How to cite this article:

Mirshekari, A., Ghasemi, R., & Fattahi, A. (2020). Digital accounts after death: A case study of Iranian law. *UUM Journal of Legal Studies*, *11*(2), 153-182. https://doi.org/10.32890/uumjls.11.2.2020.7505

DIGITAL ACCOUNTS AFTER DEATH: A CASE STUDY OF IRANIAN LAW

[1]Abbas Mirshekari, [2]Ramin Ghasemi & [3]Alireza Fattahi

[1] Department of Private Law, University of Tehran, Tehran, Iran
[2]Tehran University of Science and Culture, Iran

[3]University of Judicial Sciences and Administrative Services, Tehran, Iran

[1]Corresponding author: mirshekariabbas1@ut.ac.ir

Received: 11/12/2020 Revised: 11/6/2020 Accepted: 18/6/2020 Published: 31/7/2020

ABSTRACT

In recent times, as cyberspace is being widely used, virtually everyone has a digital account. This naturally entails its own legal issues. Undoubtedly, one of the main issues is what fate awaits the account and its content upon the account holder's death? This issue has been neglected not only by the primary creators of digital accounts but also by many legal systems in the world, including Iran. To answer this question, we first need to distinguish between the account and the information contained therein. The account belongs to the company that creates and allows the user to only use it. Hence, upon the death of the account holder, the account will be lost but the information will remain because it was created by account holder and thus belongs to him/her. However, does this mean that the information will be inherited by the user's heir(s) after his/her death? Can the user exercise his/her right to transfer account content to a devisee through a testament? In comparing digital information with corporeal property, some commentators believe that this kind of information will be inherited like corporeal property. This is a wrong deduction because corporeal property is capable of disclosing the privacy of the owner and third parties much less than in cyberspace.

This paper aims to show what happens to a digital account after its user passes away by examining the subject using the content analysis method in various legal systems in the world, especially in Iran through a case study. The information required was collected from law books, articles, doctrines, case laws, and relevant laws and regulations of different countries. To protect the privacy interests of the deceased and others, it is concluded that financially valuable information published by the account holder before death can be transferred to his/her successor(s). As a rule, information that may violate privacy through disclosure should be removed. However, given that this information may be a valuable source in the future to know about the present, legislators are suggested to make digital information available to the public for a long time, which may no longer lead to the invasion of the decedent's privacy.

Keyword: *Privacy, property, inheritance, testament, information.*

INTRODUCTION

Not so long ago, people would take photos with simple cameras and put the printed photos in albums or write letters to each other and keep the letters for a long time. Since these photos and letters are tangible, there is no particular problem with their status after the owner's death. The owner himself/herself would usually decide on the matter through a testament; otherwise, his/her heirs would assume ownership of the photographs, letters, and other legacies of the deceased inasmuch as they own the other goods of the deceased (Carrel & Romano, 2011). The abundance of such objects was not large enough to attract the attention of the legal system. Today, people can easily set up accounts in cyberspace and save information or, send and receive messages. The account holder will naturally manage his/her own account as long as he/she is living. Here the question arises, what happens following the account holder's death? Will the account owner or the information contained therein be inherited or will the account expire when the account holder dies? This is not merely a theoretical question as it has also been raised in the case-law of other countries. For example, when Ellsworth died, his family in America decided to create a memorial for their son using his e-mails and photos. Consequently, they asked Yahoo for

the copies of the emails. However, Yahoo considered the account non-transferable by resorting to the contract terms accepted by the user. It also claimed that "publishing the emails" violated the privacy of those who sent or received the messages. After litigation by his father, a court in Michigan ordered Yahoo to provide copies of the contents of all emails without giving them access to the account of the deceased (Conner, 2011; Truong, 2009). There are two points about accepting the possibility of transferring digital information to successors. First, in the past, a photo or letter was kept in a personal album or library. The owner of the album or a personal library was naturally the owner of the photos and letters. However, nowadays, the opportunity to create digital accounts is provided by companies. Therefore, we own the content of these accounts, though the tools employed for its maintenance and publishing cannot be ignored. Thus, the interests of the company must be considered when judging the posthumous status of these accounts (Dickens, 2007). Particularly, the heirs will need a password to access the account, which is almost impossible if not assisted by the company (Beyer, 2012). Besides, User Privacy is an integral part of digital accounts. The information contained in the account is considered private and part of user privacy; therefore, the user may not want to transfer his/her account ownership after death (Watkins, 2014). Consequently, "accepting the legal transfer of ownership of digital accounts to the successors" conflicts with user privacy**.**

On the other hand, undeniably, there is no difference between the characteristics of digital information and old pictures/letters. They are similar in nature, therefore why should these two lead to two separate judgments? Moreover, the account contents can serve as a valuable memorial for survivors, so why should they be deprived of them (Cha, 2005)? Sometimes the account has a financial value (e.g., those used for downloading music or books), or the user would use his/her account for financial purposes (Banta, 2014). Depriving an heir of this financial opportunity is not rational (Watkins, 2014). These accounts sometimes serve as a good source of information that can help administer a deceased person's estate or answer questions raised by the survivors (Cummings, 2014). In 2011, for example, a 15-year-old boy committed suicide in America, leaving various "questions about the causes" of his death unanswered. His parents thought that their son's Facebook page could provide answers to

their questions, though Facebook refused to help them due to the likelihood of privacy violations (Watkins, 2014). The same approach has been followed in other cases (McCullagh, 2012).

This article will first examine the concept of account and digital information, followed by an overview of the approaches employed by legislators and the administrative procedures used by digital account providers. Then, we will discuss what happens to digital information following the user's death. Finally, the discussion will be concluded after exploring the Iranian legal system as a case study.

MATERIALS AND METHODS

Concept of Digital Account and Information

A digital account is an electronic tool that allows one to create, send, receive, store, and display information in cyberspace (Carroll, 2012; Mazzone, 2013). This feature allows the user to send or receive letters, pictures, songs, and any other information. There are different instances of a digital account (Conway, 2017). Some have attempted to divide it into four categories: financial, business, personal, and social (Cahn, 2011; Carroll, 2011); however, it would seem to be of little use to categorize them, given the increasing growth of such instances and the creation of new accounts with new functions (Beyer, 2013). Therefore, it seems that one should look at the instances instead of focusing on categorization.

Emails are one of the widespread and comprehensive examples of digital accounts that allow users to send or receive a digital letter. Social networks are also an emerging example of digital accounts. These networks (e.g., Facebook) which emerged in the past decade, allow people to create their accounts and upload their information. Unlike emails where information is only accessible to the email owner and his/her contacts, information on social networks is visible to more people (depending on user preferences) (Conner, 2011). Mobile networks, such as Instagram and Telegram, are other examples. Furthermore, some accounts have been created for financial purposes. Accounts that allow users to buy from online markets fall into this category e.g. e-Bay, PayPal and Amazon. Some

sites also enable users to upload content so that it is later accessible by the user himself/herself or others.

