

"MEMORY" PRODUCTION

Findings and Policy Recommendations on the Production of MAC

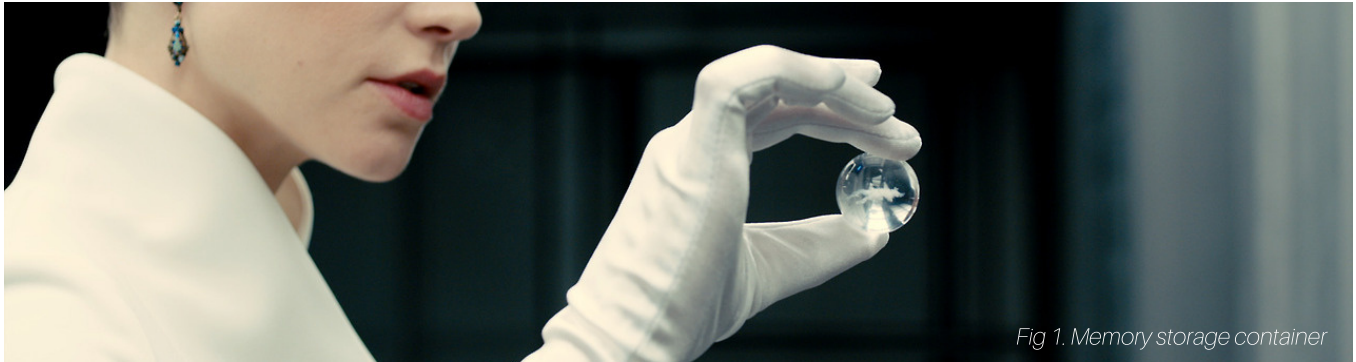


Fig 1. Memory storage container

Names of researchers redacted

Project funded by the NTFORP Congressional Committee

DECEMBER 2037

Addressed to the National Task Force on Replicant Production (NTFORP),

We are pleased to provide this report on our findings regarding the Memory as Commodity (MAC) replicant technology. Our research included analysis of data practices from the Tyrell and Wallace (T&W) corporations, and interviews with private individuals who used products from these companies. The suspicions of the task force proved to be true, as we found evidence of dubious practices being conducted by T&W in the production of MAC.

To briefly describe MAC to incoming members of the committee, MAC is a product consisting of memory as data. MAC is both extracted and constructed - extracted from personal human data, and constructed as an imitation of human memory.

MAC will be used in the production of replicants- otherwise known as humanoid AI, which are coming to market in the near future. Replicants can only imitate their human predecessors with these packages of complex digitized memories.

As the task force foresaw, we were unable to gain full access to the memory construction technologies of T&W, and instead focused our study primarily on the area of memory extraction.

SUMMARY OF FINDINGS

- PRODUCTION OF MAC IS EXPLOITATIVE IN ITS USE OF PERSONAL DATA
- TRADEOFFS EXIST BETWEEN CORPORATE INTEREST, INDIVIDUAL GOOD, AND TECHNOLOGICAL INNOVATION
- RECOMMENDED APPROACH: **LET TRENDS CARRY ON, CONTINUE MONITORING DEVELOPMENT OF MAC AND REPLICANT TECHNOLOGY**

STAKEHOLDERS IN STUDY

CORPORATIONS PRODUCING REPLICANTS (TYRELL AND WALLACE)

SUPPLIERS OF MAC PRODUCTS

NATIONAL TASK FORCE ON REPLICANT PRODUCTION (NTFORP)

INDIRECT: PRIVATE INDIVIDUALS AND CORPORATE STAKEHOLDERS

Problems with MAC Production

Per the contract brief, this report will stay away from the moral discussion of memory, and instead focus on how MAC is produced - particularly where the data informing MAC come from.

The Tyrell and Wallace corporations (T&W) are subjects of interest in this study. We discovered that in the past, preceding companies such as Alphabet and Meta pioneered the practices of collecting and monetizing mass user data. These two companies were immensely powerful in their heyday, and their access to capital directly funded the development of replicant technology.

Alphabet and Meta were large conglomerates that offered free access to services in exchange for personal information provided by their users. This data was immensely valuable as it could be sold and analyzed by advertisers to sell goods and services to those same individuals (Esteve 39). T&W operate in a similar way, however, in addition to these practices, they are also packaging this data in the form of MAC.

In our interviews with 300 users of T&W products, we found that the producers of MAC intrusively monitored and extracted information without participants full and informed consent. T&W both offer a wide range of digital products, from personal productivity devices to augmented reality companions. We found that while users gave their consent to having their interactions recorded, they were unaware of the extent of data being produced, stored, and how it was being used. 48% of interviewees simply believed T&W used the data to improve their own software and services. We found that this lack of transparency on the data practices of these companies to be very concerning.

