ISRAEL INTERNET ASSOCIATION ISOC-IL

Digital Remains:

What happens to our personal data after we die?

Research and Policy Report

Prof. Michael Birnhack* & Dr. Tal Morse**

July 2018

* Professor of Law; Associate Dean (Research), Faculty of Law, Tel Aviv University, birnhack@post.tau.ac.il

** PhD in Media and Communications, Adjunct lecturer, Departments of Politics and Media and Photographic Communication, Hadassah Academic College, Jerusalem, talmor@hac.ac.il

The Israeli Internet Association (ISOC-IL) commissioned the authors to write a research and policy report on the issue of digital remains.

This is an English summary of the Hebrew report.

The full Hebrew report, including full empirical data is available at: https://www.isoc.org.il/about/position-papers/policy-paper-digital-memories.

BACKGROUND

As our lives go digital, so, inevitably, will our death. When somebody dies, he or she leaves behind digital content and data which was accumulated and stored online during their lifetime. Emails we send, pictures we post, and thoughts we share are all stored digitally. Once we die, they remain online. These are our ***digital remains***, which are the bits and pieces that reflect our digital personality, and at the same time, make up the memories our friends and family. As long as we are alive, we, the users, control our own personal data, as a matter of social practice and as per the contract with the service provider. But once we die, these social norms and legal conventions are no longer clear, and a conflict might arise between the dead user's privacy and his or her family and friends' wish to access the digital remains for purposes of grief or commemoration. What happens to our privacy once we die? What happens – and what should happen – to personal data after we die? Who should gain access and control to these materials? What are the considerations for allowing—or denying—access to orphaned online accounts? What are the social functions of digital remains? Who should control them? How would the answers affect the ways we wish to manage our posthumous data before we die?

It is tempting to borrow offline, analog notions to make sense of the digital situation. But analog data differ from digital data in volume, processability, retainability, and in that the latter contain both data and metadata. Moreover, online intermediaries such as email providers or social networks hold the key to accessing the data, unlike the equivalent offline situation, wherein often, no intermediary exists. The online environment reshapes many social practices, allowing new possibilities of social interactions and compelling us to rethink current norms and perceptions. Attitudes towards privacy and death are no exception. The current research and policy report explores the complex quandaries of managing digital remains, identifies the key players, clarifies their rights and interests, examines existing technological and legal solutions, and proposes a regulatory framework for the emerging phenomenon of digital remains.

THE CURRENT RESEARCH

This research focuses on four popular digital platforms and services, each has its own characteristics for holding and managing personal data: email service, social network site (SNS), cloud storage and online dating applications. Drawing on a

literature review about the complexity of engaging with death in the digital age; and based on a comprehensive national online survey of a representative sample of Israeli internet users, conducted in 2017, the current research examines contemporary practices and perceptions of Israeli internet users regarding the management of access to digital remains. In addition, the research maps the legal rights and interests of the relevant players. Since at the time of research and of writing there is no concrete legal regulation in place of these matters in Israel, the research explores Israeli law and compares it with other legal systems, namely the American and French systems which do offer some regulation. The empirical findings and the legal analysis stimulates the discussion and informs the proposed policy and regulation.

METHODOLOGY OF THE QUANTITATIVE SURVEY

In order to have a better understanding of what Israeli internet users wish will happen to their digital remains, we conducted a national online survey among a representative sample of Israeli internet users. The sample was consisted of 478 participants that were randomly sampled via a CAWI (Computer-assisted web interviewing) system operated by Shiluv I^2R research firm. To reach a representative sample, we monitored and control the demographic profile of the participants, including gender, ethnic background, age and geographic location, so it reflects the profile of Israeli internet users. The questionnaires were distributed in Hebrew and Arabic, according to the language of the participants. The survey was conducted in June 2017.

In the survey, we focused on four types of online activities/platforms: email services, SNS activities, cloud storage, and dating applications. For each, we asked about online usage habits and practices. We inquired the awareness of online tools for managing digital remains, and probed on wishes of internet users as to whom they wish to grant access to their digital remains.

MAIN FINDINGS

- **Internet usage**:
    - Israeli internet users are active users: All maintain an email account, and more that 90% have an account on at least one SNS. They use these services regularly and frequently: the vast majority of users use these two services every day. 80% use cloud storage services, but less often.