Digital accounts, although economically viable, do not include bank accounts and digital wallets where cryptocurrency is stored in the definition of digital accounts. Cryptocurrency, like the financial credit of bank accounts, replaces money and can be used for any transaction (Raskin, 2013). In addition, it has the ability to trade itself but the financial credit in digital accounts has certain consumption, so they have to be spent to buy certain site products.

According to this definition, the account mentioned contributes to information transfer. Accordingly, we can distinguish between an account and its content (Perrone, 2012). Account content is any information stored therein (Conway, 2017). The provider's claim to the account could be accepted since the user is only allowed to use the account, a nontransferable license (Haworth, 2014). Since "everyone owns the product of their legitimate business" (Article 46 of the Constitution of Iran), the company cannot stake out digital information (Truong, 2009). To justify this distinction, the status of these companies can be compared with that of the renter of a warehouse (Conner, 2011) or a carter (Darrow, 2008). When you rent a warehouse from A or ask him/her to carry a commodity to a specific destination, does A own the property? Of course, not. You are still the owner of the goods and A cannot claim ownership. Accordingly, the provider will not own photos or letters saved in your account (Darrow, 2007; Mazzone, 2012). It can be stated that the information received is owned by the person (Perrone, 2012; Darrow, 2007; Conner, 2011). In this regard, email providers such as Yahoo, Google, Microsoft, and Dropbox and some social networks such as Twitter have explicitly declared that the content belongs to the account owner (Dropbox, 2019; Google [APA], n.d.; Microsoft, 2019; Verizon Media, 2020; Twitter, n.d.).

Legislation System Approach

Legislation systems often fail to determine the posthumous status of accounts (Watkins, 2014; Tarney, 2012). Indeed, many questions have arisen following the emergence of technology, which has remained unanswered by legal and legislation systems (Varnado, 2014). As an

example, in Iran, the creation and utilization of digital accounts have also grown rapidly and according to a survey conducted in February 2016, currently, 59.7% of people over the age of 12 have at least one social network account (Aghaei, 2018). This is because Iranian legal literature has paid less attention to this issue, whereas jurists in other countries, especially the United States, have acted on this issue quite considerately (Conway, 2017). This may be either due to the fact that most account service providers are of American nationality or the age of the Iranian users. According to the above survey, 81% of young adults (the youngest age group: 18-29 years) are currently active on social networks, which forms the highest percentage. This issue has hardly been raised for this age range (Aghaei, 2018).

As an exception, it should be noted that seven states of America have enacted laws on this subject, with Connecticut as the first state. Under this law, which came into force in 2005, email providers must give a copy of the messages sent to and received by the user's heir. Besides, Rhode Island (Cummings, 2014) and Indiana (Hollon, 2013) followed this approach. However, these rules only apply to emails and cannot be applied to other digital accounts (List of state laws and proposals regarding fiduciary access to digital property during incapacity or after death, 2013).

In some states, such as Nevada, only heirs are allowed to terminate an account without having access to the account content (Perrone, 2012). Other states have also extended the heir's authority over other digital accounts. For example, under an act approved by Oklahoma House in 2010, an estate executor or administrator has the authority to control and decide on operating or terminating the activity of a deceased person's accounts on social networks, blogs, messengers, or emails (Lamm, 2012). The same is true for Idaho (Hollon, 2013). The last state to enact this code was Delaware. Under the state legislature approved in 2014, heirs, families, and estate administrators of the deceased will have full control over the content and the deceased's digital accounts, including email and social media, just as they have control over tangible documents (Gaied, 2016). Other states are still in the process of drafting legislation (Pinch, 2015).

Current Procedure used by Account Providers

Account providers do not use a single approach, but a rather different approach depending on their discretion. These different approaches

are like a spectrum, which can be divided into two sides: minimum and maximum. Regarding the minimum approach, the only option available after the user's death is to terminate accounts without managing them, and even less, to access the account content. Twitter falls into this category. It allows the user's close relatives to request account termination after his/her death by providing specific evidence, including the user's death certificate (Deceased User, n.d.). According to Yahoo's e-mail account creation rules, a person's account will be terminated upon his/her death (Verizon Media, 2020).

Therefore, only the user himself/herself will be allowed to use it. After the user's death, his/her close relatives can send a required certificate to Yahoo. Yahoo will also terminate the account without leaving anything out of the account content (Cummings, 2014; Perrone, 2012). Thus, this approach does not specify what should happen to an account. Users will most likely want to terminate it, but not in all cases. Thus, they should be provided with other options.

In the maximum approach, survivors are given more authority. Accordingly, some companies such as, Microsoft provides the user's heirs and representatives with access to the account content (Microsoft answer, 2012).

Google employs a similar approach, except that it will allow heirs to access the account content in rare cases but does not specify what exactly a rare case is (Google account help, n.d.). In practice, Google has rarely exercised this option (Perrone, 2012).

In the latest version of the policies regarding the accounts of deceased users, Facebook enables users to determine the fate of their postmortem account before death. He or she may decide to terminate the account in the event of death or remain in the situation at the time of death without having the opportunity to sign in (Conner, 2011; Edwards, 2013). Likewise, he/she can allow his/her survivor(s) to download the account content. Thus, these options do not enable the survivor(s) to get a username and password to access the account itself. In practice, however, this regulation is ambiguous as the terms and conditions of their application are unclear (McCallig, 2014). Besides, these authorizations are not contained in contract terms, but

rather in the so-called auxiliary section. Therefore, it can be doubted whether it is binding on either side (Edwards, 2013).

Interestingly, Iranian companies providing digital account services, i.e. companies of Iranian nationality and with a majority of Iranian users, have not stipulated, in their terms, any rules on the status of an account after a user's death. Among these sites include Picofile as a file upload site, and Soroush and Eitaa as messengers. The same applies to email provider sites such as Mail.iran and Vatanmail.

RESULTS

There are four factors to consider when analyzing the possibility of inheriting a digital account. First, we can look at the issue from a property rights perspective. Here, we can determine whether an account can be considered as property or not. Accepting an account as a property reinforces the possibility of inheriting it. Moreover, it should not be overlooked that the account is the result of a bilateral contract, one side being the company that creates the account and the other being a person who uses it. Thus, the terms of the contract between them must be taken into consideration. In addition to the above two factors, the user's privacy rights should also be taken into account. Since the account contains the user's personal information, his/her privacy rights must be protected. Finally, public interest cannot be ignored, such as, the interests of heirs, companies, users, and the social conflict with one another. It is worth noting that some commentators have considered the user's testamentary intention as a solution (Watkins, 2014). However, digital accounts are usually neglected when writing a testament (Conner, 2011). Moreover, it will be reasonable to accept it if the information contained in the digital account is solely about the user himself/herself, yet it is known that third-party information may also exist. Therefore, if the user has permitted others to access his/her account in his/her testament, the privacy of third parties may be endangered. The risk in particular increases if the account belongs to a physician, psychologist, or a lawyer (Obesnshain, 2015). Hence, it does not seem rational to hope that the user will write his/her will. Nevertheless, this section attempts to examine the conflict of interests mentioned using different approaches.

