Memory and Privacy in The Entire History of You

Bianca Rodrigues Teixeira and Flavia Maria Santoro

¹ Federal University of the State of Rio de Janeiro, Rio de Janeiro, RJ, Brazil {bianca.teixeira, flavia.santoro}@uniriotec.br

Abstract. Privacy is a concerning issue today, with millions of people sharing their everyday lives on various social media platforms. Everything people share can be considered as part of their digital memory, which can be consisted of thoughts and feelings posted online. Memory is the focus of "The entire history of you", third episode of British television series "Black Mirror". The characters use a device that records and saves what their eyes see, and it's also possible to browse through all previous memories. The device contains most, if not all, of the user's life, which is undoubtedly useful in many daily events, like court cases, debates, reliving previous experiences, security checking, etc. However, it can be a huge problem if somebody tries to see memories that are supposed to be private. To try to combat that possibility, we defined an ontology for Digital Memory and specified our proposal of new features for the device regarding privacy using artificial intelligence. We believe that there is still room for improvement and for more discussion about video-memory and privacy, which is a topic that is not frequently debated.

Keywords: memory, privacy, black mirror, ontology

1 Introduction

In the past few years, technology has experienced some major advancements. British television series "Black Mirror" highlights several scenarios in which those said advancements could potentially lead to a dystopian society. As its creator Charlie Brooker stated [4], its episodes are about today's society's future if people are not careful. This paper is concerned with the third episode of Black Mirror's first season, entitled "The entire history of you". It is set in a world in which most humans have the "grain" device implanted in their bodies. The grain captures the images seen from the user's eyes and saves them so that they can watch previous times of their lives. It acts as a digital memory, browsable and rewindable.

That device makes sense since every day, as over one billion people actively use Facebook, sharing their lives online [7] and all this data has been stored and can be revisited on demand. In a way, we are already digitizing part of our lives and, thus, creating digital memory. However, "The entire history of you" leaves a gap on an issue that also applies to today: privacy. Acquisiti and Gross [8] performed a study and found that a minimal percentage of Facebook users even change the default privacy settings. Moreover, this issue has been addressed through the concept of Privacy-by-Design which is related to a proactive incorporation of privacy principles in a system's design, i.e. an approach to minimize information systems' privacy risks through technical and governance rules [14].

In this paper, we explore the issue of privacy related to the memory recording technology presented in Black Mirror. The episode's main character forced himself into seeing other people's memories, threatening their safety. So, the privacy aspect of memory needs to be addressed in order to avoid such situations.

We propose a way to prevent privacy invasion of a person's memory by using artificial intelligence, guided by an ontology for the broad concept of digital memory that includes the concept of private memory associated to the context in which it was produced. Regarding "The entire history of you", we aim at specifying a technique for the grain device to be able to control unwanted requests from third parties to view a person's memories in certain situations of privacy violation.

The paper is organized as follows. In Section 2, we present the digital memory ontology. Section 3 serves as the correlation between the ontology and a new feature for the grain, which would solve the privacy issue we are referring to in this work. Section 4 discusses related work. Section 5 concludes the paper and points open issues for future work.

2 A Digital Memory Ontology

According to Megill [12], "Memory is an image of the past constructed by a subjectivity in the present." The operations related to memory – the acts of remembering and forgetting – undergo an ontological shift with a possibility of also representing and recording both thoughts and speech established within social groups as an extension of itself, through the modeling, construction, and organization of external memories [13].

Information technology artifacts derive from an infrastructure capable of storing, generating and manipulating all the online traces created by individuals and by society. This organization includes sophisticated computational models and algorithms of semantical data processing, which are property of public or private institutions able to conduct social engineering processes in all spheres: political, civic, commercial, and individual. Individuals are the providers of their own memories, which are collected and manipulated by the real holders of power.

The use of the grain in "The entire history of you" potentially makes private memories available to anyone who chooses to see them. The choice for the visualization of the memories might pass through the permission of the individual, who sees in the device an option of control and security; however, this control is actually made by the device, which unveils the world for the human who does not find an exit for that attractive device. We propose to use the technology to support users in finding this way out. So, as a starting point, we argue for a formal definition of memory and privacy through an ontology extended from [13] and [11]. Ontology is a formal language designed to represent a particular domain of knowledge, so as a critical component of knowledge management, as well as for Semantic Web [9].

