by large corporations with extensive resources at their disposal, where the end-user may be compelled to agree to terms against their interests.

    (b) **Anti-competition** (anti-trust) considerations; Consideration of Australian Consumer Law protections that cannot or should not be ousted by EULA.

    (c) **Right to be forgotten;** should local legislation 'read-into' EULAs on behalf of Australian users some inalienable rights – such as the right to be forgotten – that cannot be varied or extinguished by EULA?

    (d) **Fine-print:** many EULAs are multiple pages of small-print text, beyond the ability of most ordinary individuals to comprehend.

    (e) **Ease of click-through;** the rights of individual clients (and potential customers of corporate clients) are potentially affected by careless agreement to the terms of the EULA. How much emphasis & importance should be conveyed to the user about potential rights displaced?

    (f) **Lack of understanding of rights dispossessed;** should plain English drafting be required? Similarly the use of simple language and short (non-compound) sentences? If EULA can potentially affect property rights and testamentary considerations of user, what is the appropriate way of dealing with incapacity issues? Ie can/should a EULA be upheld against the interests of a user if it can be demonstrated that the user lacked capacity at the time of agreeing the EULA?

(g) **Data sovereignty**; USA is ubiquitous when it comes to data traffic on the internet/cloud, and its national security apparatus (NSA/PRISM[xiv]) can have an impact on how business is conducted – especially within the cloud where data is circulating across the globe. USA also often pushes other countries to open-up on their privacy laws, while USA itself has relatively lax policies concerning how companies like Google and Facebook can use the data they gather online.

(h) **Hidden transfer of jurisdiction/data**; a service provider can be located anywhere in the world, and yet still attract CLOUD Act complications, such as if the provider contracts with Amazon Web Services (AWS) for the storage of the user's data. Even if the AWS data centre is not located in the USA, the mere fact that AWS has a connection with USA would be sufficient nexus for USA authorities to demand production of Australian data. Some providers' EULA reserve the right to require that data be transferred to the USA, (such as Trello) ie if their employees and contractors need access to data stored in Australia or the EU from USA for technical and support related reasons. Should Australian legislation mandate a commitment to ensuring such transfers are compliant with applicable data transfer laws, including GDPR?

(i) **Data Security** (protection); what rights are afforded to the end-user? Should common law compensation for breaches be permitted to be ousted or varied in EULA, and if so should quantum of damages be permitted to be varied according to nationality of user (eg USA users are typically entitled to higher damages in some types of claims).

(j) **Geo-blocking:** many USA-based service providers wish to restrict services based on the location/nationality of the user – eg Netflix. However Australian laws might not necessarily prevent circumvention mechanisms (such as VPN) which would otherwise be impermissible under USA law. Should Australian laws seek to prevent a EULA enshrining effective penalties for Australian users doing something that would be lawful within Australia?

(k) **Data portability**; (pain-of-disconnect) Once data has been captured by the service provider, can it be easily accessed, migrated and transferred to an alternate provider, or is it locked to proprietary formats (walled garden)? Australian laws protecting the consumer's right to take their own data elsewhere should be considered.

(l) **Privacy and confidentiality**; Facebook's Cambridge Analytica issue has emphasised the need for caution when considering how and to what extent EULAs are permitted to displace Australian Privacy Principles. EULAs which absolutely prevent sharing of passwords (even to trusted agents and fiduciaries) require consideration. It is desirable to enshrine in local legislation the ability to displace or make unenforceable any terms in EULAs

which interfere with a local fiduciary's ability to lawfully deal with their principal's affairs and assets.

(m) **Displacement of local laws and customs** by overseas companies (for example, most Australians would expect that their local Power of Attorney legislation would permit an agent to operate the digital accounts of their principal under PoA. However most American EULAs preclude this.)

56. The rules of private international law have grown up in a pragmatic way, sensible of the degree to which a State may project beyond its borders. Changes to the rules of private international law would need to be modest and focused. Unintended impact of any such change must be mitigated. That said, this seems to be a necessary aspect to your deliberation, especially to safeguard Australian users from the extraterritorial effects of foreign laws and contracts.

Laws Affecting Access to NSW Person's Digital Assets after Death

57. Your terms of reference suggest that the laws applicable include those relating to intellectual property, privacy, contract, crime, estate administration, wills, succession and assisted decision-making.

58. We agree with that listing, but would add that private international law must also be considered.

In particular, we suggest that the following statutes be considered:

(a) *Crimes Act 1900* (NSW), which as noted in your terms of reference prohibits "unauthorised access" to restricted data held in a computer;

(b) *Succession Act 2006* (NSW), which (as noted in your terms of reference

(c) *Probate and Administration Act 1898* (NSW);

(d) *Trustee Act 1925* (NSW);

(e) *Privacy Act 1988* (Cth);

(f) *Copyright Act 1968 (Cth);*

(g) *Acts Interpretation Act 1901* (Cth);

(h) *Anti-Money Laundering And Counter-Terrorism Financing Act 2006* (Cth).

