From Cyberpunk to Regulation

Digitised Memories as Personal and Sensitive Data within the EU Data Protection Law

by **Krzysztof Garstka***

Abstract: Every new medium through which information can be communicated is likely to bring new challenges for the established data protection laws and paradigms. In the light of progressing research aimed at deciphering the human brain, this article seeks to analyse the General Data Protection Regulation's ability to respond to the possible appearance of memory digitisation technology. To this end, the article draws on the fictional setting of a PC game entitled Remember Me, where such a technology was developed and embraced by the society. In an exploratory analysis, the GDPR's definitions of personal and sensitive data are tested regarding their ability to remain "technology-neutral" in the face of an information technology capable of identifying individuals in unique and unprecedented ways. The article confirms the Regulation's preliminary potential to accommodate the studied invention and proposes an interpretation of the corresponding articles of the GDPR, aimed at the adequate protection of data subjects.

Keywords: Personal Data; Sensitive Data; General Data Protection Regulation; Digitised Memories; Sensen

Recommended citation: Krzysztof Garstka, From Cyberpunk to Regulation – Digitised Memories as Personal and Sensitive Data within the EU Data Protection Law, 8 (2017) JIPITEC 293 para 1.

A. Introduction

1 The General Data Protection Regulation (GDPR)[1] was adopted on the 27th of April 2016, over twenty years after its predecessor, the Data Protection Directive (DPD).[2] One may wonder whether this lengthy legislative gap is based on the premise that during the last two decades, there were not many changes in the technological realm regulated by those two instruments. This is certainly not the case, as the opposite occurred. The more plausible explanation is one put forth by Bygrave, who wrote that the legislative process leading to the enactment of the DPD "took over five years and was subject to hefty debate and frenetic lobbying"[3], characteristics he

* PhD, LLM, LLB. Information Governance Research Associate at the Centre for Intellectual Property and Information Law, Faculty of Law, University of Cambridge; member of the Trinity Hall.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

3 Bygrave L, *Data Privacy Law: An International Perspective* (2014) OUP, at p. 6.

also found in the development process of the GDPR and other data protection instruments. Undoubtedly, this area of law can be seen as very volatile and one in which achieving consensus on regulatory steps might take many years.

2 Consequently, it seems that the GDPR is going to be the main data protection instrument in the EU for quite a while, maybe for another twenty years. Hence, it is particularly crucial to turn the academic attention in its direction, in order to assess the likelihood of Regulation's success as a key regulatory response to the vast array of data protection challenges faced, currently and in the future, by Europe's information society.

3 It goes without saying that the immediately valuable and required writing in this field should focus on the technological *status quo*; and indeed, multiple academics approached the GDPR from this angle.[4] Nevertheless, from the perspective of IT law scholarship, it might be worth occasionally looking towards certain selected visions of the future. After all, multiple technological developments of the digital age - which posed new, considerable regulatory challenges, catching the established legal frameworks by surprise - were predicted in science-fiction literature and cinematography.[5] Cyberspace itself – which continues to create new challenges of the discussed kind – is a term coined in a 1980s short story *Burning Chrome*, written by probably the most appropriate author to be referred to in this paragraph, William Gibson. In his works, the network in question is already omnipresent in society, much like and beyond what it is today.

4 Among the various genres of science-fiction, the one represented by Gibson is probably the most deserving of IT lawyers' attention. This genre is called cyberpunk, and revolves around the visions of a not-so-distant, dystopian, urban future where technology permeates every aspect of human life (not necessarily making it better) and where corporations hold much of the real power in the world. The impact of information technology on both society and the individual often plays a key, underlying role in many cyberpunk novels.

5 This is where this article takes a second detour towards the unconventional. Instead of reaching out to a cyberpunk novel or short story, the creative work chosen to shed a futuristic light on the GDPR is actually a video game. Its title is *Remember Me*, and it was developed and released by Dontnod Entertainment in 2013. Following the protagonist "memory hunter" Nilin, the game paints a vivid and sophisticated image of a world in which human memories can be digitised; and through this image, explores a plethora of social, economic, cultural and personal consequences of the said invention. As it will be seen, the nature of those consequences (described in a latter section of this piece) brings data protection issues to mind almost instantly, and prompts the question of whether the GDPR would be able to accommodate the arrival of memory digitisation technology.

6 It is a question which might be even more deserving of attention if certain current directions of scientific research are taken into account. For example, a team of researchers from Harvard Medical School used fMRI (functional magnetic resonance imaging) to discover how our hippocampus "replays experiences during quiet rest periods", and how such experiences are prioritised.[6] A group of US and Japanese scientists recently discovered how long-term memories are created and stored in mammal brains,[7] and Facebook is intensely attempting to create the technology which could detect what we say silently in our heads.[8] While direct memory digitisation has not yet appeared (especially not in the way it did in the world of *Remember Me*), there is a growing body of research consciously or unconsciously approaching this invention.

