DIGITAL DEATH

"Most of us now live two lives, one in our actual world and the other in the virtual. When we die, our physical existence might come to an end, but the virtual presence lingers on"

By: S. Balasubramanya[i]

1. Introduction – Digital Asset

In a time when most of our daily life has gone digital — from socializing, to banking, to ordering pizza — have we thought of what to do with all our digital data and assets on our 'death'? It is quite normal to expect plethora of digital assets that get created during our modern day life – from emails-ids (Gmail, yahoo-mail, etc.), social media accounts (WhatsApp, Facebook, Twitter, Snapchat, YouTube, etc.), various financial accounts for using mobile and internet services (banking, insurance, brokerage, depositories, etc.), commercial trade (Amazon, Flipkart, etc.), Entertainment (BookMyshow, Netflix, Amazon Prime, etc.), government interactions (Income tax, municipal tax, pension, etc.), health data (Hospitals, health authorities like the present COVID-19, etc.), travel (airlines, train-IRCTC, bus, etc.), transport (Ola, Uber, Redbus, IRCTC, etc.) and so on and so forth. In addition to having various accounts, many people could have created digital IP (Intellectual Property) like a book, songs, lyrics, art, blogs, photos, training & education material, and many more. What about real money held in various e-wallets like PayPal, Paytm, Uber, Ola, etc., and crypto currency like Bitcoin. These are the 'Digital Assets' created and belonging to individuals operating in the present digital economy and society.

The United States Department of Commerce reported from census data that from 2000 to 2010, the percentage of Internet-connected households jumped from 41.5% to 71.5%[ii]. From domain names to blogs, avatars to social media, this rising tide of Internet use translates into more digital property that can have both financial and sentimental value assets, stored across multiple digital devices, at an average of $55,000 per person. Apart from financial value, some digitally stored assets (photographs, poems, messages, videos, emails, etc.) may have sentimental (rather than financial) value to members, users, or subscribers—as well as their families and friends.

Does this, so called 'Digital Asset', has any mechanism to bequeath it to the designated beneficiaries? Can an individual designate beneficiary for inheriting these digital assets through the mechanism of 'Will' or 'Trust'? What happens to it in the absence of a will to bequeath the same – does the state has any form of succession or inheritance act to ensure transfer of these digital assets in an orderly manner? What happens to the contents in these accounts – will it be private and belongs to the individual which may be prohibited to be accessed by the respective service providers? Are there any laws or statutes or regulations governing the responsibility of such service providers? Does the physical location of such 'content' have any bearing on where service providers keep such data? Does this impact the execution of wills containing digital assets? As can be seen, we need to think and address these issues when it comes to the management of 'Digital Assets'.

2. The importance of privacy in digital asset after death

A privacy breach exposes an individual's personal information to the public. This can even happen after the death of the individual. The impact of such a breach can affect a few individuals or millions — and there have been many instances of large-scale data breaches over the last five years including individuals who are no more in this world. Does the individual, who is no more in this world have a right to privacy – if so, how will it be addressed? Do the legal heirs have any responsibility or a right to protect such privacy of the deceased person? How will this be enforced and against whom – the service provider who has stored such data or against the culprit who caused the breach? What are the possible remedies for a such a breach of personal information of a deceased person? So far most of the privacy laws have excluded the data belonging to deceased persons. Should this position change?

As we can see, as we go through this more and more, there are more and more questions to be addressed. It is not going to be simple and straightforward. One has to be in for some surprises in dealing with such situations. So, how can these potential difficulties be reduced when one is alive through the process of WILL or TRUST?. Let's look at few possibilities to designate beneficiary through will or other mechanism for various digital assets

3. Position of few service providers

Before we move to look at the legislation, let's look at what some of the service providers are providing to enable such a situation.

Blogs, photos, financial accounts

Like all creative products, literary writings, research notes, photographs, etc., that are created online will pass on to the legal heir of the deceased. There is, however, no specific law in India on this, but they are seen as intellectual property and treated likewise. Similarly, legal heirs have the right to access bank accounts and online records with, say, the Income Tax Department. Companies will have first right to stuff lying in official email services and servers.