The use of online dating application is more contracted – 16% of the sample replied that they use such services.

- Most users habitually perform passive activities of media consumption – read posts of other users (84%) and hit the *Like* or *Share* buttons in response to other users' posts. As for active engagement – uploading original content – these activities are performed less often, with 58% users posting verbal content and 44% uploading pictures.

- Based on the findings from these two questions, we calculated a ***Digital Remains (DR) Potential Index*** that incorporates the frequency of online activities *and* the nature of activities on SNS. 24% of Israeli Internet users have a high DR potential; 49% have a medium DR potential, and 27% have a low DR potential.

- **Access by default**: Third to half of the users keep their accounts logged in and their domestic devices unlocked; or have shared their passwords with other; or have a (physical) accessible list of passwords. In the case of the user's death, other people will thus have access by default to their digital remains.
  - Users subscribed to emails, SNS and cloud services will leave access by default in 44%-50% of the cases.
  - With dating applications, the rate drops to 36%.
  - In most cases, participants named their spouse as the person who will be able to access their accounts.

- **Awareness and use of online tools for managing access to digital remains**: Google and Facebook designed and deployed online tools for managing access to digital remains, which are already available for their users.
  - Awareness to the existing tools is rather low, with less than 20% of the participants confirming they have heard about these tools.
  - Only a third of those who are aware of the service have actually activated it (6% of the overall sample).

- **Users' wishes to allow or deny access posthumously**:
  - Users' approach to the four platforms in *not* uniform
  - Approaches to emails, SNS and cloud services are similar, with 45%-50% of users who have accounts on these services who replied that they wish to leave *full access to all* their digital remains.

  - 31%-36% expressed the opposite approach, wishing to *deny all access* to their digital remains.
  - About a fifth of the participants wish to allow access to some content, but not to all.
  - Participants with profiles on dating applications mostly opposed enabling access to their profile, with nearly 70% who wished to deny access to all content.

- **Access to Whom?**
  - 68% of Email users, 68% of SNS, 71% of cloud services wish to enable access to their digital remains to their spouses; 34% wish spouses to have access to their accounts on dating applications.
  - Most respondents *did not* mention their parents

MAIN CONCLUSIONS

- Access to digital remains is a matter that applies to all Israeli internet users. We developed a *digital remains potential* index that incorporates the frequency of online activities and the type of engagement on SNS. It indicates that approximately 3 out of 4 Israeli internet users have a medium or high *digital remains potential*.
- There is no one-size-fits-all solution that is suitable to all platforms or is preferred by most users.
- Awareness to existing online tools for managing access to digital remains is low and the actual use is limited.
- Spouses are the preferred fiduciary by most users.
- With no policy in place, between third and half of the users will leave, after they die, access by default to the person who retains the personal devices.

LEGAL FRAMEWORK

From a legal point of view, digital remains are not uniform: these remains can be intangible assets, intellectual property, information about physical or tangible property, or personal data. Thus, there are multiple relevant legal frameworks: property law, privacy law, and contract law. We need to discern the status of the data at stake and apply the legal framework accordingly.

- **Intangible property**: e.g., virtual currency, domain names, purchased (music, software, avatars, etc., may be considered property. Their fate after their owner has died should be determined according to the contract under which they were created or purchased in the first place.

- In case there is no contract in place, or that the contract does not require otherwise, intangible property is part of the estate, and the legal heirs of the deceased user should become the new owners, either according to a will or pertinent to inheritance law.

- **Intellectual property**: Digital content can be protected under copyright law, e.g., unpublished manuscripts and articles, or original photographs. In such a case, the rights belong to the legal owner, and upon his or her death, the material rights are transferred to the heirs. If the heirs have access to these works, whether because they were published or shared with them, or because they have access by default to the deceased personal devices, no problem emerges, and the heirs do not need the assistance of an intermediator.

- When the heirs do not have access to the protected content it seems that the platform is not obliged to enable access to these materials, albeit it can choose to do so, according to its policy and considerations or according to the terms of use that were agreed upon beforehand. This may sound an awkward result, but it may occur in offline contexts as well, for example when there is one copy of a work, such as a painting, owned by one party, but the copyright is of the heirs.

- Under Israeli law, moral rights can be managed only by the immediate family.

- The platform itself is subject to copyright law and cannot perform any action that would otherwise harm the copyrighted materials, unless it was agreed in advance in the terms of use.