7 Consequently, it can be stated that this exploratory piece can be seen as aimed at two symbiotic, mutually supportive goals. Firstly, it seeks to test the degree to which the GDPR is technology neutral, by pitting it against a novel, strongly disruptive technology. Secondly, the article strives to begin the search for an appropriate regulatory response to the potential invention of memory digitisation, a search conducted within the realm of EU data protection law – where the GDPR is the key, flagship instrument. Hence, while the discussed technology would be certain to bring a host of regulatory challenges to multiple branches of law and legal instruments, the article focuses on

4 See e.g. Vanberg AD and Unver MB, 'The right to data portability in the GDPR and EU competition law: odd couple or dynamic duo?' (2017) EJLT 8(1), at p. 1; Bolognini L and Bistolfi C, 'Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation' (2017) C.L.S. Rev. 33(2), pp. 171-181; or Kornbeck J, 'Transferring athletes' personal data from the EU to third countries for anti-doping purposes: applying Recital 112 GDPR in the post-Schrems era' (2016) I.D.P.L. 6(4), pp. 291-298.

5 Though there were of course many failed predictions of this kind – at the time of writing, we haven't colonised Mars, flying cars do not fill the city skylines, and aliens have not emerged from the outer space (probably due to the fear of being non-compliant with the GDPR).

6 See <https://www.biorxiv.org/content/early/2017/08/06/173021> (last accessed on October 12th, 2017).

7 See <http://science.sciencemag.org/content/356/6333/73> (last accessed on October 12th, 2017).

8 See <https://techcrunch.com/2017/04/19/facebook-brain-interface/> (last accessed on October 12th, 2017).

data protection matters. Conversely, while GDPR's degree of technological neutrality could be explored with multiple, as of yet fictional technologies (such as swapping bodies, teleporting, or uploading one's consciousness online), this article is focused on *Remember Me's* memory digitisation technology, which by itself provides a wide array of relevant legal challenges. The two adopted research aims are strongly intertwined, and lead the article to adopt the following structure. Section B describes in detail the game world's memory digitisation technology (called Sensen), as well as its applications in the city of Neo-Paris (where action takes place). Section C introduces the GDPR and analyses the first crucial challenges, which the Sensen technology would bring in front of this key legislative instrument. Section D concludes the article with a preliminary suggestion that digital memories could indeed be accommodated within the scope of the Regulation.

B. Sensen technology and the world of Remember Me

I. Introducing the world and the invention

8 Some of the readers who are less familiar with the state and variety of modern PC games might be asking themselves at this point, how is the author going to extract a sufficient amount of useful, relevant information from a PC game? After all, it is not a book, where information is laid out in written phrases, in an approachable format, ready to be used by researchers. The response to this concern is that many contemporary games, especially those with a role-playing component, developed a conceptual and storytelling depth which might be compared to that of the more conventional literary works. It suffices to mention that the script for Witcher 3 (a major role-playing PC game, winner of multiple Game of the Year awards) amounted to 450,000 words, roughly four times more than the average novel.[9] And given that the budget for gaming productions can reach truly colossal levels (Grand Theft Auto V's amounted to $250 millions[10]), one could expect that a sufficient part of this money reaches script writers, who are then able to create – for the relevant titles – worlds, stories, characters and dialogues of correspondingly high quality and robustness. Moreover, the interactive element of games might facilitate understanding certain concepts, from a different (not necessarily better, of course) angle than when they are presented in the books. *Remember Me* provides the player (or researcher) with a lot of material – not only through dialogues and general interactions with the denizens of Neo-Paris, but also through a range of Mnesists, "memory journals" found in-game, which provide ample information on the historical, technological, sociological and cultural background of the game world. As it will be shown, the game contains more than enough information for the purposes of this article, which relies on particular Mnesists as direct points of reference.[11]

9 Onto the storyline background - the year is 2084, in a bustling city of Neo-Paris,[12] which arose on the ruins of old Paris, destroyed during the war. The city revitalisation process progressed in parallel to the development and implementation of the Sensen - an invention based on a brain implant (connected directly to the spinal cord),[13] which isolates the human memories from the "hard drive" of the human brain and allows the user to perform a range of activities on his or her memories. First of all, the implant enables the *storage* of memories on external hard drives. Just like with normal digital files, a person can choose to store the copy of a memory, or move the original from the brain to the digital drive. Secondly, with Sensen, memories can be *shared* – either directly, between the two users, or by uploading a memory and sharing it through a network of choice. Thirdly, memories can be *erased* – a person may choose to isolate a specific memory and delete it, again, either directly from the brain or from the external hard drive. Finally, human memories can be *hacked* – while this possibility was not initially predicted by the Memorize corporation (in-game entity, whose main product is the Sensen implant),[14] the holes in Sensen's security were soon

9 See <https://www.pcgamesn.com/the-witcher-3-wild-hunt/the-script-for-the-witcher-3-has-over-over-450000-words-4x-larger-than-the-average-novel> (last accessed on October 12th, 2017).

10 See <http://www.ibtimes.com/gta-5-costs-265-million-develop-market-making-it-most-expensive-video-game-ever-produced-report> (last accessed on October 12th, 2017).

11 As not every reader wishing to consult the mnesists might have the time and will to look for them in the game, the following Wiki page gathers all in-game mnesists: <http://dontnodentertainment.wikia.com/wiki/List_of_Mnesist_Memories_in_Remember_Me> (last accessed on October 12th, 2017).