DISCUSSION

Property Law Approach

This approach treats the digital account content as property (Kutler, 2011; Mazzone, 2012; Hopkins, 2013; Atwater, 2006). Consequently, like all other property, the digital account will be inherited by heirs as well. According to this approach, in a well-known case, i.e., Ellsworth's v. Yahoo, the judge sentenced the latter to provide evidence against the claimant to access their deceased child's account. In the context of this sentence, the content of the digital account is compared to real property (Chu, 2015; Schneider, 2013). Can all digital accounts be considered property? Can a poem shared on a Facebook page or an image on Instagram be considered property with financial value? To answer this question, some deny the financial value of digital information and refuse to consider it property (Chu, 2015; Shah, 2012; Carroll & John, Tyler G. Tarney, 2011 & 2012). Others argue that the financial value is not determinative of its status as property (Beyer & Griffin, 2011). Rather, as long as an object is valuable to its owner, it must be regarded as property. Contrary to what has been said (Hopkins, 2013), undoubtedly, the value of account information is different: some with financial value and some with only an emotional aspect (Conway, 2017). Therefore, not all of them can be considered as property; however, that does not mean digital information is not one's property. Personal photos and letters may also be of no financial value, but there is no doubt that they are part of a person's property and are inherited after death (Varnado, 2014). Thus, since digital information is regarded as part of the user's assets, they must be inherited after his/her death.

Nevertheless, the disclosure of a digital account may translate to user privacy violations as it may contain private information. Just imagine, A sent an email to B in which he spoke about his feelings for B, something that A did not want others to know. Then one day, A passes away. Now, if the deceased person's heir gets access to the account and reveals the contents of the email, it would definitely go against the deceased's will and violates his privacy.

It may be argued that possessing private information is not specific to digital property because some real estate contains the same

information as well. In this regard, to explain the possibility of the inheritance of digital accounts, some cite letters, pictures, and diaries. Similar to digital property, besides violating one's privacy such property may contain personal information that can be transferred to heirs. On the other hand, nobody believes in the impossibility of inheriting such property (DeRoss, Pa. 2002; Jonathan J. Darrow & Ferrera, 2007). This indicates that privacy cannot seriously impede the transfer of property to heirs. Accordingly, digital property should also be inherited; however, some argue that digital accounts are not comparable to corporeal assets in terms of the volume of information (Chu, 2015). However, this feature also does not seem to be specific to digital property. Others believe that there is no specific requirement to access real property. There is no need for encryption to access such property; thus, one may assume that such property will be released after death. However, digital property is not similarly accessed. You will need a username and password to access such property, thus the user writes in such a way that others cannot have access to it (Varnado, 2014). The whole gist is in doubt as well; you should only imagine that a person's diary or personal photo album would be in a safe. What seems most likely to indicate the inaccuracy of comparing digital information with information contained in corporeal property is that digital information contains a bilateral or multilateral relationship, thus information may be disclosed as a result of the heir's access to the user's account information. Besides, digital information can be rapidly shared and reproduced, while corporeal property cannot. In light of this feature, there is a greater fear of privacy violations. Therefore, privacy concerns should be considered separately.

Contract Law Approach

When creating a digital account, a letter of agreement is placed ahead of the person and he/she is asked to declare his/her consent to its terms by clicking on a specific option. Before this announcement, no account will be created. Therefore, this agreement letter is a good platform for the provider to declare its volition for the postmortem account status and to obtain the individual's consent (Carroll & Romano, 2011; Banta, 2014). These agreements involve several modes for determining the postmortem account status. Some of them allow for the transfer of account information upon the user's death

(IHG, 2017; Marriott, 2020). Some companies, such as Microsoft, Twitter, and Yahoo, explicitly introduce non-transferable accounts in their agreement (Microsoft, 2019; Twitter, n.d.; Verizon Media, 2020). The validity of these agreements can be doubted for two reasons. First, because the agreement is an adhesion contract. One side of the deal with more power in the negotiation predetermines its terms and the other side that seeks to create an account has no choice but to accept or reject it. Therefore, he/she declares his/her agreement with the least thought (Conway & Grattan, 2017). If he/she admits, it is impossible to bargain, even being unaware of these terms. Some studies show that only about two out of every 1,000 people in the US read the terms of these agreements (Varnado, 2014). It is not clear whether those who read the contract understand the exact meaning of its terms. If yes, they will not be able to change the terms even if they want to (Roy, 2011). Thus, some believe that conditions likely stipulated in the postmortem account status in this agreement cannot be validated. They actually believe that the terms of these contracts should be ignored (Darrow, 2007; Dickens, 2007). Others do not judge in absolute terms and decide according to whether or not to get one's consent. They maintained that these agreements are of two types: click-wrap and browse-wrap (Preston & McCann, 2011).

Regarding the former, once the agreement contents are displayed, the user is asked to express his/her consent by clicking on a certain option. If it is not clicked, then the user will not be allowed to create an account (Facebook, 2019; Instagram, 2018; Linkedin, 2020). Concerning this agreement, the user is required to read the terms of the contract to be allowed to create an account and then express his/her consent by clicking on the "Agree" or "Yes" button below the agreement.

Regarding the latter, however, the terms of the agreement are not presented to the user in the first place. Instead, the user can usually view them through a specific link by clicking on it, which will take the user to another page where the agreement is posted. Unlike the click-wrap agreement, this method does not oblige the user to click on a button before creating an account. Therefore, the user is not asked to do anything to show his/her satisfaction (Kutler, 2011). Some commentators only validate the first type in light of this difference. They noted that conditions are valid only if they have

been communicated to the person and that he/she has given consent (Banta, 2014). Some courts also follow this belief. For example, in *Ajemian v. Yahoo! Inc.* (2013) the court held that it could not establish whether the contract was displayed on a person's computer screen or that the audience had reasonably accepted it because they had no place to declare their acceptance. This procedure was repeated in other cases (*Groff v. America Online*, 1998*; Specht v. Netscape Communications Corp*, 2002).

Instead of emphasizing intention and consent, some will focus on the impossibility of negotiating for making changes to the terms. The user can only declare his/her acceptance or rejection without being allowed to change the terms of the contract (Chu, 2015). Accordingly, they believe that the contract in question cannot be validated. However, in a famous case, the US Supreme Court had stated that the mere negotiation or non-negotiation does not determine the invalidity of adhesion contracts; however, whether this agreement is unfair in both form and content should be taken into consideration (*Carnival cruise lines, Inc. v. Shute*, 1991; Dickens, 2007; Hetcher, 2008).

The other objection is associated with the content of these contracts. In US Law, as an imperative rule related to public policy, the property should be transferred to an heir after the owner's death. Therefore, a contract that prevents postmortem property transfer is against inheritance rules and this is void. Consequently, some render this condition as invalid (Banta, 2014).