- Copyrighted works may contain personal data of third parties, e.g., a personal diary or a draft of a book. The copyrighted status of the works does not obliterate such privacy rights. Thus, the ISP or platform that enables access to such content, might be subject to privacy laws.

- **Data about Property**: Increasingly, we manage financial accounts online. Such data is ancillary to property, and thus property law can govern it. The estate manager might not know of such assets, and access to the deceased's digital remains might be crucial for this purpose. However, such data is also subject to privacy law. Therefore, we need to figure out a procedure in which the estate manager can gain access to digital remains for estate management purposes only, while keeping the personal data sealed.

- **Personal Data and Posthumous Privacy**: All other data – which is not itself virtual property, intellectual property or information about real or virtual property, should be treated as personal data. During the life of the user, such data is regulated under privacy (or data protection) law, and is considered a personal right, rather than an in-rem right. We argue that privacy, rather than property law, is the suitable legal framework for regulating digital remains which are not part of the previous categories discussed above.

- Privacy, as a personal right, ceases to exist after death. Nevertheless, the living person's expectations and right to privacy, regarding what will happen with their personal data after their death, is a right that survives and should be protected. The living user is best placed to make decisions regarding his or her personal data.

- The challenge in shaping the optimal policy is that many users have not expressed their wishes regarding their personal data during their lifetime. It is tempting for a court, facing such a case, to assume the user's wish, based on social norms. However, the empirical findings clearly indicate that any such assumption about the social norm, whether for or against posthumous access to personal data, will be wrong.

- Another policy option is to set default rules, either that all posthumous access will be permitted, unless the user objected during his or her lifetime, or the opposite default rule, that no access should be allowed, unless the user expressed his or her will to enable such access. However, default rules tend to be sticky, i.e., users do not change them, for various cognitive,

social and technological biases. Hence, and due to the diversity of interests as indicated by the findings, any such default rule will be misguided.

- Eventually, the choice is a normative one. We side with the users' privacy interests, especially when we add third parties' privacy, since one's digital remains would often contain other people's personal data. We submit that the best option is thus to avoid enabling general access to a deceased user's digital remains. However, we should encourage the formation of mechanisms that can decide otherwise: the platforms should have some discretion to make a decision; courts should hear petitions to enable access. Given the burden, we anticipate that there will not be many such cases.

RECOMMENDATIONS

After mapping the legal context of access to digital remains and drawing on the findings from the empirical research, we offer the following recommendations:

USERS' AUTONOMY

- Since coping with loss and death is a personal, individualistic matter which changes from one person to another; and since Israeli internet users hold different, sometimes contradicting views on possible regulations; and since a tailor-made self-regulation that meets the specificities of each user is at hand – we believe the best regulatory response is ***to allow each internet user to choose their own terms of access to their digital remains***. This approach reflects the human dignity and the privacy of the users, and it leaves it to them to choose with whom they wish to share which personal content after they die. Or, to instruct the erasure of the accounts forever. This approach will allow the bereaved family and friends to access the deceased user's digital remains according to the user's own wishes.

RAISING AWARENESS

Along with leaving the decision to each user to set their own terms of accessing their digital remains, we believe much more needs to be done in order to raise awareness to the issue of digital remains and the possibilities to regulate the access to them. Thus, we recommend the following:

1. Launching a national campaign that will provide general information about these issues.

2. Identifying potential crossroads or milestones in users' life course, which create meeting points that can be used to convey information and encourage management of digital remains, for example by setting terms and activating online tools for managing digital remains. These crossroads include (but not limited to) joining the army or the police, issuing a driving license, issuing an ID card or passport, and special classes in high schools.

3. The time of registering for ISP services directly with the ISP, or through the workplace or academic institution, creates a convenient meeting point to raise the issue.

4. ISPs should be required to design a policy on the matter and bring it to the users' attention at the time of registration, and make it available thereafter.

5. Raising awareness amongst "digital-remains-agents" and training them for this task. Possible digital-remains-agents are social workers, lawyers who handle wills and inheritance, pension and insurance agents, end-of-life spiritual caregivers, and other professionals that accompany people regarding end-of-life decision making.