12 It is quite an interesting coincidence, that a game raising such potent matters of data protection was developed and located in France, a country with a very well-established data protection framework and a proactive approach, seen, for example, by requesting Google to implement nominative deindexing on a global scale – see the judgement in *Google Inc v CNIL* (2017) Conseil d'État, Section du contentieux, 10ème – 9ème ch. réunies, décision du 19 juillet 2017.

13 Mnesist – First Sensen Prototype. It has to be mentioned here that the game does not clarify whether each Sensen is connected to Internet/another central hub all the time – what would have very significant implications, including for data protection law and obligations.

14 Mnesist – Sensen 6: Response to the Memo Criminals.

discovered, allowing not only for the extraction, but also for *changing* or *remixing* the very content of human memories.

II. Sensen's applications

10 In the world of *Remember Me*, the technological possibilities outlined above have been realised in a myriad of ways. For the purpose of this section, they are divided on personal, commercial, state, and criminal uses.

11 Among the personal uses of Sensen by the citizens of Neo-Paris, three stand out in particular. The first and most popular one is backing up memories. A range of memory banks appeared, and their users may store memories there, for any future uses.[15] The second personal use, which was demonstrated in-game is sharing of memories, either between physically proximate users (e.g. family members, lovers, friends),[16] or with others, for example through the use of next-generation social networks. For the third and final example, some citizens embraced the practice of removing memories from their brains, as a way of reinventing themselves.[17]

12 The commercial applications of Sensen are quite evident in the world of *Remember Me*. Apart from the memory banks and next-generation social media platforms, the best example of a new business relying on memory digitisation are the operators of secondary markets for memories, where people can sell their own memories and buy those which were created in others' minds.[18] The most striking demonstration of this "commercialisation of memories" takes place when Nilin, the protagonist, is passing by a vending machine with memories and witnessing a man buy a memory of (someone else's!) first kiss, like a can of coke.

13 As the game plot centres on the Memorize corporation, there is comparatively less information on the use of Sensen technology by public bodies. However, the two examples which do appear in *Remember Me* are definitely noteworthy. The first one is tied to the prison authorities and the prison system *per se*. On arrival to La Bastille, Neo-Paris' main prison, the inmates are deprived of nearly all their memories – these are returned upon the completion of a sentence.[19] Apart from the punitive element, this is supposed to decrease the likelihood of escapes, the assumption being that someone who hardly knows who they are is unlikely to possess the will to attempt a break-out. The second use covered in this section is related to the military sector. According to one of the Mnesist journal entries, a practice emerged within the military, of wiping the traumatic memories from soldiers' brains in order to avoid Post-Traumatic Stress Disorder (PTSD). This process is supposed to have been automated and occur almost immediately, with a backup copy of the memory being nonetheless retained for later review by military officials.[20]

14 The final, potentially criminal dimension of Sensen's use (or misuse) is focused on hacking into the user's memories, for the purpose of extracting or changing them. This practice is the domain of freelancers, also known as the memory hunters – Nilin, the protagonist, being one of them.[21] On one occasion, she alters the memory of a dispute between a man and his wife, so that the man is convinced that he killed his wife at the end of the argument, which ultimately leads to his suicide.

15 These are the key uses of Sensen encountered during the course of the game; the scope of this technology's potential application is of course much wider. It is enough to mention the impact it could have on the sector of state and commercial surveillance and monitoring, making the PRISM system publicised by Edward Snowden[22] look like a harmless database of gherkin sales. Not to mention the revolution which Sensen would trigger within the sector of Big Data analytics.[23]

16 For the final point in this section, it is worth underlining how prevalent Sensen became in the world of *Remember Me*. Practically everyone has the implant plugged in, and those without it (either due to lack of funds or the will to embrace the Sensen) have virtually become second-class citizens.[24] An in-game Mnesist aptly compares this situation to that of social networks in the early 21st century;[25] and it could be added that the similar development might be currently occurring with regards to smartphones or digital literacy in general, for example within older age groups.

15 Mnesist – First Civilian Application.

16 Memorize commercial/game trailer - <https://www.youtube.com/watch?v=Aij7dNUHQ9M> (last accessed on October 12th, 2017).

17 Mnesist – First Civilian Application.

18 Mnesist – Globalization.

19 Mnesist – La Bastille.

20 Mnesist – First Military Application.

21 Mnesist – Hunt Glove.

22 See <http://www.bbc.co.uk/news/world-us-canada-23123964> (last accessed on October 12th, 2017).

23 A term denoting a high computing power-supported search for factual connections and patterns within large datasets.

24 Mnesist - Globalization of Sensen.

25 Mnesist - Globalization of Sensen.

C. General Data Protection Regulation applied to Sensen technology

17 Should the Sensen technology come to appear in the real, non-virtual world, it would certainly be capable of improving and positively revolutionising various aspects of human life. However, it would be similarly certain that such a development would carry a myriad of new regulatory challenges. Among them, those pertaining to the field of data protection would be one of the first ones begging for adequate, balanced, and comprehensive answers – can GDPR, in its current state, be seen as capable of providing those? How far is this instrument "technology-neutral" – as the regulatory keyword goes – towards the new formats of information that may contain personal data?