59. Further, since some of the digital assets may be (or purport to be) subject to different legal systems interstate and overseas, we suggest that recommendations take into account the current state of cross-border recognition and private international law affecting those arrangements. This might lead to consideration by you of any necessary modifications to the rules of private international law. One example would be terms of service said to be subject to the laws of a foreign country, or terms of service purporting to submit disputes to

a particular dispute resolution process, whether here or abroad. We acknowledge there are practical issues which may arise.

60. We recommend an analysis to identify any privacy or criminal law barriers to fiduciary access to digital assets in current Australian law.

Laws Affecting Access to NSW Person's Digital Assets on Incapacity

61. We repeat the views expressed under the previous heading.

62. The NSW and Commonwealth statutes that require examination are:

    (a) *Crimes Act 1900 (NSW);*

    (b) *Powers of Attorney Act 2003* (NSW);

    (c) *Mental Health Act 2007* (NSW)

    (d) *Guardianship Act 1987* (NSW);

    (e) *Trustee Act 1925* (NSW);

    (f) *Privacy Act 1988* (Cth);

    (g) *Copyright Act 1968 (Cth);*

    (h) *Acts Interpretation Act 1901* (Cth); and

    (i) *Anti-Money Laundering And Counter-Terrorism Financing Act 2006* (Cth).

Jurisdictional Issues

63. Your terms of reference raise relevant jurisdictional issues, including the application of Commonwealth laws. We expect that the following laws require consideration:

    (a) *Electronic Transactions Act 1999;*

    (b) *Australian Privacy Principles.*

Further Work with You

64. STEP is committed to working with you on this reference. We would welcome the opportunity to meet, as needed. As the reference progresses, we would value your invitation to participate further.

Annexure A

Examples published in the Media

- http://www.dailymail.co.uk/news/article-2286816/Loren-Williams-Facebook-photos-lost-forever-death-account-holder-current-law.html
- http://www.dailymail.co.uk/news/article-2153548/Family-fights-access-sons-Facebook-Gmail-accounts-suicide.html
- https://www.themorningbulletin.com.au/news/children-devastated-after-dead-dads-facebook-profi/2634234/
- https://www.yahoo.com/news/father-fights-facebook-remove-photos-of-my-girl-164043995.html
- http://kfor.com/2016/01/18/its-nonsense-apple-refuses-to-give-widow-a-password-without-a-court-order/
- http://www.wday.com/news/3660582-family-fights-access-late-sons-digital-data
- https://www.telegraph.co.uk/news/2016/07/30/apple-tells-mourning-father-to-get-court-order-to-access-sons-da/
- http://www.sandiegouniontribune.com/sdut-winchester-grieving-mother-calls-for-facebook-2012jan13-story.html
- http://today24news.com/offbeat/phoebe-princes-suicide-cause-of-death-revealed-232219
- http://www.browndailyherald.com/2007/02/22/facebook-profiles-become-makeshift-memorials/
- http://www.bbc.com/news/world-latin-america-22286569
- https://www.cnet.com/news/facebook-fights-for-deceased-beauty-queens-privacy/
- https://www.law360.com/articles/1032671/family-sues-apple-seeking-late-loved-one-s-icloud-info
- https://www.cnet.com/news/taking-passwords-to-the-grave/
- https://www.huffingtonpost.com.au/entry/death-facebook-dead-profiles_n_2245397

Case Law

- *In Re Ellsworth, No. 2005-296, 651-DE (Mich. Prob. Ct. 2005)* – where a US court ordered Yahoo! to providing the deceased's family with copies of emails.

- *In re Air Crash Near Clarence Ctr., N.Y., on Feb. 12, 2009, No. 09-CV-961S, 2011 WL 6370189, at *6 (W.D.N.Y. Dec. 20, 2011)* – where federal court in the USA ordered the estate of a woman to produce all of the deceased woman's social media accounts, emails, text messages, and instant messages that related to the decedent's domicile and the estate's loss of support claims.

- *Davis v. Google, Inc., No. 09CH15753 2009, 2009 WL 995128 (Ill. Cir. Apr. 9, 2009)* - where a Court in the USA was unable to grant a court order (due to applicable laws and no fiduciary being appointed) compelling Google to take down the post that included an allegedly defamatory statements.

- *Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 657 (N.Y. Sup. Ct. 2010)* – where a court in New York, USA ordered a plaintiff to give the defendant "access to the plaintiff's current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information."

- *Stassen v Facebook 2012* – where a court in the US ordered Facebook to provide a family access to their deceased son's account and assets.

