The ontology of digital asset after death: policy complexities, suggestions and critique of digital platforms

Yong Jin Park, Yoonmo Sang, Hoon Lee and S. Mo Jones-Jang

Abstract

Purpose – *The digitization of the life has brought complexities associated with addressing digital life after one's death. This paper aims to investigate the two related issues of the privacy and property of postlife digital assets.*

Design/methodology/approach – *The understanding of digital assets has not been fully unpacked largely due to the current policy complexities in accessing and obtaining digital assets at death. This paper calls critical attention to the importance of respecting user rights in digital environments that currently favor service providers' interests.*

Findings – *It is argued that there are ethical blind spots when protecting users' rights, given no ontological difference between a person's digital beings and physical existence. These derive from the restrictive corporate terms and ambiguous conditions drafted by digital service providers.*

Originality/value – *Fundamentally, the transition to the big data era, in which the collection, use and dissemination of digital activities became integral part of the ontology, poses new challenges to privacy and property rights after death.*

Keywords *Privacy, Data ethics, Digital remain, Privacy and property rights, Postlife digitalization, Data ethics*

Paper type *Conceptual paper*

Yong Jin Park is based at the School of Communications, Howard University, Washington, District of Columbia, USA. Yoonmo Sang is based at the Faculty of Arts and Design, University of Canberra, Canberra, Australia. Hoon Lee is based at the Department of Journalism and Communication, Kyung Hee University, Seoul, Republic of Korea. S. Mo Jones-Jang is based at the Department of Communication, Boston College, Chestnut Hill, Massachusetts, USA.

1. Introduction

The public debate on the digital management of one's assets after death has hardly commenced. The digitization of our life has brought far more complex new challenges. Our daily lives have increasingly revolved around the internet and algorithmic digital environment and we are now living in so-called the "big data" era in which we virtually leave traces of the entirety of our lives in digital form. When a person leaves behind digital assets, however, we do have a little clue about what would happen to those assets after death. The issue is more than the protection of monetary values, as it also concerns one's memories, dignities and more importantly, the respect over identities associated with life.

This paper dissects these challenges and explores the nature of societal responsibility in defining user rights to exercise control over digital traces and assets, such as social networking sites and e-mail accounts, beyond the point of death. The issues that we are raising are twofold:

1. Privacy; and
2. property rights of postlife digital assets.

These are intertwined issues, which will never be mutually exclusive, but we treat them as two separate issues for analytical purposes. The analysis undertaken in this paper

Received 10 April 2019
Revised 2 July 2019
25 August 2019
12 October 2019
Accepted 8 November 2019

proceeds as follows: First, we propose a new conceptual building block for the future discussion of digital assets by defining it and reviewing its various forms. Then, we explore the policy and ethical issues revolving around postlife digital assets – privacy and digital property – through a summary review of:

- existing examples in the USA; and
- regulatory responses so far.

This is followed by our proposition for an ethical framework entailing broad guidelines beyond the transferability of digital assets.

We argue that the ethical codification of digital integrity (Nissenbaum, 2004) will be the first efficient step toward enabling user autonomy. The nature of digital assets has not been unpacked largely due to the current complexities in accessing and obtaining digital assets at death. We critique that these, in part, derive from restrictive terms and ambiguous conditions drafted by digital service providers. Our fundamental focus here is on those regulatory contours, especially in the regulatory context of the USA, which perpetuate power asymmetries between a user and a commercial digital platform when exercising control over the ontology of one's existence via various forms of digital assets. To be clear, we are not proposing to strike a balance between account users and service providers, but instead we are casting a critical eye over emerging complications from the current status of market-based solutions offered by digital service providers. Thus, our goal is not to present a legal argument but to formulate an informed and ethical perspective that can serve as a basis on which a policy framework can be built. Accordingly, this paper strives to develop ethical stances that are not symmetrical but which favor user autonomy through which the individual control over digital asset and content is possible.

2. Ontology of digital asset: its significance and background

Laws and policies cannot keep pace with the speedy development of new technology (Neuman, 2016; Pool, 1983). The digitization of a person's life makes the disjuncture between policy and technology even greater. As a wide range of and a large portion of daily activities are increasingly algorithmized and performed via the internet, many day-to-day activities exist exclusively in digital form. According to Pew Research, as early as October 2015, 65 per cent of American adults used social networking sites (Perrin, 2015). In this context, the creation and distribution of digital content have become extremely fast and efficient. Another key feature of the digital age is that storing and retrieving information has been easier. Once created, digital assets can exist in perpetuity, with almost no or little additional cost of data retention.

The question of who accesses, owns and ultimately controls digital assets after death entails complicated policy challenges. As of now, no unified legal system governs digital assets at death. It is no surprise that current property, contract and probate laws do not properly address emerging issues and the contextual complications related to one's digital asset after death. Not to mention legal voids, market solutions and social norms governing this new social issue are also incipient, if not nonexistent. Consequently, it is unclear to what extent the perpetual remains of one's digital traces, properties and associated identities will affect the shaping of the digital sphere and its transformation (Öhman and Floridi, 2018).