18 In order to fully answer these questions, a wide array of challenging, demanding research inquiries would have to be conducted. This paper approaches the questions which would arguably have to be answered first – the ones concerning the classification of Sensen memories as personal and/or sensitive data within the definitions of arts. 4 and 9, respectively, of the GDPR. The said definitions stand as gateways to the realm of rights and obligations aiming to protect the (personal) data subjects. Rights such as the right of access to information (art. 15), the right to rectification (art. 16), or the right to erasure (art. 17), data processing obligations based on principles established in art. 6, would, together with all other relevant provisions, be enabled only if the digitised memories were to be found as lying within the definition of art. 4, and in case of certain stronger protection measures, within that of art. 9. GDPR's veil of protection against the negative consequences of Sensen uses described above (such as inadequate commercialisation of data, or novel security threats, to mention the very first few) would hinge on those preliminary questions – hence, it is most fitting to dedicate this article to such a path of inquiry.[26]

19 One additional disclaimer has to be made; while considering the indicated definitions from the perspective of secondary "memory subjects" (ie. those who appear in someone else's memories) would be a very interesting endeavour, this article – due to its exploratory character – focuses its analysis on the primary memory subjects, that is those whose brain created the later digitised memory.

26 This is without denying that multiple subsequent legal dilemmas would be requiring academic attention, such as the application of the domestic purposes exception, set out in art. 2(c) of the GDPR, (as supported by rec. 18), the distinction between the "right to be forgotten" and the "right to forget yourself in the context of Sensen, and the shape of exemptions for detecting and preventing crime.

I. Digitised memories as personal data

20 The preliminary question approached by this paper is whether digitised memories, as presented in the world of *Remember Me*, could be classified as personal data at all. Art. 4(1) of the Regulation defines the latter concept as "any information relating to an identified or identifiable natural person". The notion of identifiability is of key importance in this sentence, and hence, it is necessary to consider whether a human memory could be seen as being related to an identified or identifiable individual. According to recital 26 of the GDPR, when considering this matter, "account should be taken of *all the means reasonably likely to be used*,[27] such as singling out, either by the controller or by another person to identify the natural person directly or indirectly." While the definition emerging from art. 4(1) and recital 26 is a broad and open one, the first provision offers a list made of two groups of factors which, if present, would tip the scale towards the fulfilment of the discussed criterion.

21 The first group of factors contains specific forms of identification, starting with the individual's name. A Sensen memory file, which would be labelled with such a name would pass the test in a straight-forward manner. However, if such a label would be missing or adequately anonymised, the more interesting dimension of this inquiry begins. The content of the memory itself could contain an individual's name – the memory might include someone hearing his name spoken, it might include someone typing his name into an online form, it might even include someone *thinking* his name, or being sufficiently conscious of it, so that an external party accessing this memory through their Sensen could tell that it is a memory of someone bearing the name in question.

22 The second factor from the first group is an identification number. Like an individual's name, it could appear as a label attached to the memory file; but it could also appear within the memory itself. For example, this could be a memory of someone completing their tax paperwork, or looking at their ID or driving licence when perusing through their wallet. However, there would arguably be a lower presumed chance of such presence than in the case of an individual's name, which is more often found in everyday, casual use.

27 (Emphasis added). The recital offers further guidance with regards to the reasonability criteria in this sentence - "To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments". GDPR, supra fn. 2, rec. 26.

23 The next factor indicated in the provision is location data. Apart from metadata,[28] which could be tied to the memory (e.g. which brick and mortar memory bank was used to deposit the memory), the potential for identifying an individual by location-related information present in the memory can be seen as particularly high, even when we merely consider the visual dimension. Seeing one's home, place of work, or favourite pub can already give a good indication of who the person is – and if that information is combined with additional sources of data; for example, land registries or direct inquiries, the probability is quite high indeed. Certainly, it is possible to imagine a memory of someone in a locked, indistinctive room, staring at a blank wall, not thinking about anything; but this would in all likelihood be an exception.

24 The last identifier from the first group of factors is an "online identifier". Apart from labels, such as a next generation social media account name, or a memory bank account name, there would be a low, yet possible likelihood of this criterion being fulfilled – imagine someone's memory of playing an online game, which requires creating a dedicated account or a virtual character, imagine this person looking at his character's/account's name, receiving chat messages addressed to his online name. Out of the four factors from the first group, it seems plausible to state that name and location data would most likely be present in memory files, followed by online identifiers, and, finally, identification numbers. Of course, this is an estimate based on the idea of information present in an average person's memories – there could very well exist individuals escaping this prediction due to the uniqueness of certain aspects of their lives.

25 The second group of factors indicated in art. 4(1) is less focused on specific forms of identification, and more on various broader aspects of one's identity. The first such aspect which, if present, can serve as a factor turning a piece of information into personal data is labelled as physical identity. Setting aside any supplementary descriptions of a memory file (e.g. "memory of a male, height - 185 cm, weight - 80kg"), its content would almost always disclose information of the discussed kind. Firstly, it could be due to visual information – imagine someone looking at himself/herself in a mirror, looking at their own hands while doing something, or looking at their clothes in the morning. Such a mode of identification could be seen as supported by Article 29 Working Party's *Opinion 02/2012 on facial recognition in online and mobile services*, which stated that "when a digital image contains an individual's face which is clearly visible and allows for that individual to be identified it would be considered personal data".[29] The Opinion indicates that several parameters ought to be considered in order to verify whether data falls within such a case, such as quality of the image, or the use of a particular viewpoint[30] – factors that could very well be applied to digitised memories. However, the non-visual factors present in this new medium could also be quite informative for the discussed purpose, in a manner thus far unknown to personal data definitions. Consider an individual "playing" someone else's memory in their own Sensen; the former person would be able to hear the tone of the latter's voice, feel one's smell, feel the recorded individual's weight etc.