- *Fairstar Heavy Transport NV v Adkins. Reference [2012] EWHC 2952* – where a court in the UK found that emails could not be considered as property.

- *Facebook, Inc.'s Motion to Quash Subpoena in Civil Case, No. C 12-80171 LHK (N.D. Cal. Aug. 6, 2012)* – where a court in California, USA granted Facebook's motion to quash the subpoena, but refused to address whether Facebook could voluntarily disclose the content.

- *Ajemian v. Yahoo!, Inc., 478 Mass 169 (2017)* – where a court in the US held that the personal representatives may provide lawful consent on the decedent's behalf to the release of the contents of the Yahoo e-mail account.

- *United States v. Nosal 2016* – where a court in California, USA held that sharing a password can be a crime of accessing a protected computer "without authorization" under the *Computer Fraud and Abuse Act.*

- *Vitacost.com, Inc v James McCants (No. 4D16-3384)* – where the court held that there had been inadequate notice of the relevant terms and conditions because each purchaser had to scroll multiple pages to find the hyperlink; and

- *Digital Central (Assets) Pty Ltd v Stefanovski [2017] FCA 738* – where the Federal Court emphasised that misuse of password-protected information is likely to breach an equitable obligation of confidentiality.

NOTES

[i] Donna Molzan has been Legal Counsel with Alberta Justice & Solicitor General (JSG) for over 25 years. Her work has included reforms to limitations of actions, personal directives, fatal accidents, survival of actions, Surrogate rules and a significant number of statutes under the responsibility of the Department of JSG. She was appointed Queen's Counsel in 2014. Donna was senior counsel in working on the reform of the Wills and Succession Act in Alberta in 2012. She was seconded to the Alberta Law Reform Institute in 2009 for one year where her projects with ALRI included lapse in wills (predeceasing beneficiaries), rectification of wills, caveats and bonds in the administration of estates, issue identification in the administration of estates and review of the JSG draft of the Alberta Rules of Court. Her work was published in ALRI Final Report No. 98, Wills and the Legal Effects of Changed Circumstances, August 2010.
Donna was the Project Lead for the reform of laws relating to estate administration resulting in the Estate Administration Act in 2015. Donna was an observer on the US ULC committee and participated in the ULC development of UFADAA and RUFADAA.
Donna was the Chair of the Uniform Law Conference of Canada (ULCC) Access to Digital Assets by Fiduciaries (ADAF) Project which resulted in the adoption of the Uniform Act in 2016.
Donna is currently the project lead for the reform of the Trustee Act in Alberta. Donna worked jointly with the Alberta Law Reform Institute to conduct consultations across Alberta on ALRI Report for Discussion No. 28, A New Trustee Act for Alberta, November 2015. Her work is published in ALRI Final Report No. 109, A New Trustee Act for Alberta, January 2017.
For the last ten years, Donna had been an instructor at the University of Alberta, Faculty of Law in the area of Civil Procedure. Prior to her work as an instructor at the University of Alberta, Donna was an instructor in the Alberta Bar Admission course for 10 years in the area of legal writing and drafting.
[ii] Kathleen Cunningham, B. Comm, LL.B, MPS, TEP is the Executive Director of the British Columbia Law Institute / Canadian Centre for Elder Law. Ms. Cunningham is a distinguished lawyer with particular expertise in trust law and law reform. Ms. Cunningham's career includes extensive experience in estate, trust and adult guardianship matters through her work for RBC Wealth Management, and with the Public Guardian & Trustee of British Columbia. Ms. Cunningham served as a Director of BCLI from 2007-2009 and as a Committee member on BCLI's Modernization of the Trustee Act project and on BCLI's Undue Influence project.
[iii] From 1983 to 1985, Peter J M Lown QC was Executive Director of the Canadian Institute for the Administration of Justice; from 1990 to 1992, he was Chairman of the Uniform Law Section of the Uniform Law Conference of Canada; and from 1993 to 1995 was the President of the Uniform Law Conference of Canada. He chairs the Uniform Law Conference Advisory Committee on Project Development and Management. He is a Director and Treasurer of the Federation of Law Reform Agencies of Canada, Treasurer of the Commonwealth Association of Law Reform Agencies, and was a Director of the Canadian Forum on Civil Justice from 1997 to 2005.
After a year as special counsel to the Alberta Law Reform Institute to report on electronic depositories and transfer of securities, he was appointed Director of the Institute in April 1988 for a term of 5 years, and reappointed for further 5 year terms in 1993, 1998, 2003 and 2008.
During this time he has spearheaded the implementation of legislation on enduring powers of attorney, personal directives, limitations of actions, and a new system of Surrogate Rules. More recently he has been concentrating on pilot projects on Caseflow Management, proposals for recognition of judgments with the Uniform Law Conference of Canada, and a comprehensive revision of the Rules of Court. In January 2001 he received the Law Society/ Canadian Bar Association Award for Distinguished Service to Legal Scholarship.
He has participated on working groups for a number of Uniform Law Conference of Canada projects – Enforcement of Judgments, Choice of Law in Consumer Contracts, National Class Actions, Limitations, Privity of Contract, and Trust Law Reform.
[iv] Further information about the SIG can be found at the following link: https://www.step.org/digital-assets-global-special-interest-group.
[v] These include: s478.1 *Criminal Code 1995* (Commonwealth); s247A and 247G *Crimes Act 1958* (Victoria); s308H *Crimes Act 1900* (New South Wales); s44 *Summary Offences Act 1953* (South Australia); s420 *Crimes Act 1900* (Australian Capital Territory); s440A of the *Schedule to the Criminal*