The e-mails of historical figures, for instance, hold significant economic or historical value. Nevertheless, we are concerned with the mundane contexts of ordinary people in their daily engagement with digital technologies. Pictures, videos and various types of digital documents on social networking sites or cloud storage services hold deep sentimental value for lay people, even though the digital remains might be of no importance at all in terms of their transactional value. As Tarney (2012) put it, "Intangible value that individuals attach to today's written electronic communications can be fairly compared to the value they

formerly attached to things such as letters and pictures" (p. 775). As our life goes digital, many tangible assets including family photo albums, business documents and letters have been also supplanted by their digital counterparts. If anyone wants to fully address estate planning for one's assets, they need to understand what a digital asset after her/his death would be and to what extent the digital remains could become the property of an heir. Dosch and Boucher (2010) echoed this by saying, "the sentimental value of those heirlooms has not diminished, but an heir's ability to access them may be limited or restrained" (p. 10).

We argue that the issue at stake is more complex than estate planning or asset inheritance. First, it can concern more than tangible financial values because digital assets carry not only sentimental value but also intangible reputation or personal information of a content creator or user. Second, a narrow scope of legality debate alone, though relevant and valid as we spell out later in this article, misses the fundamental point of how digital technology entails newer contextual challenge to our own ontology, that is, our existence after death in digital forms. Furthermore, the future stake of digital asset cannot be reduced to just a matter of an heir/heiress and an owner/a content creator with concern over associated transferability. What are missing in the existing analyses are the critical roles that intermediaries such as Facebook, Google or Yahoo play in cementing a commercial condition. To say the least, amid a narrow technical focus on the transferability of digital assets, the significance of the issue has been misconstrued as defining a "correct" legal process of who has a "right" legal ownership or not of digital content.

2.1 Definition of digital asset

Currently, there exists no unified definition of what is a digital asset. With regards to the term "digital asset," Romano (2011) proposed the following definition: "[A] digital asset is digitally stored content or an online account owned by an individual" (p. 2). The concept of an asset is usually associated with property. However, given that there is no clear interpretation of an asset that is digitally formed, owned, managed and exercised, it is difficult to define it and grasp its complicated dimensions. In addition, established procedures of transferring assets that readily fit in the traditionally defined forms of physical property are not likely to be useful in disposing of digital assets.

Admitting the difficulty of defining a digital asset, Dosch and Boucher (2010) posited a definition which should include the following components:

- any online accounts; and
- any file stored on a person's computer or on a server.

Adopting this, we define different types of digital assets in the following ways. First, digital assets can include a wide range of online accounts. Here, online accounts can comprise numerous personal digital belongings associated with e-mails, social networking sites, photo-sharing sites and any online accounts that contain a user's private information and content. Arguably, virtual goods, such as in-game currency/bitcoins, items or avatars, can fall into this category. Second, digital assets can include files that are stored on an individual's personal computer or on a server of cloud services, such as Mozy, Google Plus or Dropbox. Digital pictures and documents saved on your personal computer, mobile/smartphones, wearables or a cloud service company's server are typical examples of digital content. Ebooks or digital sound recordings like iTunes songs also fall into this category.

Here, we add intangibles to the definition of a digital asset. The intangibles include one's digital identities, emotional as well as behavioral traces, psychographic profiles and cumulative knowledge about individuals. These, of course, can take the form of digital archives, curation, data libraries or databases. Note that they can be perhaps even more important assets than the prior two types because databases, for instance, serve as a basis

for continuous exploitation by commercial algorithms even after an individual's death. In other words, we believe that digital assets introduce serious ontological complications derived from the intangibility that defies finite characteristics of physical properties.

We summarize this classification in Figure 1. The quadrant of postlife x intangible asset, as circled, remains perhaps the most vulnerable area due to the lack of any policy protecting curated intangible assets after a person dies. To us, this dynamic offers an opportunity to:

- reexamine the practices of commercial digital platforms such as Facebook which are the dominant gatekeepers to digital lives of most people; and
- understand the inadequacies of current law based on narrow legalities of transferability among stakeholders, namely, a deceased person to another.

More importantly, by positing multiple dimensions of a digital asset, we lay the conceptual grounds on which to develop a policy framework supporting ethical data practices.

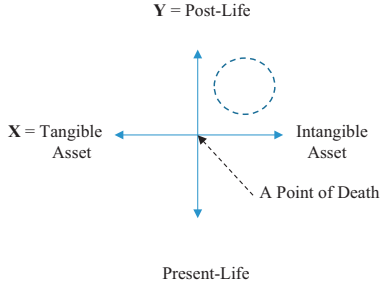
3. Complexities associated with digital asset

3.1 Privacy v. access

Until recently, one's privacy during life and after death has not been discussed by policymakers, scholars, civil society and the like (Wilkens, 2010). At a fundamental level, it can be said that the US regime regarding privacy does not have a long history, and its rules and regulations do not pay enough attention to recent technological developments, such as geolocation and mobile devices. Unlike European countries that value one's privacy, Americans have not been given the same level of protection to information. Privacy is not explicitly recognized in the US Constitution and Congress has passed no overarching law. For this reason, the privacy legislation landscape has been fragmented on a state-by-state basis (Park and Skoric, 2017; Park, 2011).