26 The next factor in this set is physiological identity. The Oxford Dictionary defines the term "physiological" as "relating to the branch of biology that deals with the normal functions of living organisms and their parts".[31] Taking this into account, a Sensen memory could potentially reveal quite a lot about an individual's living functions and physiological conditions. Setting aside the obvious scenarios, such as a memory of a cold or a visit to a doctor, a memory could contain a set of factors (e.g. specific cough, the feeling of slight nausea, specific texture of the tongue) which, if examined by a medical professional, could point (for example) to a specific medical condition suffered by an individual.

27 Following physiological identity, art. 4(1) moves on to elevate one's genetic identity in a similar fashion. Definition of genetic data from art. 4(13), as complemented by recital 34 of the Regulation, is that of "personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question".[32] Assuming that the Sensen tech would allow for the digitisation of memories without the inclusion of any biological material from the brain, such memories would not automatically point towards the genetic identity criteria. As for the content of memories, in contrast to many instances previously discussed in this section, it would most likely be exceedingly difficult to find memories containing genetic data.

28 Metadata can be defined as secondary data, describing another set of data.

29 Article 29 Data Protection Working Party, *Opinion 02/2012 of the on facial recognition in online and mobile services* (2012) 00727/12/EN, WP 192, at p. 4. The Working Party is an influential advisory body which "provides the European Commission with independent advice on data protection matters and helps in the development of harmonised policies for data protection in the EU Member States" (see <https://edps.europa.eu/data-protection/data-protection/glossary/a_en>).

30 *Opinion 02/2012*, supra fn. 30, at p. 4.

31 See <https://en.oxforddictionaries.com/definition/physiological> (last accessed on October 12th, 2017).

32 GDPR, supra fn. 2, rec. 34.

28 Moving forward, mental identity is indicated as another possible path to the realm of personal data. Digital memories would be extremely likely to contain such information, almost always offering a unique insight into one's mental state and identity. Private journals and video logs would pale in comparison.

29 Economic identity, another example from the provision, would similarly be very likely to be revealed by one's digitised memories. What one is wearing in the memory, what belongings he/she has in his/her house, what car one is driving, how much money does one have in his or her bank accounts etc. All those factors would likely reveal a lot about one's economic status and perspectives. Of course, there could be memories which are devoid of such information; imagine a millionaire swimming in a communal swimming pool, not thinking about his possessions and financial standing, and not wearing swimming shorts made by Armani with Swarovski crystals. Nevertheless, the chances of at least some relevant information being contained in an average digitised memory would be quite high.

30 The two final indicated factors are a person's cultural and social identity – for the purposes of this section, it is possible to consider them in one paragraph. Both would have a good chance of being conveyed by a Sensen memory. Apart from visual representations, such as clothing (think about the memory subject wearing a Jewish kippah or a t-shirt with one's favourite rock band logo on it), the memory could include someone going to work, church, a music concert, and other places holding the potential to reveal one's cultural and/or social identity.

31 One of the key thoughts emerging from the analysis conducted in this section is that if the content of memories was to be considered in deciding whether a digitised memory constitutes personal data, whether it is in fact a piece of information relating to an identified or identifiable natural person, there would be a tremendous amount of different possibilities, tipping the art. 4(1) scales in one direction or another. With Sensen memories, the context, or rather content of a memory could be extremely important, as it was shown above. After all, human memories can be as diverse as human life itself.

32 Nevertheless, the argument put forth in this article is that due to the very high probability of at least some aspects of the art. 4(1) test being fulfilled – most notably with regards to the individual's name and location data, as well as physical and mental identity – digitised memories *should be* regarded as personal data, *without* the need for an evaluative inquiry of the memory's content. Difficulties with the information vs. medium dichotomy are not unprecedented in the field of data protection law – following Bygrave, "as biological material is increasingly mined for information, justifying a distinction between the former and the latter – that is between the medium and the message – becomes more difficult".[33] The functional approach, guided by the need to provide adequate protection to Sensen memories' data subjects, justifies in this particular case focusing art. 4(1) on the medium, instead of the message – and the CJEU decision in case C-582/14, *Breyer* could be seen as supporting this conclusion. In the cited judgement, an IP address (whether dynamic or static) was found to constitute personal data[34] – variables such as which websites was the individual browsing with the IP address at hand had no impact on the indicated finding. Adopting such an approach in relation to Sensen could, among multiple others, oblige the data controllers to implement special technological and procedural safeguards to memory repositories, without the need to confirm first that each hosted memory does in fact contain personal data. Additionally, an evaluative inquiry of the memories' contents would itself present additional concerns tied not only to the efficiency of the legal framework, but also to the right to data protection and the right to privacy. In contrast to (for example) video files, digitised memories would be almost certain to carry some form of a personal stamp of the kind matching those listed in article 4(1).