Most participants stated that they would continue to use products by T&W despite learning about these problems. Many cited convenience and dependency on T&W goods and services that they could not give up.

FINDINGS

- OF 300 INDIVIDUALS INTERVIEWED, 76% WERE UNAWARE OF THE SCOPE OF T&W'S DATA USE
- 47% THOUGHT T&W ONLY USED THEIR DATA FOR IMPROVING T&W SERVICES
- 61% DID NOT KNOW THEIR DATA WAS BEING SOLD TO THIRD PARTIES
- 78% WOULD RETRACT THEIR CONSENT OF ACCESS TO THEIR DATA IF THEY HAD THE OPTION TO
- 86% STATED THAT THEY WOULD CONTINUE TO USE T&W GOODS AND SERVICES DESPITE LEARNING ABOUT PRIVACY ABUSES

Contradictory Evidence:

Representatives of T&W provided evidence of consent from their combined 4.3 billion users with data logs that identified when each individual user consented to allowing T&W to use their information for any purpose. They argued that their monitoring practices were not in fact intrusive, but necessary for the products to function.

During the course of our study, resource and legislative limitations prevented us from examining firsthand how T&W used the data they collected. But it is clear that a grey area in monitoring exists between the handover of data from T&W to MAC producers.



Value Tensions and Implications for Policy

The key value tensions in the conversation on regulating MAC include: data minimisation versus data maximization, and data privacy versus benefits of AI (Kuner et al 290-291).

These tensions are intertwined. Private individuals benefit from data minimisation (GDPR 5(1)(c)), but potentially at the cost of the benefits of AI (Norwegian Data Protection Agency 4). Private individuals are harmed by data maximization practices but the social benefits of AI are optimized (Mayer-Schönberger 52).

Previous state of policy:

While data policy was still in its infancy before the Blackout, governments around the world were on the right path.

In the USA, California implemented the California Consumer Privacy Act (CCPA) in 2018, four years before the Blackout. This policy was very comprehensive in protecting the privacy rights of consumers in California:

1. The right to know about the personal information a business collects about them and how it is used and shared;
2. The right to delete personal information collected from them (with some exceptions);
3. The right to opt-out of the sale of their personal information; and
4. The right to non-discrimination for exercising their CCPA rights.

In the decade and a half since the Blackout, a policy regime as rigorous in protecting the consumer as the CCPA has yet to be re-established in America.

Pre-Blackout, the European Union implemented boundaries around data usage: "[Personal data] must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed ('data minimisation')" (GDPR article 5(1)(c)).

Kuner et al found that the practice of placing limits on data retention had the consequence of "potentially strip[ping] organizations and society of the benefits of using that data for AI development, deployment, and oversight" (290).

A tertiary implication for policy for the Task Force to consider is the risk of disrupting economic activity in America.

One of the NTFORP's key mandates is to prevent the loss of market capitalization on the novel economy of replicant technology, which is expected to be valued at 50 trillion dollars by the mid-century. If possible, loss of suppliers in the chain of production should be prevented, and domestic economic activity encouraged.

Corporate scholar Svetlana Kamyshanka recommends putting the onus on corporations to "understand and minimize any negative impacts of AI" (7), which is another possible avenue for the task force to consider.

ALTERNATIVE OPTIONS

a1: Companies pay consumers in exchange for the data extracted from the consumers usage of the company's technologies

a2: In addition to existing products, data companies must sell a new tier of privacy focused products to a standard set by the NTFORP

a3. Increase pressure on companies to disclose memory (data) extraction practices

a4. Let present trends continue while monitoring the situation around MAC and replicant production

Criteria for evaluating outcomes:

c1. National capitalization of replicant market in dollar terms (more capitalization is better)

c2. Private individual's approval of business data practices (higher approval of practices is better)

c3. Technological innovation that improves the quality of life for Americans

How outcomes should be evaluated:

- First, c1 allows the NTFORP to measure the success of national market capitalization. The measure considers the realized market capitalization versus unrealized potential

- The second criteria, c2, gauges public approval of industry practices

- Lastly, c3 is the most speculative and most difficult to measure. The NTFORP's mandate is to facilitate the innovation of American technology to better the living standards of its citizens. But at what cost?

Tensions and Tradeoffs

The NTFORP has the unique and difficult position of promoting corporate goodwill while considering the perspective of the everyday citizen.