Not surprisingly, little policy work has been undertaken regarding the privacy of digital assets (and access by third parties) after death. Most recently, in 2012, the Obama administration issued a "Privacy Bill of Rights". Setting aside the fact that the Privacy Bill of Rights is a green policy paper with no enforceable mechanism,; it, at least in its principle, delineates consumers' right to exercise control over personal data, and six additional principles, such as "focused collection", which recognizes consumers' right to reasonable limits on the personal data that companies collect and retain. The issue of obtaining (either legitimate or unauthorized) access, or/and the extent of one's privacy right to personal data after death, however, was never under explicit consideration. In this regard, complexities in

Figure 1 Dimensions of digital asset



Notes: X axis = a degree of tangibility;
Y axis = a person's life

obtaining digital assets generated by a deceased user arise from privacy and confidentiality agreements to which service providers are legally obliged. To protect a user's right of privacy and confidentiality, digital service providers, e-mail and social network service providers, tend to draft restrictive terms of access. It is ironic that this restriction seems to be a *de facto* mechanism for digital platforms to shield themselves from potential lawsuits and, more importantly, these restrictions are usually used to thwart immediate access by family members.

A well-known story illustrating the complications of respecting privacy of a deceased family member's e-mail accounts goes back to 2005. John Ellsworth, a father of a dead marine, asked Yahoo to allow him to gain access to his deceased son's e-mail account to create memorial in his son's honor (Olsen, 2005). Yahoo refused until it was required to comply by a court order. This illustrates how unclear one's privacy online will be at the time of death, and how fuzzy the responsibilities that internet service providers hold are toward family members. Service providers usually have difficulty dealing with this type of disclosure request as it is an ethical conundrum. If service providers decline to release information, they are labeled as villains by people supporting the families. Conversely, if they give it away, they are chastised for violating their own privacy statements (Cha, 2005). In this context, it is not surprising to see that the ambiguity of data practices, especially with no guidance of unified codes of conduct, tends to leave the decision up to discretions of individual families (i.e. whether they will go to court).

Similarly, social networking sites in the USA have encountered difficulties generating an explicit policy of dealing with personal data, digital traces, as well as digital content such as personal postings or comments, which were made by those now dead. Facebook serves as an illustrative example. As early as 2009, Facebook implemented its policy of "memorializing" – that is, when a person dies, Facebook memorializes the deceased's account to protect his/her privacy. The key features of the "memorializing" function of Facebook are as follows:

- no one can log into a memorialized account;
- depending on the privacy settings of the account, friends can share memories on the memorialized timeline;
- content the person shared (example: photos, posts) stays on Facebook and is visible on Facebook to the audience it was shared with; and
- memorialized profiles don't appear in public spaces such as in suggestions for People You May Know, ads or birthday reminders.

Even though Facebook provides users with the option of removing a profile entirely, it does not allow family members to access the deceased's account to remove its content (Lowensohn, 2010). What matters here is whether social networking sites, such as Facebook, Twitter or Instagram, should have sole rights over what to do with a deceased user's account – this is still a controversial issue. In a fundamental sense, it is even more significant to note that Facebook policy, as it is now, is exclusively concerned about privacy in the sense of interpersonal (person-to-person) relationships. In other words, no purview of policy discussion is spelled about institutional appropriation – namely, how and under what purposes institutions will retain metadata such as personal behavioral traces.

Another popular social networking site, Twitter, has a more liberal policy than that of Facebook. Twitter allows the family members of a deceased person access to the deceased's account if survivors provide their contact information and relationship to the deceased user, the deceased's username, and a link to a public obituary or news article that proves the death. However, this policy, like that of Yahoo and Facebook, still does not consider situations where the intention of a deceased user may conflict with that of the surviving family members. Family members might want to delete all tweets of their loved

one, whereas the deceased person might want his/her Twitter stream archived or vice versa. There is also the possibility that the surviving family members have different opinions regarding the deceased's Twitter stream.

Common in these examples is that digital platforms perceive privacy in an extremely limited sense of interpersonal access to digital content. Subsequently, privacy is reduced to a binary matter of access or not – and this is codified in restrictive access terms. It creates a false impression that digital platforms function as nothing but a gatekeeper that "objectively" determines the disclosure of content to third parties (in this case, families, excluding data collection by institutional actors, such as advertisers).

3.2 Personal property issues

Notwithstanding some emotional or sentimental values linked to those of a loved one, digital assets left on social media such as Facebook can have a real tangible monetary value (Sherry, 2012). When it comes to content remaining on the deceased's social media accounts, one could argue that the assets should be considered property. Such a line of thought is difficult to ignore given that the digital assets of a loved one can hold personal, sentimental and financial value linked to the decedent's usage. According to the Internal Revenue Code, the gross estate of a decedent also refers to "the value at the time of [decedent's] death of all property, real or personal, tangible or intangible, wherever situated" (I.R.C. § 2031(a), 2006).