Personality Law Approach (Privacy)

In defending themselves against access requests to deceased users' accounts, companies mainly resort to a contract whereby they must protect users' privacy (Wilkens, 2011). Why do companies always suspect unauthorized access and information used in disclosure, insist on such privacy, and stand against the disclosure of the deceased user's account information (Debatin, 2009; Gross, 2005)?. Some believe that these companies are mainly concerned about the time and cost they will have to spend on sharing account information with successors rather than being worried about user privacy (Ray, 2013). Others believe that these companies want to assure their users

that their postmortem accounts will be protected from any access by resorting to privacy. This is because their dignity will be questioned and their earnings will be reduced if it is revealed that they have shared information with others (Tyler G. Tarney, 2012; Conner, 2011). Apart from this speculation, the companies' propensity to respect privacy arises from their legal obligations (Wilkens, 2011; Zainal Amin & Zuryati, 2018).

Moreover, the Electronic Communications Privacy Act of 1986 requires the protection of personal privacy in electronic communications. Therefore, the disclosure of account information can be regarded as a breach of these rules (Eleanor Laise, 2013; Gaied, 2016).

Some courts decide based on these rules. For example, (In re Request for Order Requiring Facebook, Inc. to Produce Documents and Things, 2012), when Sahar Daftary committed suicide, her parents sought access to her Facebook account. Nonetheless, according to citations and references to the rules mentioned, in protecting the user's privacy, a court held in 2012 announced that Facebook was not required to disclose account content to her heirs.

However, some asked whether the privacy of the deceased was protected? There is no consensus in answering this question. According to one of the common law principles, personal rights die with the person (actio personalis moritur cum persona), yet property rights survive and are handled by a decedent's executor (Wilson & Jones, 2007; Harbinja, 2013). Accordingly, in the U.S., the termination of privacy rights at death has been accepted in two old cases (*Shafer v. Grimes*, 1867; *Schuyler v. Curtis*, 1895). Refer to *Reed v. Real Detective Publ'g Co.*, 1945; *Kelly v. Johnson Publ'g Co.*, 1958; *Nelson v. Gass,* 1912 and *Abernathy v. Thornton*, 1955 to view the same procedure.

The American Restatement (second) of Torts also states that privacy rights end with the user's death so you cannot litigate post-mortem privacy violations (Hannes, 2008). The same is widely accepted in the academic literature of this country (Leibowitz, 2013; Kutler, 2011; Conner, 2011; Jonathan Bick, 2005). As previously mentioned, the right to privacy according to the constitutional law belongs only

to the living and a dead body is not a person (*Swickard v. Wayne Cty. Med. Exam'r*, 1991; *Infante v. Dignan*, 2011).

By following this belief, some commentators justify access to the deceased's account. They believe that when a user dies, the main concern should be about successors' rights rather than the user's privacy (Perrone, 2012). As stated in some cases, "life belongs to living creatures and should be controlled by them, not by the dead" (*Atlantic Richfield Co. v. Whiting Oil and Gas Corp.*, 2014). This belief is justified by the fact that a privacy breach is meaningful when the dead are unaware and not capable of suffering (Ray M. Madoff, 2010; Feinberg, 1984).

Notwithstanding, awareness is a condition for claiming compensation rather than incurring losses. If Mr. A converts Mr. B's property or harms his reputation while Mr B is unaware of these, has Mr B not been harmed? Certainly, Mr. B was harmed because whether Mr. B knows it or not, his property has been converted or his reputation damaged (Levenbook, 1984, Feinberg, 1987, Mirshakari, 2017). Therefore, some legal doctrines prescribe that the damage will be done regardless of our experience and understanding (Feinberg, 1980; Winter, 2010).

People do not commonly believe in expired privacy at death (Buitelaar, 2017) as there is a greater tendency in civil-law countries to recognize the duration of postmortem personality rights. Hence, the heir is allowed to litigate the violated rights of the dead (Harbinja, 2013).

For example, in Germany, Article one of the Constitution requires the protection of personality rights, which has been applied in German case law. In Mephisto and Marlene Dietrich cases, the courts upheld both the economic and non-economic aspects of the deceased person's personality rights. It is argued that humiliating or defaming a person upon his/her death is against the spirit of the Constitution. Accordingly, death does not put an end to the responsibility of the government to protect its citizens' personality (Ronsberg, 2017).

Even if it can be claimed that privacy ends with death, it is very difficult to accept this belief about information published in

cyberspace (Chu, 2015). This is due to the almost perpetual and proliferative nature of the information published in cyberspace. The US Supreme Court has reaffirmed the above belief and declared that digital information requires more privacy protection because of their quantitative and qualitative nature (*Riley v. California*, 2014; Gaied, 2016). Postmortem privacy protection is also more consistent with the will of the individuals themselves. Typically, individuals tend to maintain their privacy in postmortem cyberspace as well (Hollon, 2013). According to a survey in 2007, 70% of Americans wanted their private online communications to remain private after death (Obesnshain, 2015). Also, the following evidence can be deduced this will. Whether people's passwords on their digital accounts, or whether some digital accounts are private and require the permission of their owners to view information contained therein; all these imply users' will or intention to protect their privacy (Varnado, 2014; Haworth, 2014). The evidence suggests that users usually do not want anyone to have access to their accounts. The law should also respect the users' will. It should be remembered that people using digital accounts store their personal information, send private messages to others, or receive such messages; these messages may be presented in such a way that the users are not willing to allow their nearest relatives to access them, as it affects their reputation (Atwater, 2006). Therefore, posthumous transfer of information must be prevented because of the possibility of users' privacy violations.

Society Interest Approach

In discussing the status of the digital account after death, one should not forget the interests of society: destroying the digital account and information after the user's death is not only detrimental to the successors but also to society since digital information can be a valuable resource for presenting the status of the present society to future generations. In fact, future generations can gain valuable information about the current generation and their way of life by using digital accounts. For this reason, it is anticipated that future historians will write the history of this age based on the information contained in the digital accounts. As of today's historians, if they had access to the letters of ordinary people in centuries past, they would be better able to write the history of that era. For example, the recently discovered three hundred years old unopened letters

in the Netherlands which helped historians to understand the social situation of the people then (Kennedy, 2015). It seems that future historians should not be deprived of an important source of information (Mazzone, 2012). This is probably why the US Library of Congress is currently archiving all public tweets because it is a good source for the next generation to understand the meaning of life in the 21st century (Kutler, 2011).

Accordingly, it is suggested that the contents of the user account be made public after the death of the user and, of course, after a reasonable time when the privacy concerns is no longer present. This group found this solution for the benefit of science and history so that future generations can easily understand our way of life (Banta, 2016).

Digital Accounts After Death in the Iranian Legal System

This section specifically investigates the fate of digital accounts after the user's death in the Iranian legal system. To do so, the subject will be analyzed based on inheritance and testament using Iranian sources, including laws, customs, doctrines, theories, general principles of law, and Islamic jurisprudence, which has played a significant role in shaping the legal concepts of the Iranian legal system. For example, according to Article 167 of the Constitution of the Islamic Republic of Iran, authentic jurisprudential fatwas should be referenced by judges when a matter is either not clearly specified or defectively stipulated, or has been dealt with briefly and may involve a contradiction in the law.

