Consultation Response to the European Commission's White Paper on Artificial Intelligence and its accompanying report on the safety and liability implications of Artificial Intelligence, the Internet of Things, and robotics

Executive summary:

- The European Commission's White Paper on a *European approach to excellence and trust in AI* (2020) provides for a broad and early stage framework for developing AI in a way that implements ethical considerations to further consumer trust in the technology. The proposals acknowledge important aspects for regulatory development such as:
    - Data privacy and protection considerations
    - Non-discrimination
    - Accountability
    - Transparency
    - Liability
- This response addresses a gap in the publications on AI in the European Union arguing that acknowledgment of harms to consumers caused by dark patterns in AI is necessary to further the goal of improving consumers' trust in the technology.
- It sets out the importance of engaging with user design on two levels:
    1. Due to an increasing trend in the anthropomorphization of AI systems such as chatbots and voice assistants (Kerr, 2004, Leong & Selinger, 2019), and what this may mean in future technology to better codify the rules of interactions between humans and machines.
    2. To further build upon GDPR (2016) regulations surrounding data mining and ownership and delineate to what extent this can be continued when mining human-AI conversations in chatbot or voice assistant (*Siri*, *Alexa*, *Cortona*)

dynamics where AI can elicit the self-disclosure of private consumer information (Thomaz et al., 2020), and how this can be contextualized within the data economy.

- It argues for the importance of grounding ethical frameworks for AI in existing UX design principles, along with the cognitive and psychological implications of the technology which are exploited via dark patterns.
- A focus on one aspect of consumer-facing AI which can be split into two-types of engageable technology is adopted:
    1. AI powered text based chatbots used for customer service and information
    2. General conversational agents/voice assistants such as *Siri* and *Alexa*
- From this, a working definition is proposed to define AI systems which allow users to make autonomous decisions regarding their "best interest":
    1. If the consumer/user is consulted during the design of the system in order to integrate the users' characteristics, methods of coordination, and purposes and effects of an intervention, along with the users' right to ignore or alter interventions. All while integrating the correct Level of Abstraction to explain an AI in an appropriate manner in relation to the system and the user, then these characteristics can ensure that the purpose of the AI system is knowable to its users, and thus allow users to interact with the system in a way which preserves their autonomy. In this case, the system would be seen as enabling users to determine what decisions are in their best interest.

- Lastly, applying new institutional economic analysis linking AI's increasingly important role in transactions in the data economy, the following recommendations are made partially informed by proposed U.S. Senate legislation, the DETOUR Act (2019):
    1. Dark patterns should be explicitly mentioned and acknowledged as possible harms to consumers.
        - They should be explained in a way which informs users of what they are while giving examples such as the ones given in this response.
        - There should be an explanation of how dark patterns will be prevented from exploiting users through AI, providing a definition such as the one provided, guiding how AI can be made in order to preserve user autonomy.
    2. Creation of a professional standards body registered with the relevant european authority, or incorporated into the excellence and testing centers, which focuses on best practices surrounding user design in AI.
        - The association would act as a self-regulatory body providing updated guidance on design practices that impair user autonomy, decision-making, or choice.
        - Continuous testing should be undertaken, and the quality label awarded for low-risk AI should make the regulations put forth by the body binding.
        - Funding could come from the €100 million put towards developments in AI in Q1 of 2020.
    3. Further policy prohibiting the segmentation of consumers for the purposes of behavioral experiments, unless with informed consent.

- Any behavioral or psychological experiments using AI performed with the user's consent should provide routine disclosures of the research not less than once every 90 days.