However, online service providers might well point to their contractual terms, possibly arguing that their users' digital assets should someday die with the termination of their service use. Depending on specific conditions, service providers sometimes declare ownership of accounts. Under most contracts between users and digital platforms or service providers, users have no legal rights (or very limited rights) to transfer access to digital assets along with their monetary values. For instance, Zynga Inc., one of the world's largest providers of social game services, enforces the rule that the following terms of use shall bind its users:

You do not own any Account that you create on our Services, including in our games, and your Account is not your property. Likewise, you do not own any Virtual Items that you obtained through our Services, regardless of whether you "earned" those Virtual Items or "purchased" them. Your account and any related Virtual Items are owned by Zynga. You are not allowed to sublicense, trade, sell, or attempt to sell Virtual Items for "real" money, or exchange Virtual Items for value of any kind outside of a game.

Different service providers often use their own languages, but in the similarly restrictive terms of a service contract, and the above-noted terms, used by Zynga, capture well the sheer difficulty faced by users when they claim their rights to digital content.

Here, it is critical to note that the most common way for digital platforms to enable users to access and use their service is a license between users and the service. It is quite likely that these contractual licenses impose serious limitations on a user's ability to not only transfer but also create value and claim the rights associated with digital assets even before death (Sang, 2017). In many cases, a user's digital assets take the form of writings, pictures and videos. Although a conceptual distinction between physical assets and intellectual property is necessary, a murky area emerges, as these digital assets can also be classified as intellectual property, that is, to say, even though intellectual property rights are both transferrable and descendible, the right to access and claim one's online account as her property dies with the user. Our point is that the continuance of user autonomy over digital content and assets can and should be possible even after death by the conditions set forth for a user from the outset of the use of services. This condition can be set to cover both the present and the future regarding the terms about content, assets and any related traces that an individual may leave behind.

The restrictive yet comprehensive nature of the Google's terms of service that governs Google Plus, Gmail, Google Drive and YouTube account illustrates our point:

When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make), communicate, publish, publicly perform, publicly display and distribute such content. This license continues even if you stop using our Services.

The comprehensive scope of licensing, enshrined in ambiguous terms, such as "worldwide" and "works better" and in a range of digitalization, such as "host" "modify" and "reproduce" is overwhelming. In addition, the termination of use, either by intention or by death, does not constitute the termination of the licensing agreement. Fundamentally, we are concerned about the limited extent of user autonomy over their digital content and asset is not simply lost at the point of one's death, but also exacerbated to a point that perpetual existence of digital content and associated personal data becomes vulnerable to continuous exploitation.

Similarly, the way in which commercial platform environments, such as massively multiplayer online role-playing games (MMORPGs), bind their users in ambiguous terms, raise questions about preexisting property principles. In fact, the creation of property in virtual worlds fundamentally challenges our understanding of the ownership of artifacts (or digital assets). One may think that private companies that have created and controlled virtual environments are the owner of artifacts within MMORPGs. An increasing number of internet users, however, have come to believe that the ownership of avatars and other artifacts they create within virtual worlds belongs to them. This increasing phenomenon among users of MMORPGs arguably requires a reconfiguration of the restrictive concept about property created by the users of MMORPG.

So far, the idea that existing intellectual property laws can be applied to virtual worlds has turned out to be not an easy task. Residents in second life, for instance, can buy land through linen-dollar bought with real money. However, it appears that users and second life as a platform both perceive digital asset as being equivalent to physical property; hence, confusion and conflict potentially arise when a user's life ends, but a digital life of property continues and often evolves into different derivatives. A second life avatar can be hacked at death, used and adapted by others.

Importantly, it is worth noting that the current legal framework does not have a unified understanding of what constitutes digital property (Mezei, 2018). The boundary, however, between the digital world and the real world is increasingly blurred, but there has been no change in the legal notion of property as it continues to be solely based on physical assets. Such a disjuncture adds to the complications associated with the control of digital assets after death, that is, there is complete silence about how the digital property (derivative or original) of a deceased user will be ever restored, exploited and retained. *De facto*, the absence of clarity in this regard means no prohibition on the action of digital service providers.

We emphasize the "digital" nature of properties that remain perpetual, with low additional cost of maintaining user content. As much as the privacy of digital assets is constructed as an interpersonal matter in commercial platforms, property issues have been understood as a contractual dispute (that is, between a user and another user or a provider) concerning the transfer of assets or inheritance at the time of death. Consequently, the contour of institutional practices has rarely been imagined beyond a custodian role in customer relationship management whereby service providers are reduced to a managerial role over potential disputes that happen to occur in their platforms.

3.3 Trend in policy development

Legislation for addressing the issue of digital assets is still in its infancy, although lawmakers and the courts are now increasingly recognizing the necessity of policy

remedies to this issue. A dominant view (Reeves, 2006) is that one unified approach is needed to avoid unnecessary expense and social confusion involved in accessing and controlling one's digital assets after death.