33 There is, however, a potential challenge to the reasoning of the preceding paragraph. What if the memory in question is fake? What if it was e.g. altered by one of the memory hunters? Even worse, what if an individual does not know that his memory was altered, or maybe he unknowingly bought a fake memory at a vending machine akin to those in Neo-Paris, and with time started to treat it as his own, merged it with his other, own, pure memories? Additionally, what about the practice of covering up one's personal data (e.g. in order to avoid digital surveillance), well described in Brunton and Nissenbaum's book *Obfuscation: A User's Guide for Privacy and Protest*?[35] It is possible to imagine wary citizens altering the copies of their memories stored in a memory bank or uploaded to a dedicated social network. Would all those kinds of memories still qualify as personal data even if the factual connection would be false?

34 In order to answer this question, it is worth reaching back to the fundamental aims of data protection law, and contrasting them with those of the law of defamation. In the latter branch of law, truthfulness of information plays a key role – in

33 Bygrave, supra fn. 4, at p. 126.

34 Case C-582/14 *Breyer v Germany* (2016), at para [49].

35 Brunton F and Nissenbaum H, *Obfuscation: A User's Guide for Privacy and Protest* (2015) MIT Press.

the UK, for example, truth is a defence to a claim in defamation.[36] This is because the regulatory goal at hand is protecting the citizens' reputation from being tarnished by false statements; and if a statement made about someone is true, their legally perceived reputation is not harmed.[37] The situation is different with data protection law. It is aimed at protecting the data subjects from harm, which might be inflicted as a result of other people accessing and using the former's personal data. Data protection law is principally not concerned with the truthfulness of information – in order to fall within the GDPR's scope, it is sufficient for information to "relat(e) to an identified or identifiable natural person".[38] Hence, there is a strong argument to consider the indicated examples of fake/remixed Sensen memories as personal data. Such an approach can be supported by a comparison to the phenomenon of the so-called "fake nudes", based on spreading falsified nude pictures of celebrities, where e.g. an actor's face is Photoshopped onto a naked body.[39] In such a scenario, the information is clearly false – however, he/she is clearly identifiable from the picture, and deserves the protection of measures bestowed by the GDPR. Even if we take into account the sophisticated obfuscation measures, with data subjects anonymising their memories before uploading them online, such persons should not be losing the shield of data protection, especially given the fact that it would be extremely difficult to ascertain that a memory has been *actually* cleared of any indicators of personal data.

35 While the issue of straight-forward "truthfulness" of Sensen memories could be solved in the manner outlined, it should be acknowledged that the emergence of fake memories could potentially undermine our understanding of *identity* and its presumed integrity, with potential consequences for the notion of *identifiability*. Consider the earlier mentioned possibility of someone purchasing another's memory and then appropriating it, starting to perceive it as his own. If that memory is then shared further, for example on an online repository, will it be identifying the source person (in whose brain the memory was created) or the purchasing person, due to e.g. being changed/personalised in the latter's mind? Will it identify both at the same time? *Remember Me* does not suggest an answer here, and much more importantly, it is not known how such a situation would play out in the real world, should the memory digitisation technology come to appear. One could hope that criminalisation of involuntary memory alterations, coupled with a way to somehow "watermark" the externally obtained memories could help in mitigating the risk of such conundrums arising. However, it is very much possible that aside from the technological experts and IT lawyers, the regulators would have to also turn towards the philosophers exploring the theories of essentialist and constructive identity in a novel and very challenging setting.

36 Without doubt, the emergence of various forms of fake/swapped memories described above could bring a host of considerable problems in front of the regulators, extending far beyond data protection law. However, even if the scenario from the end of the previous paragraph is taken into account as a potential, currently unsolved dilemma, it still seems that analysing the *content* of memories for uniquely identifying information or for truthfulness, as a preliminary condition to classify them as personal data, would most likely be disproportionate, inefficient, and against the main aim of data protection law.

II. Digitised memories as sensitive data

37 Assuming that the conclusions of the previous section are embraced, and digitised memories are found to be personal data *per se* within the meaning of article 4(1), a predictable, subsequent question appears – should such memories be treated as one of the categories of "sensitive" or "special" data, warranting additional protection? In order to answer this question, this section must turn towards article 9 of the GDPR.[40]

38 Article 9 of the Regulation prohibits (subject to several, important exceptions – most notably, consent)[41] the processing of certain types of personal data which, as recital 51 explains, merit special protection due to the significant risks they might pose to data subjects' fundamental rights and freedoms, and risks corresponding to the processing of such data. Article 9 sets out seven categories of the described data, in a closed list - as in section C.I of this paper, it is worth considering Sensen memories in the context of each category. The first of the seven is data which reveals the data subject's

36 See section 2 of the Defamation Act 2013 c. 26.

37 See *McPherson v Daniels* (1829)10 B. & C. 263, at 272.

38 Art.4(1) of the GDPR.

39 See <http://theconversation.com/celebrity-fakes-where-porn-meets-a-sense-of-possession-20829> (last accessed on October 12th, 2017).

40 Art. 10, focused on processing of personal data relating to criminal convictions and offences, would be relevant in this context as well, but for the purpose of this exploratory article, only art. 9 is considered, due to the variety of data categories it contains.