Facebook

When a user passes away, Facebook gives their friends and relatives the option of memorializing their account to protect privacy. "Memorializing an account sets the account privacy so that only confirmed friends can see the profile (Timeline) or locate it in search. Friends and family can leave posts in remembrance. Memorializing an account also prevents anyone from logging into the account," says the Facebook blog. Facebook does not divulge the login details of the account to anyone, but "verified immediate family members" can request the removal of any Facebook account if they do not want to get it memorialized.

Google

Google says that in rare cases it "may be able to provide the Gmail account content to an authorized representative of the deceased user". But the post on Google Support adds that "any decision to provide the contents of a deceased user's email will be made only after a careful review, and the application to obtain email content is a lengthy process. Before you begin, please understand that Google may be unable to provide the Gmail account content and sending a request or filing the required documentation does not guarantee that we will be able to assist you". The same applies to all Google services.

Yahoo

Email accounts of Yahoo are automatically deleted if it stays dormant for over four months.

Yahoo will also close the account if a copy of the death certificate is emailed to cc-advoc@yahoo-inc.com.

LinkedIn

Account is closed if death verification form is filled.

PayPal

If a death is reported, the account will be closed, and a cheque made out to the account holder is issued to the legal heir.

Twitter

Account closed if request is received.

Other considerations:

Though we considered few of the service providers, it is not exhaustive. There could be differences, as can be seen above, with respect to treatment of such digital assets by various service providers. It may vary across different parameters; few are listed below, from testator's view:

- Should the account be handed over to legal heirs?
- What happens to the data held within these accounts? Should those be also given or has a consideration of Data Privacy aspects before the same can be given?
- What about historical data?
- How should the financial digital assets be distributed? Can the person specify through will or trust or gift the disposition of such assets?
- What about sensitive data about health aspects which the person does not want to be shared due to privacy considerations?
- Old sensitive emails
- Personal emails in employer's email systems
- Where the data is stored – in India, in USA or elsewhere?
- Impact of laws prevailing in multiple jurisdictions – which laws govern what & where?
- What are procedural issues and potential bottlenecks?

Briefly, provided below is a peek into few prevailing legislations in USA in this area. Also, there are at times competing interests from service provides as opposed to testator, like[iii]:

- Use of privacy
- Contractual expectations of user
- Contractual compliance by service provider
    - Make accounts non-transferable, and any rights to them terminate upon the account holder's death
    - User may designate a person to manage account upon testator's death; only that designee or person identified in valid will or trust with clear consent to whom to disclose the content after death will be able to seek disclosure of content
    - Require executor of other fiduciary to get a court order
- Statutory compliance by service provider – Stored Communications Act of 1986 (SCA)
    - Protects personal information stored by electronic communication service providers and prohibits providers from knowingly disclosing the contents of customer's electronic communications or subscriber records
    - Criminalizes voluntary disclosure of communications content while in electronic storage
    - Common exceptions (not inclusive) are:
        - Addressees, intended recipients and their agents
        - Lawful consent of originator or addressee
        - Official reports to NCMEC (National Centre for Missing & Exploited Children)
        - Law Enforcement in some circumstances where communication shows commission of crime
- Statutory compliance by service provider – State Law / RUFADAA (Revised Uniform Fiduciary Access to Digital Assets Act)
    - Many enacted before advent of email or social media and did not account for digital assets
    - RUFADAA enactment – gives unfettered access to deceased user content which is strongly opposed by tech industry and privacy advocates

- RUFADAA hierarchy – Online Tool of Provider >> Will, Trust, POA or other record >> Service Provider's Terms of Service (TOS)
- 41 states and the U.S. Virgin Islands have adopted this act

- Conflicts between federal and state laws
- Estate planning / Estate's interest in administration
  - Requires explicit consent by deceased user for disclosure
  - Executor must petition the court & explain why the asset is needed
  - Providers may ask for court orders, limit their compliance, may charge fees to comply and may even reject burdensome requests and ensure disclosure does not violate SCA and ECPA (Electronic Communications Privacy Act)
  - Providers may not provide access to deleted assets or joint accounts
  - Providers have immunity if they act in good faith to comply
- Family interest in content of loved one

There is plethora of such factors to consider before deciding what and how to dispose of such digital assets at death.