In this regard, noteworthy is a coordinated effort at the international sphere. The internet corporation for assigned names and numbers (ICANN), which is in charge of managing domain names and IP addresses, modified its policy to make domain names transferrable. This is arguably a step toward achieving legislative clarity to avoid confusion in domain transfer processes. This approach by ICANN deserves attention with regard to its applicability to digital asset problems. For instance, ICANN recognizes the possibility that instances of fraud and mistakes may occur. Therefore, it implements a predictable and cost-efficient dispute resolution process for such incidents. According to ICANN, the registry operator is entitled to cancel a transfer if it receives notice that there was a mistaken transfer or somehow did not follow the protocol. It can also do so upon receipt of a resolution by a proper authority or by a court order. This approach might turn out to be fruitful in addressing some of the problems related to digital assets, such as fraudulently obtained access after one's death.

Nevertheless, such remedies barely touch on the fundamental complexities of digital assets as we outlined earlier. We argue that there are at least two reasons for this. First, the transferability of assets does not resolve the issues regarding the continuous exploitation of one's digital intangibles. Related, the focus on the transferability of digital asset effectively presumes that the matter is confined between the two entities, namely:

1. those who used to own the asset originally; and
2. those who will have "legal" access to existing assets after death.

This is particularly problematic because it reduces the debate to the procedural matter of access alone, when, in fact, the complexities arise from privacy, property and one's postlife ontological existence, and the question of who has ultimate control over the formation of these rights. This remains true of the 2015 Uniform Fiduciary Access to Digital Assets Act (UFADAA) in the USA. Despite its potential, UFADAA focuses on the property aspects of digital assets and their access and transfer. The narrow scope of defining digital assets effectively not only excludes the privacy dimension of digital assets after life but also leaves the matter solely to interpersonal context, providing unfettered power to institutional actors (Banta, 2016; Meese *et al.*, 2015).

As a result, we foresee that:

- restrictive terms, which particularly limit users' autonomous creation and control of digital property; and
- ambiguous service conditions, which exacerbate the difficulty of defining one's private–public distinction of her/his digital identities, will remain to be *de facto* uniform solutions to postlife complexities.

Even the EU General Data Protection Regulation (GDPR), enacted as of May 2018, hardly raised the issue of postlife digital assets and potential complications that may bear on the future of user rights. Although GDPR's focus on user consent is a step forward to protecting privacy, its protection, as far as temporally concerned, is addressed only with the respect to the "past" traces of personal data and assets. To us, this reflects the inherently retrospective nature of legal remedies, which will be ineffective, especially because it assumes future complications can be best preventable through user consent articulated through the textual clarity of a law.

Fundamentally, we feel that the uniformity of law might lead to a singularity of solutions, only based on physical property and the tangible assets that are easily transferable to monetary value. The void in this line of logic is the extent to which users exercise autonomous control over digital assets, of which the future ontology poses not only legal complexities but also

ethical and societal dilemmas over the perpetual nature of digitalization beyond a point of one's biological death.

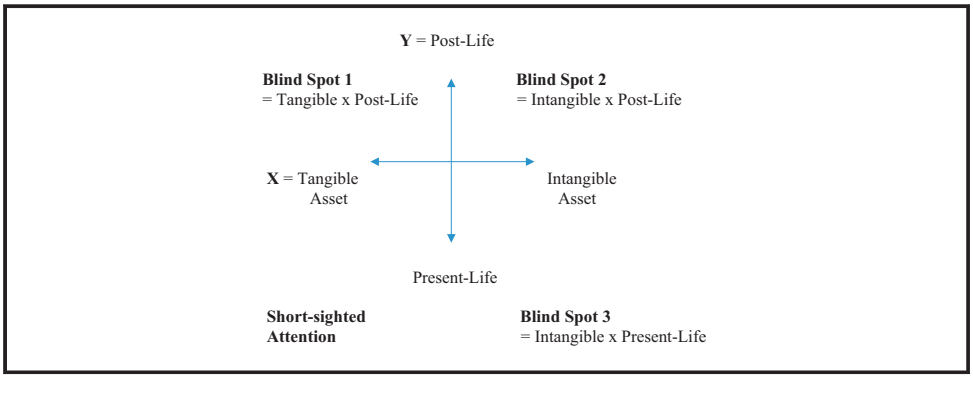
4. Ethical blind spots in digital asset

We are not arguing that it is in vain to search for a uniform law that guides the data practices of digital platform providers. Nor is it our contention that clarification of laws in textual detail will not matter to the point every new technology poses newer and more complicated challenges than originally perceived. Rather, what we are concerned with is the disjuncture between policy communities and digital service providers in their focus, and what we see as the ethical conundrum that urgently needs a clear demarcation of social responsibilities. Put it differently, our compiled summary review of practices and suggested remedies as discussed above illustrate ethnical blind spots in understanding the issue of digital assets after death.

Notice that there are three blind spots in Figure 2, to which no attention has been paid by service providers or policymakers. These three spots contrast with one spot (the quadrant labeled "Short-sighted Attention") in which tangible forms of digital asset are easily identifiable in terms of their monetary value before one dies. It is no surprise that all corporate measures – restrictive or ambiguous – concentrate on what will happen to those tangible assets and their future prospect. Even Facebook's statement about their accounts after death, which describes clear rules in some detail, remains silent about the ownership of personal data and its contents, and how knowledge about the personal histories of its deceased users will be maintained. In a similar vein, second life's permissible property policy avoids any clarity in terms of protecting privacy or potentially revealing details related to virtual property.