4. Regulation of the wider data economy should include explicit protections afforded to the consumer regarding data collection via chatbots and conversational agents/voice assistants such as *Siri* and *Alexa*.
    - Place restrictions on what data can be collected based upon the level of anthropomorphization of the AI system and how this data can be used.
    - Include the strengthening of GDPR (2016) regulations to ensure that autonomous and un-coerced consent is given for any form of data collection via AI, and that users are consulted in order to tailor the terms and conditions of these agreements in a way which is accessible and understandable to them

Dark patterns: the current landscape in UX

"Dark patterns" were coined by UX specialist Harry Brignull in 2010 to refer to tricks used in websites and apps to make users do things they otherwise did not mean to do such as purchase extra items or sign up for misleading services (Brignull, n.d.). Since then, there has been greater awareness over user design and how websites and algorithms are used to nudge users towards outcomes which benefit company shareholders as opposed to general consumers (Gray et al., 2018). Dark patterns exploit human psychology (Gray et al., 2018) manifesting themselves in intentionally manipulative and coercive ways to ensure consumers spend more money and give up their personal data (Gerner, 2020). Despite countries' enacted legislation concerning unfair or

deceptive practices such as section 5 of the U.S. FTC Act (2004), the Consumer Rights Directive (2014), and the GDPR (2016), which all employ varying levels of consumer protection from things like the sneak into basket pattern, hidden costs, and forced continuity as a form of bait-and-switch (Brignull, 2014), these protections focus solely on e-commerce aspects at the point where consumers are ready to make a purchase. But what of the dark patterns which increasingly nudge us to give up our personal information? Although the GDPR has been instrumental in defining "consent" (Stern et al., 2019) which has structured the architecture of European data collection in opposition to that of the U.S., an "opt-in" framework for the former and an "opt-out" for the latter, there is a lack of direct engagement between policy makers and how far data mining can go. Research since then has shown that thousands of dark patterns are still utilized across shopping websites (Mathur et al., 2019), and large tech companies such as Google, Facebook, and Microsoft have continued to employ dark patterns to skirt GDPR Articles 5,6,7,9, and 25 protecting consumer data (Myrstad, 2018, Forbrukerrådet, 2018a, Forbrukerrådet, 2018b). This showcases the importance of directly addressing data gathering and how it can be conducted ethically through anthropomorphized AI.

AI: ethical design should be addressed holistically and incorporate existing UX principles

AI must be ethical by design (Floridi et al., 2020, Leslie, 2019, Berdichevsky & Neuenschwader, 1999), of which value-sensitive design (Wynsberghe & Robbins, 2013) is a useful approach towards building ethical AI. However, to understand AI ethics, we must understand the economic systems which fund the development of AI capabilities, specifically large-scale data mining undertaken by the likes of Google, Facebook, Apple, and others who engage in the creation of these technologies. Therefore, before we are able to theorize how AI can be created

ethically, we must take a step back and acknowledge the economic motives for why AI might be employed to deceive and coerce, and how dark pattern tactics utilized in the website UX space can be transferred into AI tools.

I will be focusing specifically on one aspect of consumer-facing AI which can be split into two-types of engageable technology:

1. AI powered text based chatbots used for customer service and information
2. General conversational agents/voice assistants such as *Siri* and *Alexa*

This selection of AI is due to their consumer facing nature and widespread usage (Liu, 2019a, Liu, 2019b) as well as projected adoption and future investment in the technology (Liu, 2019c). According to the designation between low-risk and high-risk AI, conversational agents would fall in the low-risk category since they are employed to improve customer experience in situations where impact on affected parties is low. While the Commission's categories of AI are useful in establishing a hierarchy ensuring the proper functioning of high-risk AI, it will be low-risk AI which will be widely interacted with and adopted by society, so equal attention and oversight should apply to both to ensure widespread consumer trust in the technology.

The High-Level Expert Group on AI's (2018) upcoming revised ethical guidelines for trustworthy AI should therefore be partly grounded in existing principles provided by international UX organizations such as the UXPA (2013), as well as academic literature specifically outlining the various cognitive and psychological implications of user design

(Acquisti et al., 2017, Nouwens et al., 2020, Gray, 2018, Waldman, 2020). This would serve to ground future legislation intervening in AI dark patterns based upon its origins in website design.