Rodrigues et al. [13] state that thinking memory as a opens the possibility that, from a new situation or a new encounter, the past can be both remembered and reinvented. In this way, the history of a subject, individual or collective, can be the history of the different senses that emerge in their relationships. It makes possible that

2

memory, instead of being recovered or rescued, can be created and recreated from the new senses that always occur for both individual and collective memory, since they are all social subjects. The polysemy of memory, which could be its flaw, is indeed its richness. Rodrigues et al. [13] proposed a preliminary ontological model to represent the concept of external digital contemporary memory which encompasses classes (concepts) and their relationships.

Collective memories result from the interactions between individuals, the past and present reality. The processes of collective memory production are diverse and transformed over time according to the social experience and the technological devices of that context. Fundamental operations, such as, generate, store, manipulate, modify, retrieve, and share, affect external memory. So, the creation of digital memories occurs through various processes, through social networks on the web, applications, surveillance cameras in public and private space, closed systems, content production, GPS, cookies, digital traces, among many others. The production of the memory operates in "real-time" or "online" both in individual and in collective layer. Thus, digital memory can provide relationships between individual and collective memories, and might subvert ontological experiences, such as the processes of remembering and forgetting, as well as cultural, social, economic, political, historical, and other issues.

By analyzing the dystopian future of Black Mirror, we first observe that people's memories are reduced to videos of interactions of the human eye with certain events, like a camera that can only capture a collection of instant pictures. Our ontology intends to broaden this concept. We are interested in how individual memories connect to collective memories in order to classify them, identify the context of one particular piece of memory, and moreover, to establish boundaries able to distinguish what is public and private. In this sense, we extended the ontology presented in [13] to include the formal definition of Private Memory and Context. Figure 1 presents the graphical representation for the ontology organized in a Unified Modeling Language (UML¹) Class Diagram. Table 1 explains the types of memory that compose the main concept of external digital memory.

¹ http://www.omg.org/spec/UML/



Fig. 1. External Digital Memory Ontological Model extended from [13] and [11]

Memory Type	Content
Individual	Part of the external memory that exchanges information shared with the external world to the cyberspace
Collective	Produced by relationships and experiences practiced among individuals and social groups through interactions with individual memory and auto- relations
Biological	Born with the individual
Private	Proprietary, not shared by any individual, organism or thing
Shared	Proprietary that interacts with the cyberspace; Distributed by an individual, collective or system agent
Artificial	Any non-biological memory of the individual
Generated	Generated or created by individuals or collectivity, explicitly or implicitly
Stored	Registered and stored within private, commercial, or governmental clouds
Manipulated	Operated by applications, social networks or systems that access the cyberspace
Retrieved	Accessed for private or collective use, or yet to obtain digital traces
Modified	Subjected to changes, with/without authorization of the individual or collective agent

 Table 1. Types of Memory

In the External Digital Memory Ontology, we define Private Memory as a type of Individual Memory that should not be shared. Moreover, we argue that a certain memory should be defined as private dynamically, i.e., depending on the context in which the set of actions within this memory occurred, as well as the context in which it has been selected to be watched. An action is executed or an event occurs in a context. While an event is a real-world occurrence that can be distinguished, context can be defined as a complex description of the knowledge shared in physical, social, historical and other circumstances in which actions or events happen. All this knowledge is not a part of the action or the event, but will constrain the execution of the action or the interpretation of the event [3].

So, the following definitions are provided. First, we will consider one instance of Individual Memory as one video registered by the grain. So, it can be retrieved as one piece of memory. Second, we define Context. We adopted the definition of context proposed by [3] which distinguishes the concepts of contextual element and context: (i) a contextual element is any piece of data or information that allows an entity to be characterized within a domain; and (ii) context is the set of instantiated contextual elements that are needed to support a task performed by an agent (human or software). A contextual element is stable and can be set at designated time, whereas context (a collection of contextual elements) is dynamic and must be constructed at runtime, when the interaction occurs. The fundamental concept adopted here is that contextual elements that are necessary to support an event. And finally, we define Private Memory as a type of Memory temporarily instantiated depending on a Situation characterized by a certain Context.

Given CE as the set of contextual elements, for all contextual elements $ce_i \in CE$, where $1 \le i \le n$ and $n = \frac{|CE|}{n}$, a domain (Dom (ce_i)) is associated, indicating the possible values that the contextual element can assume.