Aside from no clear monetary interest being at stake, we attribute these blind spots to the lack of understandings among policymakers over the ontological lifespan of digital data. The algorithmic presence of the dead, with distributed personhood in digital forms, defies current legal premises (Meese *et al.*, 2015). For instance, the succession law cannot recognize this complexity, and thus it remains vulnerable given the nature of digital assets in its perpetual traceability from which derivatives can easily emerge. In the end, it costs almost nothing or very little to replicate the original content – whether the biological life of the content creator has ended. Because the understanding of policymakers remains ensconced in the traditional succession laws of physical assets, they cannot imagine the scope of derivative digital assets and associated harm. This effectively defines ethical blind spots of the intangibles.

Figure 2 Ethical blind spots of digital asset



We find it perplexing to witness the blunt assertion that law by nature cannot cover future matters. Certainly, the idea, applicable to the transferability of property rights, helps reduce the legal complexity to a manageable scope in the present moment. Nonetheless, it will also fail to fit the lifespan of digital data that is clearly not in sync with the lifespan of the stakeholder or the person who generates personal data and associated properties. The nature of digitalization is at the core of this matter, connecting privacy and property issues. Under current conditions, any algorithmic exploitation (Lustig *et al.*, 2016) of postlife digital assets can hardly violate the person's rights (and the dignity of respecting the scope and nature of derivative use in that matter) – as far as they are anonymized at the aggregate level. Setting aside ethical points that it may violate one's integrity after death, the harm is not exclusively individual (as in individual litigation), but at the aggregate level without clear boundaries within which a user's rights can be established about derivatives of digital asset and its trace.

The apparent fact is that for digital service providers, such as Facebook, Google/G-mail and second life, there is simply no incentive to respond to any market demand because actual users who may have claimed a violation of their rights have already died. Market pressure exists only in the rare circumstances in which family members complain about losing their rights to the deceased's account and its monetization. Even in these instances, the short-sighted attention to family inheritance transferability muzzles the fact that the ethical responsibility may also belong with the deceased and not family members. It is like we are leaving the decision of disposing the tombs to a graveyard steward (or commercial custodian) simply because there is no family member to visit to claim what is to be monetized inside the tomb. This point resonates with Lambert *et al.* (2018), who argue that digital platforms are in the business of databasing digital lives as policymakers up to now have largely failed to recognize these blind spots (Öhman and Floridi, 2017; Park and Shin, 2020).

5. Toward an ethical model of integrity

Several lessons can be learned. First, it is becoming increasingly clear that "one size fits all" approaches would not be effective in covering different dimensions of digital assets. These are dimensional problems. Second, related to the first point, the ontology of postlife digital assets far exceeds the narrow scope of property transferability between the deceased and family members. Third, the rights to postlife digital assets remain entrenched in a self-regulatory market-based solution with protection left up to the discretion of service providers, whereas a jumble of civil suits on a tort basis often determines the extent to which one exercises control over digital assets. Fourth and most fundamentally, we see blind spots where market forces undermine the digital afterlife of every user to a marginalized status as appropriate attention is only given when challenged by immediate family members. The absence of such integrity, we suspect, derives from the fact that the major stakeholders (i.e. the deceased account user) do not exist to protest or voice their concern.

In the end, what we advocate is the ethical standards that guide service providers to pay critical attention to the importance of respecting the rights of users in the marketplace after death. It is critical to note that we are not proposing a uniform law. Neither is it our intention to lay out all the technical details for digital service providers. Instead, we suggest broad ethical principles on which to build data practices in respective domains related to postlife digital assets. We see this as being the first step to be done at the high level of ethical principles within which to develop more detailed but flexible policies that are not bound to specific technologies or platforms. We base our proposition on Nissenbaum's (2004) "contextual integrity." This notion, originally developed for better construing complexities of privacy issues, helps us view the contextual appropriateness of personal information flow and/or use in evaluating a violation of one's rights to privacy. In other words, the flow of information makes us constantly adjust our expectations of privacy, which is bound to differ

context-to-context or time-to-time. This is different from treating privacy as being static in one point in time, but instead opens up the possibility that:

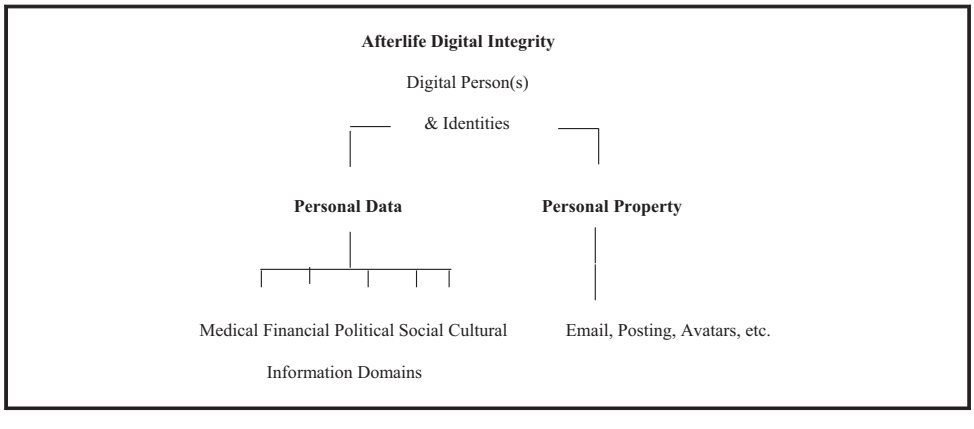
- societal expectations can be adjusted to new digital environments; and
- the rights to privacy, as well as digital property, should not die with the end of one's biological life.

Accordingly, we strive to develop an ethical stance that can corroborate contextually-appropriate expectations for postlife digital assets – we term this as "afterlife digital integrity." Fundamental to this is the shift away from a fixture in the present moment of a person's life to a contextual integrity by which the temporal disjuncture between asset holders/owners and her digital traces/assets does not necessarily mean a point of ontological separation. This is to recognize how new forms of perpetual digital traces and assets emerged to allow for the positioning of one's identities even after death. Our premise is similar to Solove's (2004) assertion of "a digital person" where we constantly create our digital beings via fragmented activities in numerous information domains that are constantly compiling information about us (Figure 3).

In this sense, there is no ontological difference between our digital beings – in the forms of postlife personal data and asset – and a sense of our identities, that is, who we are. What is integral to this transformation is how to maintain and respect the "contextual integrity" of postlife identities. Clearly, at a personal level, maintaining her/his afterlife reputation matters, but as we have argued, these are also societal responsibilities and concern in defining what is a contextually appropriate flow of digital traces, properties and associated identities. We base this position on the ethical premise that one's ontology (and the exercise of its control) is a basic citizen's right, rather than the one that is subject to the restrictive terms governed by digital service providers.

We suggest the following. First, the ethical principle, as in government-sanctioned industrial guidelines, should be explicitly codified to the extent a digital asset after life will be treated with respect. The idea is that there is the need to formulate a comprehensive regulatory framework that defines and limits the scope of commercial exploitation of digital traces, assets and related contents of the deceased. This proposition is based on two related points. The first point is procedural, namely, that standardized provisions and requirements, as in the EU GDPR, must emerge from harmonized international efforts. These provisions should have a power to enact requirements as a regulatory mandate, not as a symbolic directive that has no binding effect. We see a considerable potential for including relevant amendments related to post-life digital assets as part of updating GDPR.

Figure 3 Digital identities and afterlife digital integrity



The second point is substantive. The protection clause should clearly include a provision that any privacy and property rights to digital assets remain intact even after death and they will be free from commercial uses, altercation, inclusion in databases that may be commercialized or used for advertising purposes, or possessive takeover with no prior consent. It is important to distinguish the protection of digital assets from corporate policies governing data retention by which collected personal information expires after a certain period of time. Nor is it that we advocate a simple deletion of the deceased's accounts as equivalent to the respect over the digital afterlife. The ethical aim that we are advocating is to treat postlife digital assets with no less respect than during the time of the person's active use so that subsequent existences (even in their potential transfer) are not incompatible with the original purposes and/or contexts of the person's activities at the time of data collection.

6. Conclusion

Although we agree that complicated technical issues may prevent policymakers from laying out all of the details in practical terms, other complex remedies, such as the erasure of digital histories (e.g. the right to be forgotten in the EU), has, in fact, been codified, implemented and enacted. Assuming all consequences of policy suggestions and unintended burdens on service providers cannot be scrutinized, the claim that no policy action is possible because they are unknowable in the future is a red herring. In this regard, our work identified several alarming trends. First, we found the highly restrictive service terms in most of major commercial digital platforms that disfavor user autonomy. Second, despite the legislative efforts at the US state-level, the evolving policy excludes those intangibles such as behavioral data traces. Finally, these limits in corporate terms and legislative efforts reflect the failure to recognize ethical blind spots. There is no ontological difference between a person's digital beings and physical existence as we argue that digital protection for privacy and property should not disappear with one's death. Fundamentally, what we propose is that the importance of postlife digital asset cannot be reduced to the exchange values under the marketplace rationale. The world is constantly creating a vast reservoir of petabytes of digital information and will be soon filled up with traces of digital assets previously owned by and created by the deceased. Setting aside the emergent industry sector of digital curation that specializes in the postlife information, there will be only a few dominant platform players that can take advantage of exponential growth of digital traces Google, Facebook and Yahoo will be best positioned to exploit the digital assets of the deceased to generate new sources of profits. It is not surprising to suggest that this corporate power to constantly monetize such traces will help sustain their online dominance. Potentially, the stakes are even larger. Consider the government, as a major holder and curator of digital assets previously owned by the deceased can harness electronic databases and rely on commercial firms such as Amazon to develop the provision of public services and inform policy-making across all levels of government.