41 GDPR, supra fn. 2, art. 9(2)(a). Again, considering the application of art. 9(2) exceptions to Sensen memories would be a most worthy endeavour, one which unfortunately does not lie in the scope of this article.

racial or ethnic origin. It is fairly easy to imagine how nearly every memory would include information disclosing one's racial origin – the sight of one's hands is a perfect example. Ethnic origin could be slightly less straight-forward, but also very probable, being communicated through one's clothing, accent, as well as thoughts and conversations.

39 The second path to the "special category of data" status leads through personal data revealing one's political opinions. It seems quite likely that Sensen memories could hold the records of conversations on political matters, especially due to the fact that this term is not limited to e.g. the critique of political parties, but can be seen as including any matters "associated with the governance of a country or area",[42] or even of a group within the society. In our daily lives, such conversations tend to weave their way in, wherever we go. It might of course happen that a person successfully avoids any political conversations – however, this is where Sensen creates a unique possibility of the discussed disclosure occurring nevertheless. By providing an insight into one's mind, this technology could reveal the data subject's conscious and subconscious reactions to certain overheard conversations and even witnessed events. By way of example, imagine someone looking at a damaged road and cursing silently at the lack of action from the city council – this could then be seen as a political opinion.

40 The third category is that of data revealing an individual's religious or philosophical beliefs. Sensen memories would have a good chance of containing such information, in a similar manner to cultural and social identity, as discussed in section C.I above. This reasoning can be seen as further supported by the Art. 29 Working Party's *Opinion 02/2012 on facial recognition in online and mobile services*, which stated that if digital images "are going to be used to obtain ethnic origin, religion or health information", then they are to be treated as a special category of personal/sensitive data.[43] Sensen memories could be seen as capable of containing, in a way, such digital images. However, the context of religious and philosophical beliefs demonstrates particularly well how a more direct and unprecedented path to disclosure could be found with the Memorize corporation's technology. Imagine someone praying in a church: the memory of this event – upon being loaded into another person's Sensen – could show that the person does not believe in the words he or she recites. Or for another example, consider a memory of a parent lecturing his or her child that they should not have hit the boy who was bullying them, while thinking "well done kid, that'll teach him". While social and cultural identity could also be disclosed in this intrinsic manner, the context of religious or philosophical beliefs is arguably more often tied to the individual's inner thoughts.

41 Next, art. 9 prohibits the processing of personal data revealing an individual's affiliation to a trade union. In contrast to the previous three, this special category of data would be rather unlikely to be found within the digital memories, unless a person would be, for example, a very active trade union member.

42 The fifth category is one concerned with the processing of genetic or biometric data with a purpose of "uniquely identifying" a natural person. This term indicates the identification of a specific person, not as a member of a group, but as e.g. Mr. John Smith. Considering genetic data in this context first – as it was argued in section C.I above, it is rather unlikely that Sensen memories would include genetic data as understood within the Regulation. In order to see whether the same would be likely for biometric data, it is necessary to turn towards the definition of such data, laid out in art. 4(14) of the Regulation. By virtue of this provision, biometric data is "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person" – characteristics which have to allow for or confirm the unique identification of that person. Examples indicated in the text of this provision are facial images and dactyloscopic data.

43 There is a very strong argument in favour of seeing Sensen memories as likely carriers of biometric data, much in the same manner as they are likely to carry data about one's physical and physiological identity (as it was discussed in section C.I above). "Specific technical processing" (as present in art. 4(14) of the Regulation) could be found in the very process of memory digitisation. Unique identification could be based on, again, the memory of someone looking in a mirror, but also on an external party knowing the data subject very well and being able to piece together various physical and psychological details appearing in the memory, to become certain that this is a memory of one specific individual. This piece-together approach could be particularly true with regards to the third listed subtype of biometric data, that is behavioural characteristics. While two people's memories of a similar event (e.g. getting on a bus) might seem almost the same, they are likely to be riddled with small, sometimes unnoticeable details, which can add up to a unique pattern of behaviour, readable by someone with the right knowledge and/or technology. Indirect support for this line of interpretation can be found in the Art. 29 Working Party's *Opinion 8/2014 on the Recent Developments on the Internet of Things*, which stated that data originating from devices belonging to the

42 See <https://en.oxforddictionaries.com/definition/political> (last accessed on October 12th, 2017).

43 *Opinion 02/2012*, supra fn. 30, at p. 4.

"Internet of Things" category "may allow discerning the life pattern of a specific individual or family – e.g. [through] data generated by the centralised control of lighting, heating, ventilation and air conditioning".[44] Sensen memories could be used to a similar end.

44 The next special category of data set out in art. 9 of the GDPR is data concerning health. When discussing physiological data, section C.I of this article demonstrated how deeply and uniquely the Sensen technology could, on multiple occasions, convey information about one's medical conditions. To reiterate: it could be possible to discover the relevant memories of events which occurred in public (e.g. someone coughing during a garden party), to uncover facts kept hidden by the data subject (e.g. a cancer diagnosis), and finally, to analyse memories containing medical information about which the data subject has no idea – but which could be uncovered by a medical professional or an appropriate algorithm, or both combined. A comparison can be made here to so-called Quantified Self devices, measuring numbers we generate through our daily activities (e.g. calories consumed, mood state data, blood oxygen levels, steps taken etc.). The earlier mentioned *Opinion 8/2014* of the Art. 29 Working Party noted that such devices "are mostly registering data relating to the well-being of the individual".[45] While this is not seen by the Opinion as "health data" *per se*, it "may quickly provide information about the individual's health as the data is registered in time, thus making it possible to derive inferences from its variability over a given period".[46] This reasoning could very well be embraced in the context of Memorize's technology.