4. Legislation For managing Digital Assets

A fiduciary ensures that property is well managed, during the life or after the death of the property owner. In the physical world, the fiduciary's roles are widely accommodated by other bodies of law (such as contract law, banking and payments law, privacy law, criminal law, and the like). But the same cannot be said for the digital world, which has developed without close attention to fiduciaries' roles.

In tune with technological changes, legislative changes to accommodate and address potential issues emanating from such technological change is necessary. At the moment, we do not have in place any law in India pertaining to digital legacies of people. There is the Information Technology Act, 2000, which is applicable to all digital information, data and assets. However, its applicability is excluded to testamentary, disposition and wills. The law pertaining to wills is governed by the Indian Succession Act. We require specific laws in the country pertaining to digital legacies and bequeathing their digital assets to the next of kin.

Before we proceed further, let's briefly look at some of the case laws in the USA, as below:

Case: Begin Quote of the case

MARIANNE AJEMIAN, co-administrator, & another vs. YAHOO!, INC. 83 Mass. App. Ct. 565

The plaintiffs, who are co-administrators of their brother John's estate, brought the underlying declaratory judgment action in the Probate and Family Court, seeking a declaration that electronic mail messages (e-mails) John sent and received using a Yahoo!, Inc. (Yahoo!), e-mail account is property of his estate. A probate judge dismissed the complaint, concluding that a forum selection clause required that suit be brought in California. The judge also concluded that res judicata barred the administrators from bringing their claim in a Massachusetts court, but did not bar them from asserting the same claim in California. In light of those conclusions, the judge dismissed the suit (apparently without prejudice), stating that the parties' substantive arguments should be considered by the California courts.

The relevant factual and procedural background.

Around August or September 2002, Robert opened a Yahoo! e-mail account for John. Although Robert opened the account to be used primarily by John, Robert was to have access to and share the account as a co-user. Robert provided the information requested by Yahoo! to open the account, and he also set up a password to access the account.

According to Yahoo!, "prospective users are given an opportunity to review the Terms of Service and Privacy Policy (TOS) prior to submitting their registration data to Yahoo!." Robert does not dispute this but avers that he has no affirmative memory of accepting the TOS or of seeing or reading it when he opened the account. The printed version of the TOS in effect in 2002 when Robert opened the account (2002 TOS) is ten single-spaced pages long and consists of twenty-five (25) numbered sections.

John was struck and killed by a motor vehicle on August 10, 2006. At that time, there was a new version of the TOS in effect. Most of the provisions set out above were materially unchanged; however, there were at least two new sections:

"22. NO THIRD-PARTY BENEFICIARIES. You agree that, except as otherwise expressly provided in this TOS, there shall be no third-party beneficiaries to this agreement.

". . .

"26. GENERAL INFORMATION[.] . . . No Right of Survivorship and Non-Transferability. You 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."

As noted above, Robert opened the account for John, who then became its primary user. However, Robert states that he was a co-owner of the account and continued to access the account from time to time. That said, he had not accessed the account for some period before John's death and had forgotten the password.

Beginning shortly after John's death, the plaintiffs have repeatedly tried to gain access to the e-mail account. Initially, they sought access in order to obtain the e-mail addresses of John's friends to notify them of his death and memorial service. Subsequently, the plaintiffs (by then appointed as co-administrators of John's estate) sought the e-mails to help identify and locate assets and administer John's estate. Although Yahoo! initially agreed to turn over the information provided the family produced a copy of John's birth and death certificates and other documentation, it later refused them access to the account or its contents, relying on the Stored Communications Act, 18 U.S.C. §§ 2701 et seq. (2006), which Yahoo! interpreted to preclude disclosing John's e-mails even to the administrators of his estate.

Further negotiations led the parties to reach a partial resolution to the effect that if the plaintiffs obtained a valid court order requiring only production of basic subscriber and e-mail header information, and the order did not require Yahoo! to produce the contents of the e-mails, then Yahoo! would not oppose issuance of such an order and would comply with it. No agreement was reached regarding the contents of the e-mails, except that Yahoo! would continue to preserve them.