Dark patterns: a symptom of the data economy

As discussed in the White Paper (2020) and the Commission's European strategy for Data (2020), Europe is positioned to become a global leader in the data economy, of which AI will be a key tool for the collection, processing, and storage of that data. This response is meant to caution the unequivocal support for the data economy without further regulation of its operations. Although the White Paper (2020) argues that the data of tomorrow will come more from industry, business, and the public sector instead of consumers, there is a need to address existing harms to consumers and prevent the continuation of economic uncertainties which exist in the data economy.

As tech companies began to amass zettabytes of data, they became data middlemen operating in uncharted territory. However, if successful economic growth is to be sustained, lessons from new institutional economics about the importance of transactions and the interplay between formal rules, informal norms, and enforcement of policies (North, 2005) must be learned from. So far, tech companies have determined transaction costs at either end of the data economy by deciding how much data to charge consumers for services, and how much that data is worth to third party vendors and programmatic advertising companies (Micova & Jacques, 2019). This has caused mistrust amongst consumers and continuing uncertainty in the programmatic advertising industry as transaction costs remain in constant flux (Micova & Jacques, 2019). The informal norms propagated by companies like Google, Facebook, and Microsoft disregard the formal rules which

govern the institutional system, and it is this path dependence (North, 2005) which is preventing a reduction in transaction costs and limiting the possibility of further economic growth.

As Amazon grows its market share and alleged monopolistic hold (Khan, 2017) on sectors ranging from e-commerce to cloud computing services, its continued growth will lead to future obstacles to growth as external organizations fail to compete with its offerings. The solution to this as prescribed by NIE, is the continued alteration of the institutional structure to allow the market to continue to expand via new regulatory incentive structures (North, 2005). Where dark patterns come in, are as a symptom of the larger unregulated institutional structure which still provides incentives for companies to amass as much data as they can, by using tools like *Alexa* (Huseman, 2019), with only minor fines and tax schemes available for any type of enforcement (*Tackling*, 2019, Kang, 2019, Tracy & McKinnon, 2019).

The gap: what aspects of dark patterns have been acknowledged, and what remains to be addressed

While certain dark patterns in e-commerce have been banned via legislation (Brignull, 2014), work remains to be done concerning privacy, information disclosure, sharing, and advertising. The AI HLEG's report (2018) acknowledges the importance of AI systems not deceiving, coercing, manipulating or unjustifiably impairing user's freedom of choice. However, the report discusses AI systems which have a subsequent legal effect based on autonomous decision making, with no real engagement with the inherent privacy harms caused by the unethical hijacking of sub-conscious human processes.

To improve the scope of the regulation ensuring consumer trust in AI, the Commission must engage with a crucial issue in defining dark patterns in technological design:

1. Dark patterns as defined by Gray et al. (2018) are "...instances where designers use their knowledge of human behavior (e.g. psychology) and the desires of end users to implement deceptive functionality that is not in the user's best interest" (pg. 534). Therefore, in order to combat dark patterns, a definition as to what type of system would allow users to decide what is in their "best interest" is needed.

Providing a definition would require multi-stakeholder engagement to balance the benefits of user generated data to improve functionality, with excessive datamining of private consumer information. So, for now, I will briefly discuss instances where AI could be used in unethical ways which benefit corporations over consumers. This will help conceptualize new and existing issues of dark patterns in AI and allow me to provide an early approach to define a system which enables a user's "best interest" to be discerned.

Thomaz et al. (2020) argues that as the usage of VPNs and other anonymizing technologies increases, conversational agents and chatbots can become effective marketing tools towards encouraging self-disclosure of private data from consumers. This argument is supported by Moon (2000, 2003) and Nass & Moon (2000) who show that not only do human beings follow the norms of reciprocity found in human to human interactions, but as relationships with computers evolve, the blame for positive and negative outcomes of online decisions is reversed, where users come to place blame on negative online purchase outcomes on themselves rather