In fact, we have successful policy precedents that codified ethical values and societal responsibilities concerning the i.e. opt-in for donation) in the event of death by checking a box in a driver's license, is another example of how government-sanctioned codes of conduct regarding the future of one's body can serve a societal good.

In addressing such multiple complexities involving postlife digital asset, future works are warranted. On the user side, it is imperative to explore how the public begins to understand postlife-related issues, perceives and remains concerned about their digital rights. This type of user-related works will help guide policymakers to better devise policies that are not incongruent with the public demand. On the supply side, we will also need to document the perceptions (and potential attitude changes over time) among policymakers and industry

leaders, because their perceptions will have direct consequences on the future regulatory directions. Not imagined in the current policies and practices by commercial platforms is the creation of the condition in which people have an explicit option to choose how digital assets, potential creation of a property and traces via the use of particular websites will be handled after death. This will be a step forward to empower users themselves to identify contextual appropriateness in an explicitly codified condition. We see, not only a necessity but also a plausibility of our proposed model to be substantiated based on broad ethical norms and values. One might find it surprising to realize that the vitality of digital transformation of public sphere will depend upon the protection of the afterlife, as well as the current moment of our digital being.

References

Banta, N. (2016), "Property interests in digital assets: the rise of digital feudalism", *Cardozo Law Review Review*, Vol. 38, p. 1099.

Cha, A. (2005), "After death, a struggle for their digital memories", The Washington Post. February 3.

Dosch, N.J. and Boucher, J.W. (2010), "E-legacy: who inherits your digital assets?", *Wisconsin Lawyer*, Vol. 83 No. 12.

Lambert, A., Nansen, B. and Arnold, M. (2018), "Algorithmic memorial videos: contextualising automated curation", *Memory Studies*, Vol. 11 No. 2, pp. 156-171.

Lowensohn, J. (2010), "Twitter's new deceased-user policy vs. Facebook's", CNET News.

Lustig, C., Pine, K., Nardi, B., Irani, L., Lee, M.K., Nafus, D. and Sandvig, C. (2016), "Algorithmic authority: the ethics, politics, and economics of algorithms that interpret, decide, and manage", in *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, *ACM*, pp. 1057-1062.

Meese, J., Nansen, B., Kohn, T., Arnold, M. and Gibbs, M. (2015), "Posthumous personhood and the affordances of digital media", *Mortality*, Vol. 20 No. 4, pp. 408-420.

Mezei, P. (2018), *Copyright Exhaustion: Law and Policy in the United States and the European Union*, Cambridge University Press, New York, NY.

Neuman, W.R. (2016), *The Digital Difference*, Harvard University Press, Cambridge, MA.

Nissenbaum, H. (2004), "Privacy as contextual integrity", *Washington Law Review*, Vol. 79, p. 119.

Öhman, C. and Floridi, L. (2017), "The policital economy of death in the age of information: a critical approach to the digital afterlife industry", *Minds and Machines*, Vol. 27 No. 4, pp. 639-662.

Öhman, C. and Floridi, L. (2018), "An ethical framework for the digital afterlife industry", *Nature Human Behaviour*, Vol. 2 No. 5, p. 318.

Olsen, S. (2005), "Yahoo release e-mail of deceased marine", CNET News.

Park, Y.J. (2011), "Provision of Internet privacy and market conditions: an empirical analysis", *Telecommunications Policy*, Vol. 35 No. 7, pp. 650-662.

Park, Y.J. and Shin, D. (2020), "Contextualizing privacy on health-related use of information technology", *Computers in Human Behavior*, Vol. 105, p. 106204.

Park, Y.J. and Skoric, M. (2017), "Personalized ad in your google glass? Wearable technology, hands off data collection, and new policy imperative", *Journal of Business Ethics*, Vol. 142 No. 1, pp. 71-82.

Perrin, A. (2015), "Social media usage: 2005-2015", in *Pew Research Center*, available at: www.pewinternet.org/2015/10/08/social-networking-usage-2005-2015/

Pool, I. D S. (1983), *Technologies of Freedom*, Harvard University Press, Cambridge, MA.

Reeves, S. (2006), "Estate planning in the digital age", Forbes.

Romano, J. (2011), *A Working Definition of Digital Assets*, *Digital Estate Resource*, available at: www.digitalestateresource.com/

Sang, Y. (2017), "The politics of ebooks", *International Journal of Media and Cultural Politics*, Vol. 13 No. 3, pp. 211-228.

Sherry, K. (2012), "What happens to our facebook accounts when we die-probate versus policy and the fate of social-media assets postmortem", *Pepperdine Law Review*, Vol. 40, p. 185.

Solove, D.J. (2004), *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, New York, NY.

Tarney, T.G, (2012), "A call for legislation to permit the transfer of digital assets at death", *Capital University Law Review*, Vol. 40, pp. 773-802.

Wilkens, M. (2010), "Privacy and security during life, access after death: are they mutually exclusive", *Hastings Law Journal*, Vol. 62, p. 1037.

Corresponding author

Yong Jin Park can be contacted at: yongjinp@hotmail.com