Consistent with this agreement, the plaintiffs filed a declaratory judgment action in the Probate and Family Court in September, 2007 (first action), seeking only "a binding declaration of right that the Administrators are entitled to access the subscriber records for the [e-mail] account," and an order that Yahoo! produce the subscriber records for that account. The complaint did not seek the contents of the e-mails themselves. The complaint informed the court of the terms of the agreement between the plaintiffs and Yahoo! as set out above. Yahoo! did not appear in the first action, nor did it oppose the relief sought. Accordingly, the plaintiffs filed an unopposed motion for summary judgment, together with a proposed form of judgment, which a probate judge entered on January 3, 2008. That order provided:

"1. The Administrators of the estate of John Gerald Ajemian, Marianne Ajemian and Robert Ajemian, are entitled to receive subscriber records, as specified below, for Yahoo! e-mail account 'jajemian__1@yahoo.com.'

"2. Yahoo! Inc. shall provide all subscriber records and e-mail header information, not to include e-mail content, for Yahoo! e-mail account 'jajemian__1@yahoo.com' to the Administrators . . .."

Yahoo! produced the subscriber information pursuant to the judgment.

Thereafter, the plaintiffs renewed their requests for the contents of the e-mail account. The parties engaged in further negotiations for several months but reached no agreement, and therefore, the plaintiffs filed a second declaratory judgment action in the Probate and Family Court on September 15, 2009 (second action), which is the suit underlying this appeal.

Unlike the first action, the second action is brought not only by Robert and Marianne as administrators of John's estate, but also by Robert individually, based on his allegation that he is a co-owner of the e-mail account. The complaint seeks access to the contents of the e-mail account on two theories: (1) that the e-mails are property of John's estate and, therefore, Marianne and Robert (as the estate's administrators) are entitled to access to them; and (2) that as co-owner of the account, Robert individually is entitled to its contents.

Yahoo! moved to dismiss the second action on four grounds: (1) the forum selection clause in the TOS required that the suit be brought in California; (2) the suit was untimely given the one-year statute of limitations in the TOS; (3) the doctrine of res judicata barred the action; and (4) the complaint failed to state a claim upon which relief could be granted because e-mails in the account are not property of the estate. A different probate judge allowed the motion, finding that the first action barred the second action under the doctrine of res judicata. Despite this determination, the judge also ruled that the forum selection clause was enforceable and that the case should be dismissed without prejudice to its being refiled in California, and that the California courts should decide whether the suit was time barred and whether the e-mails were the property of the estate. This appeal ensued. End Quote of the case

The purpose of quoting the above case, though partially, is to illustrate the complexity involved in obtaining any of the contents of the email communication between the deceased and any other persons, because of the intricate legislations and regulations prevailing in USA. Further, since most such service providers are based and Head Quartered in California, USA, one cannot hope to escape jurisdictions of the California and USA courts in such cases. This is also to illustrate the point how contractual arrangements between the subscriber and the service provider can have an influence on the outcome of such cases.

Hence, it is important for the testator to take early and necessary action either by himself or herself or through the will or a POA (Power of Authority) specifying what the intention is and what the legal heirs or beneficiaries to do in such an eventuality.

5. Possible approach to a solution

One can consider various approaches for managing the digital assets. One such approach is illustrated below. One is suggested to follow the steps indicated and plan for proper disposition of individuals' digital assets and give sufficient importance as they would give for other forms of assets.

Step-1:

Like in traditional assets, identify and inventory all the forms of digital assets, including all online accounts where such property is housed as also other digital assets housed in their laptops. Mobile phones, external hard drives and also cloud, early enough. Also, list if any such digital assets are stored in their office computers or transfer such assets from official computers to personal computers or to a common cloud service provider. This is important to recognize that in today's house office concept, there is every possibility of keeping some of personal emails and other digital assets in office computers.

Step-2:

The individual must list down information about all usernames, passwords, and any other security questions for each of such digital asset and preserve account information. Also list those accounts which may need periodic changes to security credentials, like need for changing passwords every 30 days or so. Store all such information in a digital diary or in an easily accessible hard copy.