Given Dom (ce_i)= { d_{i1} , d_{i2} , ..., d_{iMi} }, where $M_i = |Dom(ce_i)|$, the set E is defined as the set of all contextual elements with their associated values:

 $E = \{ce_1 = d_{11}, ..., ce_1 = d_{1M1}, ce_2 = d_{21}, ..., ce_2 = d_{2M2}, ..., ce_n = d_{n1}, ..., ce_n = d_{nMn}\}$

A Situation is defined as a sub-set of $E(S \subseteq E)$, where a certain contextual element only appears once. A Situation, which is activated in the context model, represents a state within the system (i.e., system variables, people, organization, and external data). We represent it in terms of Event-Condition-Action (ECA) rules, and thus a system could reason over the representation of the current state in order to continue satisfying its goal (which in this case is to decide whether a piece of memory should be set as private or not):

IF Focus(is_active = True) AND Contextual Element (name = X) THEN the Contextual Element instantiated X is associated with Focus

IF a Situation (set of contextual elements) THEN the Piece of Memory is temporarily set as Private Memory

3 Proposal: re-coding the grain

We propose to extend the conception of the grain system to use the Ontology described in Section 2 as a semantic technology that can support the identification of privacy violation. Therefore, we present the description of its new requirements and a scenario to illustrate the shift in its usage.

3.1 System Requirements

In "The entire history of you", the main character threatens other people's security to gain access to the information stored on their grain. We propose a way for the grain to detect the possible privacy invasion, which would cause the system to be temporarily blocked. The first step is to set up the combination of Contextual Elements necessary to characterize a Situation in which an Individual Memory must be set as Private Memory. Then, the main action of the system would be to identify this context (possible Situations as defined in the Ontology). This could be done in two ways: on demand or automatically. We break down the two possibilities of our proposal.

3.1.1 On demand

In the first way, speech recognition would be used. Speech recognition, as defined by Anusuya and Katti [1], is "the process of converting a speech signal to a sequence of words, by means of an algorithm implemented as a computer program". This concept allows for computer systems to follow voice commands, which is exactly what we are after on this approach. The user could set up a specific voice command that would disable the grain and another command that would turn it back on.

The grain already records audio at all times, meaning it would constantly be listening and waiting for the previously set up commands. This technique is already used today in Google's Android system, with the phrase "Okay Google", and in Apple's iPhone by saying "Hey Siri" [5]. This is accomplished with Keyword Spotting (KWS), a method which detects keywords in an audio stream, allowing for hand-free interaction [6]. In [6] a proposal is presented of a KWS approach appropriate for mobile devices. If the user detected any possible threat to their privacy, they could disable the ability to browse through their memories momentarily by simply saying the command that does that.

The "on demand" feature is useful for creating data for the system to learn some kinds of Situations that might constitute a privacy invasion directly from the owner of the memory perspective. However, since it is up to the user to define when to lock the grain, there is still room for harassment, as seen on the Black Mirror episode. The user could still be forced or threatened to unlock his or her Grain, which would defeat our purpose of protecting him or her. This leads us to another possibility to further protect people's privacy.

6

3.1.2 Automatically

The most relevant way would be for the grain to analyze, in real time, the video and audio of the current moment. The system is trained to identify contexts within the content of the image/audio in which a memory should be considered private, so it could block the memory-browsing feature.

Today, there are already many examples of intelligent surveillance systems able to analyze and identify patterns in videos. [15] does a review of some systems, including "systems able to warn against, detect and identify abnormal and alarming situations". Such systems use algorithms that could be applied specifically to the grain to try to identify the set of contextual elements set in the ontology. The big difference, though, lays on the equipment. Surveillance systems feature multiple cameras, whereas the grain relies on the user's eyes. If properly adapted, the algorithms and techniques can be helpful in our case. Another important property is that contextual elements could also be retrieved from other sources like social networks; individuals' personal data stored by the system; GPS; physical sensors; or any other configured by the system.

This goal of this feature is to obtain several types of data from different sources and combine them so that the system can infer the context of the occurrence of the event and as well the context of requesting access to this memory.

3.1.3 Application scenario

In "The entire history of you", the main character pressures his wife into showing him her memory of the sexual affair she had during their marriage. It's clear how uncomfortable she feels and how she tries to delete the memory when her husband is not looking. We argue that this memory is private and her husband is invading her privacy. So, how would this situation happen in the new grain system configuration? Our proposal is that the grain, using its artificial intelligence, would detect possible privacy invasion, and would make that particular memory private.

Since the grain has been with Ffion, the wife, for years, it learned her relationship with her husband, and also that she cheated on him with Jonas. It collects every conversation she has and sees everything she does, so it understands a lot about her life.

When Liam, the husband, was asking, and then demanding, Ffion to show him the memory, Ffion's grain was processing their speech and understanding that a certain video was being mentioned. It also understood that Ffion did not want to show it to Liam, which is one of the important the variables for this case.