45 The final category of data covered by art. 9 is data about a natural person's sex life or sexual orientation. Akin to many previous subtypes of data covered in this section, it could also be seen as likely to appear within the digitised memories, on multiple, progressively deeper levels. First, one's memories could contain representations, verbal or in writing, made by that person with regards to his or her sexual preferences. Then, a person's memory could contain details of private, even secret life – examples being memories of sexual intercourse or browsing of adult content online. Finally, memories could contain inner thoughts and physiological reactions which the person might not even be aware of or interpret as tied to sexual preferences or orientation.

46 Therefore, we may return to the key question underlying this section – should Sensen memories be seen as sensitive data? The answer proposed by this paper is a definite yes. In a similar manner to conclusions drawn in section C.I, the key reasoning underlying the proposed stance is based on the high likelihood of multiple special categories of data being encountered within the digitised memories – most notably data revealing racial and ethnic identity, biometric data uniquely identifying natural persons, data concerning health, as well as data revealing a person's sex life or orientation. Sprokkereef, when writing about a similar dilemma in the field of novel forms of biometric data, stated that "(...) it is not clear if the algorithms and machine-readable templates that contain the information are always to be considered as sensitive personal data".[47] Taking the earlier described functional approach, based on the need to offer adequate protection to data subjects, suggests that Sensen memories could and most likely *should* be elevated to the sensitive data status. To make another comparison – Art. 29 Working Party's *Opinion 5/2009 on online social networking* aptly stated that it "does not consider images on the Internet to be sensitive data, unless the images are clearly used to reveal sensitive data about individuals."[48] Sensen memories would deserve to be treated in the opposite manner, due to the overwhelming and highly concerning number of art. 9 special data categories, which could materialise in this new medium of information, giving unprecedented and unique degree of insight to parties loading the data subject's memory into their Sensen. While DNA could be seen as a blueprint for one's body (one containing health data or revealing racial or ethnic origin, as the Art. 29 Working Party's *Opinion 3/2012* noted[49]), Sensen memories could be seen as a blueprint for one's soul, thus requiring commensurate protection.

D. Conclusion

47 In the UK trailer for *Remember Me*, Nilin (the game's protagonist) puts forward a quote "the memory of a single man is a fortress, more complex than the vastest of cities."[50] If it ever comes to this, deciding on who should be granted the keys to this fortress, and what kinds of keys, should be a well thought-through exercise, oriented towards finding the

44 Article 29 Data Protection Working Party, *Opinion 8/2014 on the Recent Developments on the Internet of Things*, at p. 10.

45 *Opinion 8/2014*, supra fn. 47, at p. 17.

46 *Opinion 8/2014*, supra fn. 47, at p. 17.

47 Sprokkereef A and de Hert P, 'Biometrics, Privacy and Agency' (2012) in Mordini E and Tzovaras D (eds), *Second Generation Biometrics: The Ethical, Legal and Social Context* (Springer), at p. 92.

48 Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, at p. 8.

49 Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, at p. 15.

50 See <https://www.youtube.com/watch?v=FMyQlnnxXuk> (last accessed on October 12th, 2017).

adequate balance between the socially beneficial uses of the Sensen technology and safeguarding the data (memory) subjects' rights. Recognising the digital memories as sensitive data, regardless of their content, would be a sensible starting point towards finding the said balance in the effort to accommodate the Sensen technology within the European data protection framework.

48 At this very initial analytical point, it seems that the GDPR's definitions of personal and sensitive data are sufficiently technology-neutral to accommodate the concept of digital memories. It seems that the EU legislators' intention to construe the definitions of personal data broadly, as demonstrated by Bygrave,[51] could withstand the challenge brought by Memorize's technology – though not without an analytical struggle, as the discussion of fake memories in section C.I demonstrated. Perhaps, the Regulation's rights and obligations tied to personal and sensitive data would be able to provide an adequate shield against the potential harm to data subjects, while respecting the other stakeholders' interests. For now, this diverse path of inquiry remains to be explored – but given the earlier mentioned scientific developments, the need for further exploration of the GDPR's ability to respond to memory digitisation technologies might become more urgent than we consider it to be.

Acknowledgements

The author would like to express his sincere thanks to Dr David Erdos (University of Cambridge), Jef Ausloos (KU Leuven), Grzegorz Michalak and Paweł Przygucki, for their insightful, helpful and encouraging comments on the draft of this article. Thanks are also owed to the anonymous peer reviewer(s), for the valuable, meaningful and challenging comments, embracing the unconventional research aim(s) of this piece. The article was created within the Human Rights, Big Data and Technology project, supported by the Economic and Social Research Council [grant number ES/M010236/1].

51 Bygrave, supra fn. 4, at p. 127.