Step-3:

Select or identify an individual representative or a fiduciary, who need not be necessarily the same person who would perform an executor of fiduciary functions. The digital fiduciary preferably to have technical qualification and familiar with computer and internet usage, that makes him or her more capable and suitable of satisfying the account holder's desires regarding management of his or her digital assets. It is well-established in the common law that the personal representative of a deceased person's estate "*stands in the shoes of the decedent*" in administering that estate, and other fiduciaries have the authority to take actions necessary or incidental to achieve a principal's objectives, unless the principal directs otherwise.

Step-4:

The testator should provide detailed instructions regarding how his or her digital assets have to be managed. These instructions will help the digital fiduciary to access accounts, communicate with the relevant and appropriate service providers, manage digital assets, and coordinate with other fiduciaries and interested parties or persons.

Step-5:

In this last step, the testator should give the digital fiduciary the necessary and proper authorizations. This may be in the form of Power of Authority (POA) or a social media will[iv] or trust – which can also be extended to conservatorships which can purportedly isolate digital assets from other more traditional assets.

While the above appeals more readily, it raises one primary issue. It may cause account holders to violate the provisions of the Terms of Service (TOS) of various service providers which prohibit them from disclosing their account access information to third parties, that prohibit transfer of the account itself, or that prohibit third parties from accessing their accounts. Any of these types of violations may trigger remedial rights specified in the TOSs, sometimes including termination of service. Thus, the digital estate planning nonetheless may be impeded by the contractual issues that the TOSs raise during the planning and execution processes.

So, what is the way out to deal with proper transition of digital assets to the designated beneficiaries or legal heirs in India. What should the legislature do for addressing this issue which impinges on multiple regulations of Information privacy, IPR, Criminal law, evidence law, civil procedure and criminal procedure, property law and a host of related regulations. Also, how to deal with many service providers situated outside India and the data itself may also be residing in cloud data storage outside India.

A possible high-level approach is given below for a simplified and uniform legislation across India.

- Provide equivalence to designating beneficiaries for digital assets through the will process
- Allow testator to designate one or multiple digital fiduciaries for specified digital asset
- For money wallets or crypto currency, provision should be made to designate nominee
- Provision of a POA (Power of Authority) to the service providers of various digital services
- Review any amendments needed for the Information Privacy bill/ Data Protection Act
- International legal connect with service providers' jurisdiction as appropriate
- TOS for Indian residents' accounts to be simplified and subject to jurisdictions within India
- Acceptance of death certificate issued by Indian municipal authorities by service providers
- Online verification mechanism for beneficiaries or nominees by service providers
- Enactment of a suitable law across India (like RAFAADA in USA) & its impact on other laws

- Education and training for law enforcement bodies, judiciary and common public
- Establishment of a 'Digital Trust Services' for the benefit of Indian residents
- A comprehensive governance mechanism across different bodies of law enforcement

While authorities responsible for defining a long-term solution may take its own course and time, what is the way out in the interim? What should the account holder of different digital assets do in the interim? Let us look at possible options to address some aspects of this inheritance or succession of digital assets.

To this direction, the testator can follow steps 1 to 5 described earlier. The testator should expressly authorize the service providers to disclose their private information to their designated fiduciaries. This statement of authorization should clearly state that the testator's intent to satisfy the different laws to ensure that the fiduciaries and service providers have evidence of the testator's '***lawful consent***' and '***authorized access***'. The following could be a simple clause that can be included in the will of the testator:

> "***Powers and authorizations regarding digital property.*** *The personal representative may exercise all powers that an absolute owner would have and any other powers appropriate to achieve the proper investment, management, and distribution of: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; (4) any user account of mine; and (5) any domain name of mine. The personal representative may obtain copies of any electronically stored information of mine from any person or entity that possesses, custodies, or controls that information. I hereby authorize any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to the personal representative: (1) any electronically stored information of mine; (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service; and (3) any record or other information pertaining to me with respect to that service. This authorization is to be construed to be my lawful consent under the relevant laws (e.g. Electronic Communications Privacy Act of 1986, as amended; the Computer Fraud and Abuse Act of 1986, as amended; and any other applicable federal or state data privacy law or criminal law as in USA or any other equivalent on other jurisdictions). The personal representative may employ any consultants or agents to advise or assist the personal representative in decrypting any encrypted electronically stored information of mine or in bypassing, resetting, or recovering*

any password or other kind of authentication or authorization, and I hereby authorize the personal representative to take any of these actions to access: (1) any kind of computing device of mine; (2) any kind of data storage device or medium of mine; (3) any electronically stored information of mine; and (4) any user account of mine. The terms used in this paragraph are to be construed as broadly as possible, and the term "user account" includes without limitation an established relationship between a user and a computing device or between a user and a provider of Internet or other network access, electronic communication services, or remote computing services, whether public or private."