The Iranian legal system divides legal institutions into promissory and possessory testaments (Article 825 of the Civil Law Act 1928). A promissory testament obliges an executor to fulfill a specific task ordered by the testator, while a possessory testament orders the transfer of property like inheritance (Article 826 of Civil Law). Accordingly, the fourfold approach will be discussed in the case of a possessory testament.

It should be noted that it is possible to enforce a promissory testament for certain digital accounts. Consequently, an executor is entitled in all directions to create a memory after the user's death, decide on the

financial content, e.g., selling, donating, sending to another account, or managing the account (especially financial functions) to make a profit following the user's death. Thus, whether a promissory testament function can be applied to digital accounts and its related information will be analyzed for contract law, personality law, and society interests.

Property Law Approach

For property law, digital accounts and its related information can be evaluated from two aspects: proprietary nature/worth and ownership (capability of being acquired). From the proprietary nature perspective, it should be noted that Imamieh jurisprudence has witnessed a lot of ebbs and flows regarding the definition of property. The related notions can be divided into two sections: traditional and modern. The traditional view on property in jurisprudence involves the notions put forth by a group of jurists who only consider corporeal objects as properties (Haeri, 2002). Nevertheless, advances in human life and the emergence of valuable credit phenomena outside the scope of the above definition have revealed the inefficiency of the traditional definitions for "properties" to the public. Afterward, jurists accurately considered the customary meaning of properties such as any item that can satisfy the needs of human beings is regarded as a property nowadays (Mohaghegh Damad, 2003; Tousi, 1967; Gharavi Isfahani, 2001). For other jurists, however, items appealing to people are considered as property (Al-Khoei, 1992; Hakim Al- Tabatabaei, 2011). Legal experts believe that an item is a property if it possesses an economic value (Emami, 2015; Safaei, 2012; Katouzian, 2013). That is to say, the property is appealing to others and they are willing to pay for it.

Ownership is the relationship between a person and his/her legally acknowledged property and he/she has the legal right to benefit from the possible interests of that property (Emami, 2015). Verily, he/she will be able to own the property following the establishment of such a relationship. Thus, both the owner and the property must meet specific conditions. For instance, the owner must have the capacity to own or possess the property and the property must be capable of being owned according to Sharia and the law. In other words, the property must not be illegitimate or belong to the public

as these types of properties cannot be owned by private individuals. Moreover, the property must be acquired by the owner through one or more of the "ownership means" stipulated in Article 140 of the Civil Law (e.g. restoration of wastelands, occupancy, contracts, commitments, preemption, and inheritance).

It should be noted that "value has been associated with the public" in Iranian law, as noted by Dr. Katouzian (2013). What establishes a property is social norms or customs. The contents of digital accounts are certainly considered to have economic value for the public, meaning that people are willing to pay for them (e.g. purchasing and selling of Instagram accounts, Telegram channels, and some online games for instance, the Clash of Clans). Arguably, such deals are not common and have not yet been widely accepted by members of society. Nonetheless, it should not be overlooked that proprietary worth does not entail market popularity (Sadeghi, 2016) and there is no need for monetary assessment to consider them as property. For example, certain people are willing to sell and buy old photos, memorable letters, and family mementos that are considered property.

An important question is raised about the possibility of ownership: "Which of the means stipulated in Article 140 of Civil Law can be the basis for a user's ownership claim to account content, assuming that it can be considered property?"

To answer this question, account contents need to be distinguished according to how they were acquired. Verily, a user can acquire digital information through three distinct means. The first is the situation in which the user has purchased information (e.g., books, movies, and music) or has acquired it through a possessory testament, requiring it to be classified into contracts and commitments. The second is by way of inheritance when the user has inherited the content. Or, if the user himself/herself has acquired them or has contributed to creating them (e.g. when writing an email, sharing a post on an Instagram account, or using an account on an online gaming platform to reach a certain level), which is considered valuable to the public. Since others are willing to pay to acquire the account, it seems not irrational to refer to the notion of "occupancy" as a means of acquiring ownership of the content. This is true, in particular, given the non-exclusivity of

occupancy examples provided in the law, which is capable of being generalized to digital properties, just as this notion is established regarding the means of acquiring intellectual property (Habia and Hussein Zadeh, 2014).

In conclusion, Iranian law has attached financial, emotional, historical, social, and economic values to the content of virtual accounts deemed as property of the society. This is a property where the capability of being owned is respected and ownership claim to it has been legitimized by the law. In case of a user's death, such a property can be transferred to his/her devisee if he/she has a legally valid possessory testament; otherwise, it will be inherited by his/her heirs.

Contract Law Approach

Regarding contract law, according to what has been discussed, a contract between a user and a company can be considered as an adhesion contract. Such contracts are characterized in the Iranian legal system by the necessity of their subject matter, higher bargaining power and exclusivity by the drafting party, and unequal conditions for the drafting party and against the signing party in their clauses (Ghafi, 2004), irrespective of the various definitions and interpretations provided by different legal experts on them (Katouzian, 2015; Shahidi, 2017). In Iranian law, adhesion contracts are not yet fully integrated into the legislative system. Furthermore, they are principally considered valid unless a party to the contract has abused the needs of the other and exerted his/her desired stipulations. This assumption considers abusing the needs of a party as an instance of duress and recommends the application of the rules on the defects of volition (Ja'fari, 1993; Katouzian, 1997). This is because there is no difference if the means of duress is created by the binding party or by external circumstances and social/natural events when it is fulfilled. It is necessary to avoid the consequences of duress rather than its underlying causes. Therefore, if the binding party poses a threat by taking advantage of the current circumstances, duress can materialize if the binding party has not contributed to the realization of an emergency (Katouzian, 1997). Hence, the possibility of boilerplate contracts between a company and a user being signed under duress can be investigated.

Additionally, following Imamieh jurisprudence, the rules and regulations provided in Iranian law on the legal institution of inheritance are peremptory as they are related to public order and familial expediency. Moreover, all contracts that prevent heirs from inheriting the said properties are considered unenforceable according to Article 975 of the Civil Law (Katouzian, 2008). Obviously, similar to the U.S. legal system, the Iranian legal system annuls all contracts inhibiting the transfer of properties following the devisor's death.

It should not be forgotten that inheritance is a right that belongs to heirs while testament belongs to the said property. In other words, inheritance prescribes that the possession is out of the testator's volition and any opposing contract that somewhat limit the rights of heirs would be inevitably invalidated. However, a testament depends on individual volition like contracts as in Article 959 of the Civil Law which allows people to drop their property-related rights in minor cases (Shahidi, 2017). Thus, there is no obstacle in dropping the right of testate to special property from the owner.

Consequently, the contract between the user and the provider may entail the stipulation of a condition regarding the non-transferability or non-accessibility of the content following the user's death. In this case, such a condition will be null and void for heirs but valid for the devisee and executor.

Personality Law Approach

Allowing heirs, devisees, and executors to access the content of digital accounts may raise concerns about the privacy of the deceased user or other users that have communicated with the deceased's account.

In line with the deceased user's privacy, it is crucial to examine the postmortem privacy in Iranian law.