We focus on the automatic privacy detection. There are plenty of variables that might be considered when deciding about making a memory private. In the scene portrayed in Black Mirror, we have: the fact that Liam was asking for a memory he was not a part of; the fact that Ffion was hesitant and uncomfortable; and the fact she was having sexual relations with a man other than her husband (which would break the lover's privacy as well).

We can define those variables in terms of Contextual Elements and the domain of possible values:

 $ce_1 = location of the Individual Memory$

 $ce_2 = time of the Individual Memory$

 $ce_3 = presence$ of the requester in the Individual Memory

 $ce_4 = psychological condition of the owner of the Individual Memory$

 $ce_5 = action pattern in the Individual Memory$

 ce_6 = presence of a friend who is not friend of the Individual Memory requester

E= {ce₁= couple's room, house's dining room, park close to the house, ce₂=today, ce₂=last year, ce₃=Yes, ce₃=No, ce₄=hesitant, ce₄=quiet, ce₄=nervous, ce₅=sexual relation, ce₅=playing with the kid, ce₅=dance at a party, ce₅=sleeping, ce₆=Jonas, ce₆=Mary ce₆=Louise ce₆=Paula}

Yet, many Situations could be learned by the system from a combination of those Contextual Elements with the Focus on that particular Individual Memory. For example:

 $S_A = \{$ couple's room, last year, No, hesitant, sexual relationship, Jonas $\}$

IF S_A THEN the Piece of Memory of Ffion having sex with Jonas is temporarily set as Private Memory

And another example would be:

 $S_B = \{ \text{park close to the house, today, No, nervous, playing with the kid, Paula} \}$

IF S_{B} THEN the Piece of Memory of Ffion playing at the park is temporarily set as Private Memory

These variables should be enough for the grain to hide that particular memory. The context in which the memory was being requested was not a context for that memory to be public. If Ffion was to browse through her memories at that time, that one memory would be censored and have some caption say "private". If the context changed to a friendly context and not enough variables were presented, the memory would be public again.

The idea is that the grain understands how its user feels. It should be capable of judging the current situation and to act as a tool favorable to the user. The concept of privacy is introduced mainly to favor the user. Memories are recorded at all times, and not everything is meant to be seen by other people at any time.

4 **Related work**

To the best of our knowledge, there are no proposals yet addressing the memory/privacy issue based on a theoretical and ethical discussion to build technology able to reduce the risks of a dystopian future. Some authors argue about the problems and dichotomy raised by them. In general, they agree that there are benefits, as well as inherent risks.

Boren [2] affirms that the episode "The entire history of you" shows the potential benefits of such, as clearly stated by a woman at the house party who claimed that "Half the organic memories you have are junk—just not trustworthy". Brain implants provide the ability to have a reliable memory of the past, which can be useful in court cases, debates over who said what, or for reliving previous experiences. Like some employers already check potential employees' Facebook accounts, the company that

interviewed Liam suggested that employees should do extensive Redoes. The grain could also be useful in airport security to scan a traveler's past week for any suspicious activity. However, they are also examples that benefits might come with a cost: the invasion of personal privacy.

Lima [10] discusses from a psychological perspective that, although the device can capture and store the experience, experiencing is always subjective. The author explains that there is a strong counterpoint between the memory understood from the psychoanalytic conception and the biological memory object of the neurosciences. This opposition starts from conceptualizing the amnesic data as a record, a mark, a positive mark stored in our cerebral cortex, the mark or significant mark, which as such is defined by opposition and difference and has modes of operation. The brain capable of storing information is different from the signifying body as a record of experience.

We present a proposal to undertake such problems. By making the information about the grain's ability to lock itself public, we believe the sort of attacks seen in Black Mirror would not happen. We are trying to create a way to protect the user's memories from unwanted third parties by adding to the grain artificial intelligence, speech recognition and computer vision.

5 Conclusions and future perspectives

We have presented a way to incorporate privacy protection into the grain device seen on Black Mirror. We believe our solution is a start to many other features regarding privacy, but still leaves room for other issues. The machine learning capability we think the grain should have is not simple and requires a lot of work. It should be able to process speech and to interpret video in an extremely advanced way, so that it can think like its user. We visualize the grain as being almost part of its user, who relies on its device for protecting their privacy.

Our solution, however, does not guarantee hacking attempts won't happen, which can also break users' privacy – even though "The entire history of you" does not touch on that subject. Furthermore, the grain's context interpretation is likely not going to be perfect. Its intelligence may also overcome the user's current state of mind. For example, if the user is intoxicated and wants to show private memories to other people in a context the grain may judge as not favorable, it could block said memories from being shown. This could cause trouble, but the grain would see it as protecting its user.