than the computer if they've had a history of self-disclosure and high-level of attraction towards the system. This is because humans are highly socialized beings which when faced with a non-human entity, often defer to transferring their previous experiences from social interactions into known communication patterns, often involving disclosure if the other party initially discloses (Moon, 2000, Nass & Moon, 2000). The issues arise when the data used from the conversations is kept (Huseman, 2019) and subsequently utilized to gain insight into the opinions, views, and purchases of consumers. While the GDPR (2016) already addresses certain categories of protected data such as political opinions, ethnic origins, and religious beliefs, since the implementation of the regulation there have been alleged violations of these articles, and so it should not be assumed that these types of data need not be specifically addressed in AI regulation. Also, despite this being briefly touched upon by the AI HLEG's report (2018) under the *Privacy and Data Protection* section, the gathering of this type of data is already assumed to occur, and so no protections against the initial collection of the information in chatbot or conversational agent interactions is afforded to the consumer.

Despite existing regulatory protections for consumers over data collection, analysis, and use, we are entering a new era of data transactions which is employing tools that are becoming increasingly anthropomorphized (Leong & Selinger, 2019) and ingrained in our lives. One merely has to think about their usage of their *Siri* or *Alexa* personal assistants and how companies have gone to great lengths to instill the element of social presence (Thomaz et al., 2020) in them to give us the illusion that the AI is psychologically present during our interactions. The very nature of dark patterns exists in opposition to notions of data privacy and transparent information disclosure, which could lead to even more acute cases of emotional

toying or rewards and punishment tactics already employed to discourage users from choosing a specific option by shaming them or praising them into compliance (Gray et al. 2018, Forbrukerrådet, 2018a). Dark patterns can be employed from the start or throughout the interaction as one could hypothetically foresee that in order to begin an interaction with a customer service chatbot, the *ease* dark pattern (Forbrukerrådet, 2018a) may be employed, allowing a user to quickly accept terms and conditions and begin a conversation to resolve their query, or otherwise be forced to click a link which re-directs them to a separate page with numerous data collection settings and documents, thus favoring the ease with which "consenting" to data collection allows. Finally, whereas a webpage employing dark patterns may utilize *framing* (Forbrukerrådet, 2018a) in a more static way to highlight the positive aspects of a decision, while glossing over any negative ramifications, this can occur more dynamically via an AI chatbot where the bot may continuously follow up with a certain frame and even give the user a greater sense of confidence in its advice due to the embedded social presence element (Thomaz et al., 2020).

These issues while not yet directly discussed, can be resolved by understanding the design intentions behind existing dark patterns and then theorizing their application in AI. Below are existing dark patterns (Forbrukerrådet, 2018a) used to gather consumer data which I argue could be developed in AI:

1. Framing
2. Ease
3. Rewards and punishment
4. Forced action and timing

Although this list is not exhaustive, the unifying tactic employed is the nudging of users towards making decisions they otherwise wouldn't make if they genuinely understood all aspects of their decision (Lomas, 2018). While the assumption throughout this response, and in academic literature, argues that with more knowledge of data collection ramifications, users will therefore opt not to disclose as much information in exchange for services, this may not always be the case. But that is not the point which I, or others like Floridi et al. (2020), argue is important when designing AI, instead focusing on the preservation of user autonomy and preference elicitation. If we view AI conversational agents and chatbots as tools which have power to change our preferences, enabling the software to further contextualize future interventions via interactions, then it is clear why users should be seen as equal partners in both the design and deployment of autonomous decision making systems (Floridi et al., 2020). This means continuing to allow users to ignore or request alterations of information given to them by an AI (Floridi et al., 2020), much like in human to human interactions, but also condemning the ideology behind dark patterns which views humans as data points and upholds the perfection of AI systems above imperfect humans.

Combining the explainability and stakeholder acknowledgment needed in AI highlighted by Floridi et al. (2020), the working definition proposed for determining a user's "best interest" in relation to dark pattern deception is:

1. If the consumer/user is consulted during the design of the system in order to integrate the users' characteristics, methods of coordination, and purposes and effects of an intervention, along with the users' right to ignore or alter interventions. All while

> integrating the correct Level of Abstraction to explain an AI in an appropriate manner in relation to the system and the user, then these characteristics can ensure that the purpose of the AI system is knowable to its users, and thus allow users to interact with the system in a way which preserves their autonomy. In this case, the system would be seen as enabling users to determine what decisions are in their best interest.