From the perspective of the author, the stand on privacy duration and postmortem privacy rights are prioritized when studying the personal rights of the deceased in Iranian law. This is because a deceased person receives the same respect as the living in Islamic jurisprudence, e.g. "the sanctity of a deceased person is similar to that of a living one" (Kulayni, 1987). This indicates the importance of the personal rights of the deceased in the Islamic legal system..

Furthermore, in statutory law, the desecration of the deceased is criminalized under Article 727 of the Islamic Penal Code, Act 2013. Accordingly, "when a person intentionally commits a crime against or desecrates a deceased person, he/she shall be sentenced to 31–74 lashes of ta'zir flogging of the sixth degree besides having to pay wergild." Furthermore, in Article 222 of the Hodud section, necrophilia is considered the same as unlawful sexual intercourse (zina), indicating the special importance given to the rights of the deceased by the legislator.

Therefore, the Iranian legal system does not commonly believe in the termination of privacy rights at death as it is not in line with the principles of the Iranian legal and jurisprudential frameworks.

It can be stated that by authorizing the executor or devisee to access his/her account, the user has actually express his/her implied consent to allow his/her privacy to be violated, given the volitional nature of a testament. Notwithstanding, even if the deceased user's privacy is ignored given the reciprocity of information transfer between cyberspace users, what about the privacy of other users who have communicated with him/her? It would definitely be impossible to obtain consent from all of them. Hence, easy access to the content of the deceased person's account that could result in a privacy breach of the account holder and other users should not be allowed.

Interests of Society

From the societal point of view, there is no doubt about the various aspects of social, economic, and historical interests for the current and future generations. Keeping accounts with commercial and economic applications active by successors will be conducive to our economy as most of them provide opportunities for economic growth and development thanks to their economic benefits to society. Concerning other accounts, to ensure the interests of future generations, the Iranian legal system has imposed no restrictions on the dissemination of account contents after a certain amount of time when there are no concerns over owners' privacy violations. For instance, a similar solution has been suggested for intellectual property in Article 109 of the Bill on Comprehensive Protection of Intellectual Property Rights and Related Publication Rights, in which people are allowed to utilize work after the expiration of the legal protection time frame. In other words, once the expiration of the creator's rights protection time frame has expired, society

can exploit the work (Mohammadi & Sharghi, 2015). Given the relative similarities, it seems that a similar position can be taken for digital accounts (e.g., upon the expiration of a specific time frame). Therefore, from the societal point of view, there are no longer any concerns over the violation of the deceased person's privacy and the account and/or its content which can be shared with the public.

CONCLUSION

The posthumous fate of user accounts and the information contained therein should not be left to the whims of account providers because they usually impose a unilateral will on users so as to fulfill their own best interests. Thus, the legislator should make a decision in this regard by legislation (passing certain laws) (Banta, 2016). To submit a proposal to the legislator, we first need to know who owns the account and it looks like it is owned by the provider and the user is only permitted to use it. Thus, the account will expire once the user dies. However, this is not the case for digital information. Since information has been made by the user himself/herself, the ownership of the user can be justified. There are three scenarios for determining the fate of the information at death:

The first scenario is to keep the account active and have its activity managed by the heir, yet this conflicts with the provider's ownership claim to the account itself. Likewise, keeping the account active can mean that messages are sent and received by the deceased person, though he/she may not have consented to this (Conner, 2011).

The second scenario is to have the account expired, meaning that the provider will close it as soon as the user dies. However, this may practically lead to the violated user's ownership claim to information. Besides, this information is of economic value or newsworthy to society.

The most appropriate scenario seems to be accepting the transfer of ownership of information from the user to the heir, yet requiring some modifications. Indeed, a given right shall definitely not be transferred to the deceased person's successors if it is too dependent on his/her personality such that the two cannot be separated (Ansari, 2006; Hosseini Shirazi, 2006). Now, how much is a user's right to digital information, depending on the deceased person's personality? It does not appear to be an absolute answer to this question. Rather,

it should be judged regarding the nature of the information contained in the account. From the authors' point of view, assuming that digital information has mere financial value (such as an image of a person taking a picture and posting it on his/her Instagram) or is associated with his/her finances (such as installment loan payment information available in the user's email), the person's right to such information does not depend on his/her personality. Therefore, he/she can hand over his/her destiny to a devisee or an executor in the form of a testament or transfer them to his/her heirs (in the absence of a testament). Nevertheless, assuming that the digital information is personal; then its disclosure may violate the privacy of the user or third parties. The transfer of such information through inheritance is not widely accepted; instead, there is a tendency to eliminate or expose it to the public long after the death of the user. Hence, it seems that the court should appoint an impartial (unbiased) supervisor to decide the fate of such information according to the content by conducting a full-scale inquiry (Brubaker, Dombrowski, 2014). Apparently, the rights of all involved in the matter can be respected by terminating the account, immediately transfer financial information to the successor, and publicly disclose or delay other information after a certain time. This involves protecting the deceased user's privacy and supporting the rights of his/her successors in transferring financial information, as well as respecting public interest, particularly the right to know of the future generations.

The authors recommend retaining this information so that they can be used in the future. In this case, the information contained in digital accounts will be inherited by future generations, and not just the next generation.

ACKNOWLEDGEMENTS

This research received no specific grant from any funding agency.

REFERENCES

Abernathy v. Thornton, 83 So. 2d 235, 263 Ala. 496 (1955).
Aghaei, P. (2018). The Most Popular Messengers among Iranians. Retrieved from https://www.isna.ir/news/97072815126/

Ajemian v. Yahoo!, Inc., 83 Mass.App.Ct. 565, 987 N.E.2d 604 (App.Ct. 2013).

Al-Khoei, S. A. (1992). Mesbah Al-Feghaheh. Beirut: Dar Al-Hoda.

Ansari, M. (2006). The book of Al-Makaseb. World congress of commemoration of Sheikh Azam Ansari.

Arco v. Whiting oil & gas crop, 320 p.3d 1179, 2014 c.o. 16 (Colo. 2014).

Atwater, J. (2006). Who owns e-mail-do you have the right to decide the disposition of your private digital life? *Utah L. Rev*., 397.

Ayyub, Z. A. (2020). Right of online informational privacy of children in Malaysia: A statutory perspective. *UUM Journal of Legal Studies*, *9*, 221-241.

Banta, N. M. (2014). Inherit the cloud: The role of private contracts in distributing or deleting digital assets at death. *Fordham L. Rev*., *83*, 799.

Banta, N. M. (2016). Death and privacy in the digital age. *NCL Rev*., *94*, 928-990.

Beyer, G. W., & Cahn, N. (2011). When you pass on, don't leave the passwords behind: Planning for digital assets. *Prob. & Prop*., *26*, 40-65.

Beyer, G. W., & Cahn, N. (2013). Digital planning: The future of elder law. *Naela Journal*, *9*, 135.

Brubaker, J. R., Dombrowski, L. S., Gilbert, A. M., Kusumakaulika, N., & Hayes, G. R. (2014, April). Stewarding a legacy: Responsibilities and relationships in the management of postmortem data. In Proceedings of the *SIGCHI Conference on Human Factors in Computing Systems* (pp. 4157-4180).