Another delicate example would be if the user was in trial for a certain crime. If the user was requested to give their memories as evidence, and if the user was guilty, the grain would sense the user is in trouble. However, we believe justice is a greater good, and the grain should not block the memories. This example illustrates how sensitive this topic is and how open it is for discussion, for we have not come to a full conclusion on what the best solution regarding privacy is. We have provided one in order to try to create space for other ideas that would enable humans to live a better future than the dystopian one presented in "The entire history of you".

Future work may regard the grain's technology to process speech and video, and how to store the information it collects about the user's privacy wishes and feelings.

Besides, we also will explore the relationships among the different types of memories depicted in the External Digital Memory Ontology. For example, an important discussion would be about Collective Memory. Since one video contains an event with many participants, who is the owner (even if captured by only one individual)?

We could also extend the investigation to reflect on potential forms of abuse and discrimination that may stem from grain-like devices, e.g. the use of body-worn cameras by police. Different solutions are needed to maintain privacy in a world so public as the one portrayed in Black Mirror, in which people constantly share their memories and want to see other people's memories.

References

- 1 Anusuya, M., Katti, S.: Speech Recognition by Machine: A Review. International Journal of Computer Science and Information Security, IJCSIS 6 (3), pp. 181-205 (2009).
- 2 Boren, A.: A Rhetorical Analysis of *Black Mirror*: Entertaining Reflections of Digital Technology's Darker Effects. Undergraduate Research Journal at UCCS 8 (1), 15-24 (2015).
- 3 Brézillon, P. Context in problem solving: a survey. The Knowledge Engineering Review 14 (1), 1–34 (1999).
- 4 Charlie Brooker: the dark side of our gadget addiction, https://www.theguardian.com/technology/2011/dec/01/charlie-brooker-dark-sidegadget-addiction-black-mirror, last accessed 2017/06/03.
- 5 Chen, G., Parada, C., Heigold, G.: Query-by-Example Keyword Spotting Using Long Short-Term Memory Networks. In: 2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 5236-5240, IEEE, Australia (2015).
- 6 Chen, G., Parada, C., Heigold, G.: Small-Footprint Keyword Spotting Using Deep Neural Networks. In: 2014 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 4087–4091, IEEE, Italy (2014).
- 7 Facebook Reports First Quarter 2017 Results, available at: https://investor.fb.com/investor-news/press-release-details/2017/Facebook-Reports-First-Quarter-2017-Results/default.aspx, last accessed 2017/06/03.
- 8 Gross, R., Acquisiti, A.: Information Revelation and Privacy in Online Social Networks(The Facebook case). In: ACM Workshop on Privacy in the Electronic Society (WPES), pp. 71-80, New York, (2005).
- 9 Guizzardi, G.: On Ontology, Ontologies, Conceptualizations, Modeling Languages, and (Meta)Models. In: Olegas Vasilecas, Johann Eder, and Albertas Caplinskas (eds.), Proceedings of the 2007 Conference on Databases and Information Systems, Amsterdam, The Netherlands, The Netherlands pp. 18-39 (2007).
- 10 Lima, N.: Memoria perpetua. Comentario del episodio «The entire history of you» de Black Mirror (2011). Revista de Medicina y Cine [Internet] 11(3), 147-156 (2015). (in Spanish) Available at: http://revistas.usal.es/index.php/medicina_y_cine/article/view/13322, last accessed in 2017/07.
- 11 Mattos T.C., Santoro F.M., Revoredo K., Nunes V.T.: A formal representation for context-aware business processes. Computers in Industry (65), p. 1193-1214 (2014).
- 12 Megill, A.: History, Memory, Identity. In: Jeffrey K. Olick, Vered Vinitzky-Seroussi and Daniel Levy (eds.), The Collective Memory Reader. New York: Oxford University

Press, 193-197 (2004). (Excerpted from "History, Memory, Identity," History of the Human Sciences, August 1998, 11: 37-62).

- 13 Rodrigues, J., Baião, F., Santoro, F., Cappelli, C.: Cyberspace: Towards an Ontology of the External Digital Contemporary Memory. In: Twenty-third Americas Conference on Information Systems (2017).
- 14 Spiekermann, S., Cranor, L.F.: Engineering privacy. IEEE Transactions on Software Engineering 35 (1), 67–82 (2009).
- 15 Zabłocki1, M., Gościewska1, K., Frejlichowski, D., Hofman, R.: Intelligent video surveillance systems for public spaces a survey. Journal of Theoretical and Applied Computer Science 8 (4), 13–27 (2014).