For the reasons outlined, it is crucial that dark patterns are directly engaged with in upcoming draft regulations to standardize how data collection and analysis can be undertaken by corporations. Unlike the creation of the data economy, it is not too late for development standards for human-machine interactions to gain wide market acceptance but must do so before the market power of incumbent technologies is set in ways which expand their streams of data collection. The proposals for consideration in future drafts of AI policy for the European Commission outlined in the executive summary are therefore made taking a holistic approach to address dark patterns and their ramifications through AI and the wider data economy.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y. & Wilson, S. (2017). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3). http://dx.doi.org/10.1145/3054926

Berdichevsky, D., & Neuenschwander, E. (1999). Toward an ethics of persuasive technology. *Communications of the ACM*, *42*(5).

Brignull, H. (n.d.). What are dark patterns? (A. Darlo, Ed.). Retrieved April 21, 2020, from https://www.darkpatterns.org/

Brignull, H. (2014, August 26). Some Dark Patterns now illegal in UK – interview with Heather Burns [Blog post]. Retrieved from https://90percentofeverything.com/2014/08/26/some-dark-patterns-now-illegal-in-uk-interview-with-heather-burns/index.html

Consumer Rights Directive. (2014, June 13). Retrieved from Eur-Lex database.

Deceptive Experiences To Online Users Reduction Act (DETOUR ACT), S. S.1084, 116th, 1st. (as introduced, Apr. 9, 2019) (Congress.gov).

A European strategy for data. (2020, February). Retrieved from European Commission website: https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf

Federal Trade Commission, Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices, S. Doc. (2004).

Floridi, L., Cowls, J., King, T. C., & Taddeo, M. (2020). How to Design AI for Social Good: Seven Essential Factors. *Science and Engineering Ethics*. https://doi.org/10.1007/s11948-020-00213-5

Forbrukerrådet. (2018a, June). *Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Retrieved from https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf

Forbrukerrådet. (2018b, November). *Every step you take How deceptive design lets Google track users 24/7*. Retrieved from https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf

General Data Protection Regulation. (2016, April 27). Retrieved April 25, 2020, from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Gerner, M. (2020, January 29). What are dark patterns and how are they tricking me? Retrieved April 21, 2020, from https://www.raconteur.net/business-innovation/dark-patterns

Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3173574.3174108

High-Level Expert Group on Artificial Intelligence: Ethics and Guidelines for Trustworthy AI. (2018, December). Retrieved April 25, 2020, from https://ec.europa.eu/futurium/en/ai-alliance-consultation

Hill, K. (2014, June 28). Facebook Manipulated 689,003 Users' Emotions For Science. *Forbes*. Retrieved from https://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science/#469f9f11197c

Huseman, B. (2019, June 28). [Letter to Christopher A. Coons]. Retrieved from https://www.coons.senate.gov/imo/media/doc/Amazon%20Senator%20Coons__Response%20Letter__6.28.19%5B3%5D.pdf

Kang, C. (2019, July 12). F.T.C. Approves Facebook Fine of About $5 Billion. *The New York Times*. Retrieved from https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html

Kerr, I. R. (2004). Bots, Babes and the Californication of Commerce. *University of Ottawa law & technology journal*, *1*, 284-324. Retrieved from SSRN database.

Khan, L. M. (2017). Amazon's Antitrust Paradox. *The Yale Law Journal*.

Leong, B., & Selinger, E. (2019). Robot Eyes Wide Shut: Understanding Dishonest Anthropomorphism. In *Proceedings of ACM Conference on Fairness, Accountability, and Transparency*. Retrieved from ACM database. (Accession No. https://doi.org/10.1145/3287560.3287591)

Leslie, D. (2019). *Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector*. Retrieved from https://doi.org/10.5281/zenodo.3240529

Liu, S. (2019a, February 8). Digital voice assistant installed base worldwide in 2019, by brand [Chart]. Retrieved from Statista database.