6. The reasons for the low awareness and user's avoidance of using online tools should be subject to further studies.

DUTY TO HAVE A POLICY

7. We recommend that ISPs that operate in Israel, whether these are Israeli or foreign providers, will be obliged to determine their own policy regarding accessing digital remains, and to communicate it clearly and in an accessible manner to users. We submit that the content of these policies should not be dictated – each ISP should set its own policy. However, the proposed duty is that each ISP must have *a* policy, and each much inform users about it.

   The purpose of this recommendation is, firstly, to motivate ISPs to design such a policy and perhaps also online tools. This is a form of soft-regulation, content-neutral, and hence minimizes external interference by regulation in the ISPs' business and rights. Secondly, to achieve clarity on these matters.

Currently, many ISPs who operate in Israel do not have any policy on this matter, and those who do have a policy, more often than not, do not communicate it to their users. Thirdly, we hope that once these providers clarify their policies and inform their users, it will generate some kind of a chain effect that would motivate users to pay attention to these aspects and make choices regarding their digital remains, in accordance with the ISP's policy.

8. ISPs and platforms should be required to publish the above policy in an accessible and easy to comprehend manner.

9. ISPs and platforms should establish a designated, direct and easy-to-use channel of communication to inquire about the options, when needed.

PROPERTY AND DATA ABOUT PROPERTY

10. Intangible, virtual assets should be considered part of the estate, but are subject to the contract which has created these assets in the first place.

11. In the absence of a contractual reference, or if the contract does not otherwise limit transferability, the virtual asset is part of the estate, and its execution is to be conducted according to regular inheritance law. an order by the relevant authority or court can instruct the ISP or platform to act accordingly.

12. We recommend that contracts that create virtual assets explicitly refer to their status in the case of the owner's death.

COPYRIGHTED WORKS

13. Any regulation or policy pertaining to digital rights, should clarify that it is subject to general law, namely copyright law, privacy law, and the law about intermediaries' legal liability regarding data that they hold or control, but not own.

INFORMATION ABOUT PROPERTY

14. In order to enable estate managers to access data about property, there is no need to amend inheritance law. According to current Israeli inheritance law, the estate manager has sufficient power to search the deceased's assets, and hence can request to see relevant data.

15. Estate mangers should learn more about digital remains, and the option of such digital remains containing relevant information.

16. Courts, when appointing an estate manager or when instructing the manager, should make sure that access to digital remains is limited to the purpose of detecting the deceased's assets, while reiterating the duty of confidentiality. If the executor is a family member of the deceased, this has to be taken into consideration, for example by appointing another executor for the sole purpose of searching the digital remains, so to minimize the violation of the deceased's and third parties' privacy.

WILLS

17. Similar to the American Model law, we propose an amendment to the Inheritance Act, so to clarify that a user's instruction regarding the ownership of virtual assets and intellectual property, given by using an online tool of the relevant platform, has priority over other instructions, as long as the user can change their initial instruction.

18. In the absence of an instruction by way of using the online tool or in the form of a will, regular inheritance law should apply to virtual assets, as well as the executor's access to data about property.

19. Lawyers who assist clients with their wills should be aware of digital remains and consult their clients about the matter.

PERSONAL DATA

20. We should distinguish between information and data that are virtual assets or intellectual property or information about such property, and personal data. The latter category should not be treated under property law.

21. When clear evidence is available, about the deceased user's wishes regarding enabling or denying access to his or her personal data, we should follow such evidence. Assuming the user's wishes based on general assumptions about social norms is misguided and should be avoided.

22. We submit that the law should not adopt any default rules in this regard. The upshot of this is that any ISP or platform will be determining their own policies regarding the fate of digital remains. As stated above, there should be a duty to design such a policy and make it available to users.

23. Family and friends who nevertheless, despite the platform's policies, wish to access digital remains, should be able to petition the court. Petitioners should bear the burden of making the case. The court should separate the property-related issues from those pertaining to data protection. The court should have discretion in the matter, taking into account evidence regarding the user's wishes, third parties' privacy interests, the kind of the data and its context (an intimate photo in an online dating site is different than a word file in the cloud), and the burden to the platform. The court can consider appointing a privacy fiduciary, who will be able to access the digital remains and sift data in a manner that would minimize the violation of the deceased user's privacy interests and his or her parties to conversations.

24. A privacy fiduciary can further assist in other cases, where the data is held by third parties, such as the workplace. The fiduciary should have broad discretion in the matter. The privacy fiduciary is subject to duties of confidentiality.