Buitelaar, J. C. (2017). Post-mortem privacy and informational self-determination. *Ethics and Information Technology*, *19*(2), 129-142.

Cahn, N. (2011). Postmortem Life On-line. *Prob. & Prop*., *25*, 36-56.

Carroll, E., & Romano, J. (2010). *Your digital afterlife: When Facebook, Flickr, and Twitter are your estate, what's your legacy*? *39*, 1-25.

Cha, A. E. (2005). After death, a struggle for their digital memories. *The Washington Post*. Retrieved from http://www.washingtonpost. Com/wp-dyn/articles/a58836-2005feb2. html

Chu, N. (2015). *Protecting privacy after death*. Nw. J. Tech. & Intell. Prop., 13, ii. 45-65.

Conner, J. (2010). Digital life after death: The issue of planning for a person's digital assets after death. Est. *Plan. & Cmty. Prop. LJ*, *3*, 301-354.

Conway, H., & Grattan, S. (2017). The 'new' new property: Dealing with digital assets on death. *Modern Studies in Property Law*, *9*, 99-115.

Cummings, R. G. (2014). The case against access to decedents' e-mail: Password protection as an exercise of the right to destroy. *Minn. JL Sci. & Tech*., *15*, 898-912.

Darrow, J. J., & Ferrera, G. R. (2006). Who owns a decedent's e-mails: Inheritable probate assets or property of the network? *NYUJ Legis. & Pub. Pol'y*, *10*, 281-291.

Darrow, J. J., & Ferrera, G. R. (2008). Email is forever... or is it? *Journal of Internet Law*, *11*, 1-15.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, *15*(1), 83-108.

Deceased User. (n.d.). *How to contact Twitter about a deceased family member's account*? Retrieved from https://help.twitter.com/en/rules-and-policies/contact-twitter-about-a-deceased-family-members-account

Dickens, R. L. (2007). Finding common ground in the world of electronic contracts: The consistency of legal reasoning in clickwrap cases. Marq. *Intell. Prop. L. Rev*., *11*, 379-400.

Dropbox. (2019, December 17). *Dropbox privacy policy*. Retrieved from https://www.dropbox.com/privacy

Edwards, L., & Harbina, E. (2013). Protecting post-mortem privacy: Reconsidering the privacy interests of the deceased in a digital world. *Cardozo Arts & Ent. LJ*, *32*, 103-150.

Emami, S. H. (2015). *Civil Law*, Vol 1. Tehran: Islamieh.

Carroll, E. (2012). *Digital assets: A clearer definition, digital estate.* Retrieved from http://commcns.org/1 3ijil5

Facebook. (2019, July 31). *Terms of service*. Retrieved from https://facebook.com/terms.php

Feinberg, J. (1984). *Harm to Others* (Vol. 1). Oxford University Press on Demand.

Feinberg, J. (1987). The moral limits of the criminal law, harm to others (Vol. 1). *University Press Scholarship Online*, pp.80-100.

Feinberg, J. (1980). *Harm and self-interest, in rights, justice, and the bounds of liberty: Essays in social philosophy*, pp.40-56.

Ghafi, H. (2004). The nature and validity of adhesion contracts. *Islamic Law Journal*, *1*(2), 61-88.

Gaied, M. (2016). Data after death: An examination into heirs' access to a decedent's private online account. *Suffolk UL Rev*., *49*, 281-300.

Google. (n.d.). *Google Terms of Service*. https://policies.google.com/terms?hl=en-US

Google account help. (n.d.). *Submit a request regarding a deceased user's account*. https://support.google.com/accounts/troubleshooter/6357590?visit_id=637241259060739618-4278674119&hl=en&rd=2

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. In Proceedings of the *2005 ACM workshop on privacy in the electronic society*. Retrieved from http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook1.pdf

Habiba, S., & Hosseinzadeh, M. (2014). The process of acquiring the ownership of intellectual property. *Comparative Law Studies*, *5*(1), 335-357.

Haeri, Hosseini, K. (2002). *Contracts jurisprudence.* Qom: The assembly of Islamic belief.

Hakim Al- Tabatabai, S. M. (2011). *Jurisprudential manner.* Qom: 22 Bahman.

Harbinja, E. (2013). Does the EU data protection regime protect post-mortem privacy and what could be the potential alternatives? *SCRIPTed*, *10*, 19-38.

Haworth, S. D. (2014). Laying your online self to rest: Evaluating the uniform fiduciary access to digital assets act. *U. Miami L. Rev*., *68*, 535, 536-570.

Hetcher, S. (2008). User-generated content and the future of copyright: Part two-agreements between users and mega-sites. *Santa Clara Computer & High Tech*. *LJ*, *24*, 829-843.

Hollon, J. R. (2013). Tweets from the grave: Social media life after death. Ky. *LJ*, *102*, 1031-1050.

Hopkins, J. P. (2013). Afterlife in the cloud: Managing a digital estate. Hastings Sci. & Tech. *LJ, 5*, 209-246.

Hosseini Shirazi, M. (2006). *Eysal Al-Taleb ela Al-makaseb*. Institute of Library of Alami.

IHG, (2017, April 5). *Terms of use*. Retrieved from https://www.ihg.com/content/us/en/customer-care/tc.html

Infante v. Dignan, 782 F. Supp. 2d 32 (W.D.N.Y. 2011).
Instagram. (2018, April 19). *Terms of Use*. Retrieved from https://help.instagram.com/581066165581870
Isfahani Gharavi, S. M. H. (2001). *Glosses to Makaseb*, vol *5*. Qom: Qom Seminary pub.
Jafari Langroodi, M. J. (1993). *Law Terminology.* Ganj Danesh Publications, p.6.
Kalven Jr, H. (1966). Privacy in tort law--were Warren and Brandeis wrong? *Law & Contemp. Probs*., *31*, 326-350.
Katoozian, N. (1997). *General rules of contracts*. Publishing Company in collaboration with Bahman Borna, P. 2.
Katoozian, N. (2003). *Will*. University of Tehran, p. 1.
Katoozian, N. (2008). *Civil law in the current legal order*. Tehran: Tehran University.
Katoozian, N. (2016). *Elementary course in civil law: Juridical Acts*. Tehran: Enteshar Stock Company.
Katoozian, N. (2013). Elementary course in civil law: Properties and ownership. Tehran: Mizan. Vol. 2.
Kelly v. Johnson Publishing Co., 160 Cal. App. 2d 718, 325 P.2d 659 (Ct. App. 1958).
Kulayni, M. (1987). *Al-Kafi*. Vo1. 7. Tehran: Islamieh Library.
Kutler, N. (2011). Protecting your online you: A new approach to handling your online persona after death. Berkeley Tech. *LJ*, *26*, 1641-1651.
Lastowka, F. G., & Hunter, D. (2004). The laws of the virtual worlds. *Calif. L. Rev*., *92*, 50-75.
Leibowitz, C. (2013). A right to be spared unhappiness: Images of death and the expansion of the relational right of privacy. Cardozo Arts & Ent. *LJ*, *32*, 347-350.
Levenbook, B. B. (1984). Harming someone after his death. *Ethics*, *94*(3), 400-427.
Linkedin. (2020, March 26). *Linkedin service terms*. Retrieved from https://www.linkedin.com/legal/l/service-terms
List of States Laws and Proposals Regarding Fiduciary Access to Digital Property During Incapacity or After Death. (2013, August 30). *Digital passing*. Retrieved from http://www.Digitalpassing.com/2013/08/30/august-2013-list-state-laws-proposals-fiduciary-Access-Digital-property-incapacity-death/
Kennedy, M. Undelivered letters shed light on 17th century society. *Guardian*. Retrieved from http://www.theguardian.com/world /2015/nov/ 08/ undelivered-letters-17th-century-dutchsociety? CMP=fbgu.