Code Act 1913 (Western Australia); s408D *Criminal Code 1899* (Queensland); and s257D *Criminal Code Act* 1924 (Tasmania).

[vi] 15 U.S.C. § 45(a)(2) (2012).

[vii] To this could be added digital assets specific to business operators such as client lists, and other items of an intellectual property nature.

[viii] Ploss (2017) notes that while a personal computer, tablet, and smartphone are generally considered to be portals to the digital world, Ploss argues they should be classified as part of the digital world because such devices are generally locked down by password or finger touch encryption.

[ix] Since 2005, Suzy Brown Walsh has served as one of Connecticut's Commissioners on Uniform Laws. As such, she represents the state as a member of the Uniform Law Commission, a national organization which promotes statutory uniformity. She chairs the ULC's drafting Committee on Electronic Wills and chaired the ULC's Revised Uniform Fiduciary Access to Digital Assets Act. Suzy is currently a member of the Regulation of Virtual Currency Businesses and Directed Trust Drafting Committees. She has served on the ULC's Scope and Program Committee and drafting committees for the Uniform Adult Guardianship and Protective Proceedings Jurisdiction, Uniform Insurable Interests in Trusts, Uniform Premarital and Marital Agreements, Uniform Powers of Appointment and Trust Decanting Acts. In addition, Suzy chaired the drafting committee on Amendments to the Uniform Principal and Income Act (2008), as well as a study committee on Mental Health Advance Directives. She taught Estate Planning and Taxation at the University of Connecticut Law School.

[x] Section 2 (10) defines a "digital asset" to be "an electronic record of which an individual has a right or interest." The comments to the Act state that the following is included in the definition:

(i) Information that is stored on a user's computer and other digital devices;

(ii) Content uploaded onto websites; and,

(iii) Rights in digital property.

Section 3(a), the term "fiduciary" includes the following parties:

(a) An Agent or Attorney-In-Fact acting under a durable power of attorney executed before, on, or after the effective date of the Act;

(b) A Personal Representative (whether under a Will or intestacy) acting for a decedent who died before, on or after the effective date of the Act;

(c) A Court Appointed Conservator (or Guardian) appointed before, on or after the effective date of the Act; and,

(d) A Trustee acting under a trust created before, on, or after the effective date of the Act

[xi] Reference. Nick Esterbauer Comparing Canadian and American Digital Asset Legislation 6 April 2017 https://hullandhull.com/2017/04/comparing-canadian-american-digital-asset-legislation/ accessed 21.20 26/04/18

[xii] The Clarifying Lawful Overseas Use of Data Act or CLOUD Act is a United States federal law enacted in 2018 relating to data privacy and government surveillance laws to affect industry cloud computing practices. Primarily the CLOUD Act allows USA federal law enforcement to compel USA-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the USA or on foreign soil.

[xiii] The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU. The GDPR aims primarily to give control to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. It was adopted on 27 April 2016. It becomes enforceable on 25 May 2018.

[xiv] PRISM is the USA National Security Agency (NSA) program that collects emails and other data hosted by cloud service providers without notifying the data owners. Cloud service providers such as Microsoft, Google, and Yahoo are required to turn over customer data, to the USA government. PRISM raises immediate privacy and confidentiality issues and differs from existing legislation such as the Electronic Communications Privacy Act and the USA Patriot Act, in some key respects. The PRISM program:

- Operates in secret with limited or no transparency
- Provides no mechanism for customers to know that their data has been accessed
- Can be used to data mine all corporate emails

The issues raised by the PRISM program create a significant tension between privacy advocates with attempts to enhance USA national security. For corporations, the issues are even more complex.

Unlike individuals, corporations have fiduciary obligations, legal requirements and other business responsibilities to ensure corporate data is not only secure, but also private and confidential.
The PRISM program raises many questions for corporations considering migrating to the cloud. Maintaining ownership and control of corporate data is a separate and distinct requirement, apart from the hosting, processing, and traditional security features that leading cloud providers provide as part of their service.