The above clause in a will and a separate authorization incorporating the above provision addresses disclosure, as well as authorized access. This should cover most of the digital assets of the testator to pass onto the desired beneficiaries.

A sample stand-alone authorization and consent document that could be executed individually from a POA, Will or trust document, is provided below:

"Authorization and Consent for Release of Electronically Stored Information

I hereby authorize any person or entity that possesses, custodies, or controls any electronically stored information of mine or that provides to me an electronic communication service or remote computing service, whether public or private, to divulge to my then-acting fiduciaries at any time: (1) any electronically stored information of mine; (2) the contents of any communication that is in electronic storage by that service or that is carried or maintained on that service; and (3) any record or other information pertaining to me with respect to that service. The terms used in this authorization are to be construed as broadly as possible, and the term "fiduciaries" includes an attorney-in-fact acting under a power of attorney document signed by me, a guardian or conservator appointed for me, a trustee of my revocable trust, and a personal representative (executor) of my estate.

This authorization is to be construed to be my lawful consent under the applicable laws (e.g. USA Laws - Electronic Communications Privacy Act of 1986, as amended; the Computer Fraud and Abuse Act of 1986, as amended); and any other applicable federal or state data privacy law or criminal law. This authorization is effective immediately. Unless this authorization is revoked by me in writing while I am competent, this authorization continues to be effective during any period that I am incapacitated and continues to be effective after my death.

Unless a person or entity has received actual notice that this authorization has been validly revoked by me, that person or entity receiving this authorization may act in reliance on the presumption that it is valid and unrevoked, and that person or entity is released and held harmless by me, my heirs, legal

representatives, successors, and assigns from any loss suffered or liability incurred for acting according to this authorization. A person or entity may accept a copy or facsimile of this original authorization as though it were an original document."

While the above may not address all boundary conditions, nevertheless it is good to start with in the absence of any relevant regulations and using prevailing provisions of laws and other operative mechanism.

6. Conclusion

With increased and enhanced use of digital channels for our daily life, it is only natural that the digital assets keep growing over the life of the individual. As we have seen above, account holders, service providers and designated fiduciaries face enormous challenges regarding management of digital assets. With growing ownership, value and significance of digital property, the need to resolve these problems is great. Hence, there is an urgent and dire need to bring in multifaceted and comprehensive legislation to address proper disposition of digital assets of individuals both through testamentary documents or proper state specified inheritance and succession laws. Until the legislatures take these or similar steps, account holders, fiduciaries, and service providers can work to minimize their respective uncertainty and risk by providing clear fiduciary powers, authority, and instructions regarding digital property in powers of attorney, wills, trusts, and stand-alone documents to support existing or future fiduciary appointments.

END NOTES:

[i] S. Balasubramanya, B.E.(NIE-Mysore), MTech.(IIT-Madras), MBL(NLSIU), PGD-CLCF(NLSIU), LLB(KSLU), PGD-IPRL(NLSIU), LLM(USC-USA), is at present a practicing advocate in Bengaluru and formerly Vice President & Chief Risk & Compliance Officer with M/S. Tata Consultancy Services Limited, Bengaluru

[ii] The Digital Death Conundrum: How Federal and State Laws Prevent Fiduciaries from Managing Digital Property JAMES D. LAMM, CHRISTINA L. KUNZ, DAMIEN A. RIEHL & PETER JOHN RADEMACHER – University of Miami Law Review 14-Feb-2014

[iii] Source: LLM Cyber Law Course Material – University of Southern California – Spring-2020

[iv] Social Media Will means a document that provides a testator's intent for managing digital assets