Majlesi, M. B. (1406 AH). *Malaz al-Akhyar fi Fahm Tahzib al-Akhbar*. Public Library of Ayatollah Marashi, P.1.

Marriott, (2020, March). *Loyalty program terms & conditions*. Retrieved from https://www.marriott.com/loyalty/terms/default.mi

Mazzone, J. (2013). The right to die online. *Journal of Internet Law*, *16*(9), 13-35.

McCallig, D. (2014). Facebook after death: An evolving policy in a social network. *International Journal of Law and Information Technology*, *22*(2), 107-140.¶

McCullagh, D. *Facebook fights for deceased beauty queen's privacy*. Retrieved from http://news.cnet.com/8301 -135783 -57518086-38/facebook-fights-for-deceased-beauty-queens-privacy/

McCullough, C. (2016). Unconscionability as a coherent legal concept. *U. Pa. L. Rev*., *164*, 779-795.

Microsoft. (2019, July 1). *Microsoft Services Agreement*. https://www.microsoft.com/en-us/servicesagreement/

Microsoft answer. (2012, March 15). *My family member died recently, what do I need to do access their Microsoft account*? Retrieved from: https//answer.microsoft.com/en-us/outlook%20_com/forum/oaccount-omyinfo/my-family-member-died-recentlyis-in-coma-what-do/308cedce-5444-4185-82e8-0623ecc1d3d6

Mirshakari, A. (2014). *Practical Treatise on Civil Liability, Publication*, p. 3.

Madoff, R. D. (2010). *Immortality and the law: The rising power of the American dead*. Yale University Press, *11*, 6-7.

Mohaghegh Damad, M. (2003). *Jurisprudential Rules*, Vol,1. Tehran: Islamic Science Publishing Center.

Mohammadi, P., & Sharghi, M. (2015). An attitude to the nature of intellectual creatures after belonging to public lands. *Comparative Law Studies*, *6* (1).

Nelson v. Gass, 27 N.D. 357, 146 N.W. 537 (1914).

Obesnshain, M., & Leftwich, J. (2015). Protecting the digital afterlife: Virginia's privacy expectation afterlife and choices act. *Rich. JL & Pub. Int*., *19*, 41-75.

Perrone, M. (2012). What happens when we die: Estate planning of digital assets. *CommLaw Conspectus*, *21*, 86-10.

Pinch, R. (2015). Protecting digital assets after death: Issues to consider in planning for your digital estate. *Wayne L. Rev*., *60*, 545-570.

Preston, C. B., & McCann, E. W. (2011). Unwrapping shrinkwraps, clickwraps, and browsewraps: How the law went wrong from horse traders to the law of the horse. *BYU J. Pub. L., 26*, 17-18.

Raskin, M. (2013, April). Meet the bitcoin millionaires. *Bloomberg Business Week*, 10.

Ray, C. (2012). Till death do us part: A proposal for handling digital assets after death. Real Prop. Tr. & Est. *LJ*, *47*, 583-586.

Reed v. Real Detective Pub. Co., 162 P.2d 133, 63 Ariz. 294, 63 A.Z. 294 (1945).

Riley v. California, 134 S. Ct. 2473, 573 U.S. 373, 189 L. Ed. 2d 430 (2014).

Ronsberg, A.L. (2017). The commercial exploitation of personality features in Germany from the personality rights and trademark perspectives. *The Law Journal of the International Trademark Association*, *107*, (4), 802-847.

Rosen, J. (2011). The right to be forgotten. *Stan. L. Rev. Online*, *64*, 88-90.

Rosler, H. (2008). Dignitarian posthumous personality rights-an analysis of US and German constitutional and tort law. *Berkeley J. Int'l L.*, *26*, 153-180.

Roy, M. D. (2011). Beyond the digital asset dilemma: Will Online Services Revolutionize Estate Planning. Quinnipiac Prob. *LJ*, *24*, 376-381.

Sadeghi, H. M. M. (2016). *Crimes against properties and ownership*. Tehran: Mizan Pub.

Safai, S. H. (2012). *Elementary course in civil law*. Tehran: Mizan.

Schneider, N. (2013). Social media wills: Protecting digital assets, *J. Kan. B. Ass'n,* 82, 16-36.

Schuyler v. Curtis, 147 N.Y. 434, 42 N.E. 22, 15 N.Y.S. 787 (1895).

Shafer v. Grimes, 23 Iowa 550 (1867).

Shahidi, M. (2017). *Establishing contracts and promises*. Tehran: Majd publications.

Shirazi, Makarem, N. (1999). *Morality in the Quran*.Vol. 3. Qom: Ali ibn Abi Talib.

Swickard v. WAYNE MED. EXAMINER, 475 N.W.2d 304, 438 Mich. 536 (1991).

Tarney, T. G. (2012). A call for legislation to permit the transfer of digital assets at death. *Cap. UL Rev.*, *40*, 773-795.

Tousi, M. (1967). *Imamieh jurisprudence in detail*, Vol *8*. Tehran: Mortazaviah library to revive Jafarieh relics.

Truong, O. Y. (2009). Virtual Inheritance: Assigning More Virtual Property Rights. Syracuse Sci. & Tech. L. Rep., 21, 57-58.

Twitter. (n.d.). *Twitter terms of service*. Retrieved from https://www.twitter.com/en/tos

Varnado, S. S. (2013). Your digital footprint left behind at death: An illustration of technology leaving the law behind. *La. L. Rev*., *74*, 710-730.

Verizon Media. (2020, October). *Welcome to the Verizon Media privacy policy*. Retrieved from https://www.verizonmedia.com/policies/us/en/verizonmedia/terms/otos/index.html

Watkins, A. F. (2014). Digital properties and death: What will your heirs have access to after you die. Buff. *L. Rev*., *62*, 193-210.

Wilkens, M. (2011). Privacy and security during life, access after death: Are they mutually exclusive. Hastings *LJ*, 62, 1037-1039.

Wilson, A., & Jones, V. (2007). Photographs, privacy and public places. *European Intellectual Property Review*, *29*(9), 357-358.

Winter, S. (2010). Against posthumous rights. *Journal of Applied Philosophy*, *27*(2), 186-199.