Liu, S. (2019b, October 1). Intelligent/virtual assistant smartphone penetration rate worldwide in 2017, 2018 and 2022, by brand [Chart]. Retrieved from Statista database.

Liu, S. (2019c, May 22). Chatbot market size worldwide 2018-2027 [Chart]. Retrieved from Statista database.

Lomas, N. (2018, July 1). WTF is dark pattern design? Retrieved May 19, 2020, from https://techcrunch.com/2018/07/01/wtf-is-dark-pattern-design/

Mathur, A., Acar, G., Friedman, M. J., Lucherini, E., Mayer, J., Chetty, M., & Narayanan, A. (2019). Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites. *ACM on Human Computer Interaction*, *3*. Retrieved from ACM database.

Micova, S. B., & Jacques, S. (2019, April). *The playing field in audiovisual advertising: What does it look like and who is playing?* Retrieved from Center on Regulation in Europe website: https://www.cerre.eu/sites/cerre/files/cerre_playingfieldaudiovisualadvertising_2019april.pdf

Moon, Y. (2000). Intimate Exchanges: Using Computers to Elicit Self-Disclosure From Consumers. *Journal of Consumer Research*, *26*(4). Retrieved from JSTOR database.

Moon, Y. (2003). Don't Blame the Computer: When Self-Disclosure Moderates the Self-Serving Bias. *Journal of Consumer Psychology*, *13*. https://doi.org/10.1207/S15327663JCP13-1&2_11

Moon, Y., & Nass, C. (2000). Machines and Mindlessness: Social Responses to Computers. *Journal of Social Issues*, *56*(1), 81-103. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.87.2456&rep=rep1&type=pdf

Myrstad, F. L.-O. (2018, June 27). *Regarding how tech companies nudge users into choosing the less privacy friendly options*. Retrieved from https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-regarding-how-tech-companies-nudge-users-into-choosing-the-less-privacy-friendly-options.pdf

North, D. C. (2005). *Understanding the Process of Economic Change*. https://doi-org.gate3.library.lse.ac.uk/10.1515/9781400829484

Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). *Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence*. Paper presented at Conference on Human Factors in Computing Systems, Honolulu, HI, USA. Retrieved from ACM database.

Stern, W., Kim, L., & Graubert, J. (2019, July 9). Dark Patterns: What They Are and What You Should Know About Them. Retrieved April 21, 2020, from https://www.insideprivacy.com/consumer-protection/dark-patterns-what-they-are-and-what-you-should-know-about-them/

Tackling the Information Crisis: A Policy Framework for Media System Resilience. (2019). Retrieved from Truth Trust & Technology Committee LSE website: http://www.lse.ac.uk/media-and-communications/assets/documents/research/T3-Report-Tackling-the-Information-Crisis-v6.pdf

Thomaz, F., Salge, C., Karahanna, E., & Hulland, J. (2020). Learning from the Dark Web: leveraging conversational agents in the era of hyper-privacy to enhance marketing. *Journal of the Academy of Marketing Science*, 43-63. https://doi-org.gate3.library.lse.ac.uk/10.1007/s11747-019-00704-3

Tracy, R., & McKinnon, J. D. (2019, July 25). Facebook's Fine Sends a Message To Big Tech. *Wall Street Journal*. Retrieved from ProQuest database.

UXPA Code of Professional Conduct. (2013). Retrieved April 25, 2020, from https://uxpa.org/uxpa-code-of-professional-conduct/

Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology, 31*, 105-109. https://doi.org/10.1016/j.copsyc.2019.08.025

White Paper On Artificial Intelligence - A European approach to excellence and trust [White paper]. (2020, February 19). Retrieved from https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Wynsberghe, A. V., & Robbins, S. (2013). Ethicist as Designer: A Pragmatic Approach to Ethics in the Lab. *Science and Engineering Ethics*, 947-961. https://doi.org/10.1007/s11948-013-9498-4