The first alternative, a1, is a monetary penalty, and is not likely to bode well with industry and their stakeholders. Implementing such a policy may deter companies from conducting business stateside, and national market capitalization goals may not be reached (c1). This may lead to diminished technological development (c3) and may not necessarily improve the approval of corporate data practices from individuals (c2).

The second alternative (a2) is a call to companies to produce a new tier of privacy-focused consumer products that have limited data extracting capabilities. This will create a new space in the market, thus driving further market capitalization (c1) and technological innovation (c3). This also benefits the consumer by giving them more options (c2), although in the long term data protection for all people will diminish and likely become unequal and classist.

Tensions and Tradeoffs cont.

The third alternative (a3) proposes more transparency from companies on their data handling practices. This practice would not necessarily hurt corporate interest if they do not have anything to hide (c1). Private individuals would benefit from such an agreement (c2). Technological innovation could possibly face resistance given the constraints of regulation (c3).

The fourth alternative (a4) is to let present trends carry on and to continue monitoring how the situation involving MAC and replicants develops. This alternative would give the NTFORP more time to assess the replicant landscape before making any drastic decisions that could affect the ability of companies to maximize their market capitalization (c1) and disrupt the pace of innovation at this stage of replicant development (c3). Approval of private individuals would neither increase nor decrease in this case (c2).

REFERENCES

"Art. 5 GDPR Principles relating to processing of personal data." *GDPR*, <https://gdpr-info.eu/art-5-gdpr/>

"Blackout" *Blade Runner Wiki*, <https://bladerunner.fandom.com/wiki/Blackout>

Blade Runner. Directed by Ridley Scott, performances by Harrison Ford, Rutger Hauer, Sean Young, Warner Brothers, 1982.

Blade Runner 2049. Directed by Denis Villeneuve, performances by Harrison Ford, Ryan Gosling, Ana de Armas, Warner Brothers, 2017.

"California Consumer Privacy Act (CCPA)" *State of California Department of Justice*, <https://oag.ca.gov/privacy/ccpa>

Datatilsynet. "Artificial intelligence and privacy." The Norwegian Data Protection Authority, Jan. 2018. <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>

Call to Action

MAC is the keystone to realizing the potential of the replicant program. It represents the heart, soul, and mind of a new sort of intelligence.

As such, the actions of the Task Force in overseeing the next steps in its implementation will have consequences of a vast and systemic nature. We suggest a plan that considers the perspectives of all shareholders that mitigates consequences and amplifies success for all.

According to our criteria, **our recommendation is to let present trends continue (a4)**. Currently, the Replicant project is on the cusp of a major breakthrough: from a technological perspective it will revolutionize life, and from an economic perspective it will produce great returns for Tyrell and Wallace, and by extension this nation.

For these reasons, some may believe the benefits of MAC and replicant technology outweigh the importance of data protection. We are hopeful that what proceeds from here will diverge from the legacies of former conglomerates in the lack of transparency on user data, and it is up to the NTFORP to decide who this responsibility rests on. **We encourage increased monitoring on these companies' specific implementations of memory collection (a4)** to stay in step with the industry. An implementation of this policy should include an increase in resources to investigate these companies to this end.

REFERENCES CONT.

Esteve, Asunción. "The business of personal data: Google, Facebook, and privacy issues in the EU and the USA." *International Data Privacy Law*, vol. 7, iss. 1, Feb. 2017, pp. 36-47.

Kamyshanka, Svetlana. "AI and Data Privacy: Managing Risk in the Boardroom." *Board Leadership*, Mar./Apr. Issue, 2021, pp. 6-7.

Kuner, Christopher. "Expanding the Artificial Intelligence-Data Protection Debate." Editorial. *International Data Privacy Law*, vol. 8, no. 4, 2018, pp. 289-92.

Mayer-Shonberger, Viktor, and Ramge, Thomas. "A Big Choice for Big Tech: Share Data or Suffer the Consequences." *Foreign Affairs*, Sep/Oct, 2018, www.foreignaffairs.com/articles/world/2018-08-13/big-choice-big-tech.

Data Protection Act and General Data Protection Regulation. "Big data, artificial intelligence, machine learning and data protection." *UK Information Commissioner's office*, Sep. 2017, <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>



Fig. 2 Holographic AI



Fig. 3 Replicant Prototype



Fig. 4 Holographic Image Data



Fig. 5 Memory Construction Chamber

Screenshots from
Blade Runner 2049

Figures 1-4 downloaded from: <https://bit.ly/3EpFQr6>
Figure 5 downloaded from: <https://bit.ly/31uftSd>