Moral Issue of AI Chatbot

AI is arguably one of the leading words of the 21st century. From smart translation, smart home assistant, to automatic driving, smart city interconnection, AI plays a decisive role in them. Intelligent machine systems are changing our lives for the better. As these systems become more powerful, our world becomes richer and more efficient. Specifically, when it comes to the Internet industry, AI is dominating, even for the tech giants like Google, Amazon, Facebook, IBM, Tencent, Alibaba and Microsoft.

An important part of AI development is the simulation of human conversation and human relationships. Time reported that in 2014, a chatbot called Eugene Goostman passed Turing Test by making 33% of the judges believe it is not a chatbot but a human boy during a five minutes conversation (Aamoth, 2014). As AI technology matures, many companies are planning to create chatbots that allow people to talk to their loved ones to ease the pain of bereavement (Matie, 2017). However, others, like The Guardian, use AI chatbot to simulate chatting with people without their permission (Wong, 2019). This led to a discussion about whether it is morally wrong to develop a chatbot simulating someone without their permission.

My answer to the dispute is: it is certainly wrong to simulate someone by chatbot without permission since the AI chatbot may make the statement that against the will of the simulated person and it violates the ACM code of ethics.

Intelligence comes from learning, whether it's for human-being or AI. Before the chatbot can simulate a person, it must be trained with a huge amount of data about that person then analyze,

learn and “become” that person. The problem is the result of training is a black box, which means garbage in, garbage out, it is hard for us to control the result of the learning of chatbot. According to Stuart-Ulin (2018), Google’s image-recognition technology labelled black people as gorillas and their solution to fix is to block the gorilla tag. The reason for this error is that Google’s algorithm is getting the data set from the Internet while most of the face pictures in the data set is composed of white people, so the result of training is not diverse enough to represent other races. Most unacceptably, Google can do nothing about his algorithm, except to fix the error by banning chimp tags. Similarly, in 2016 Microsoft launched their chatbot, Tay, on twitter, and her learning results turned her into a racist Nazi supporter in just 24 hours. After Microsoft took “Tay” offline and apologized, her sister “Zo” became online on Messenger, Kik, Skype, Twitter, and Groupme a few months later. The problem solved in the exact same way Google did to their image-recognition tech: avoid all politic related messages. She refuses to talk when any of political sensitive keyword is detected (Stuart-Ulin, 2018). We should not forget that AI chatbots are created by humans, and they can contain the biases and judgments of designers. It is extremely unacceptable for the person who is being simulated that the chatbot claiming to be him/her is making a statement that against his/her will without his/her permission.

According to Ermann & Shauf (2003), the ACM code of ethics contains many rules that professionals of computer science must follow. The development of chatbot simulating someone without his/her permission violates the ACM code of ethics 1.7: Respect the privacy of others and 2.3 Know and respect laws pertaining to professional work. The former one requires the

professional to ensure the privacy and integrity of data. The consent from the individual(s) is mandatory for the data collected. And the data can not be used for other purposes without the consent of the individual(s). As for the later, literally, it means the professionals can't violate any laws related to the work they are doing (Ermann & Shauf, 2003). Obviously, the development of such chatbot is not legal. In Canada, the regulation of personal data protection is on the federal level by the Personal Information Protection and Electronic Documents Act (PIPEDA). PIPEDA has ten privacy principles including privacy issues in terms of consent, transparency, security measures, and data retention. Among the principles, principle 3 indicates that “knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate” (Law Library of Congress, 2020, para. 9). Therefore, collecting and using personal information to develop such chatbot without permission is both legally and morally wrong. The developers who do not refuse to do so will result in the violation of the ACM code of ethics.

However, some may argue that using someone’s public information retrieved from social media like Twitter, Facebook or Instagram is legal which is enough data needed to create a simulating chatbot. It is true that under the current regulation of PIPEDA, there is no specific regulation on data protection in respect to social media (Law Library of Congress, 2020). This means by agreeing on the terms of use, you are consenting the social media company to collect and use your personal information to “provide you better service”. Although you can claim that using your personal data to create a chatbot that simulates you is changing the purpose of your

personal data usage which requires your new consent by law (Law Library of Congress, 2020), the company can still be able to bypass the law by declaring that chatbot is qualified for your consent of the purpose of "provide you better service" or even directly add the term of using your personal data for chatbot into the terms of agreement since no one really read it thoughtfully. However, the chatbot that simulating and claiming to be someone may violate the law of identity fraud. In Canada, it is a criminal offence to impersonate someone. According to the criminal code, identity fraud is defined as "Everyone commits an offence who fraudulently personates another person, living or dead" (R.S.C., 1985, c. C-46). It further clarifies that "personating a person includes pretending to be the person or using the person's identity information — whether by itself or in combination with identity information pertaining to any person — as if it pertains to the person using it"(Government of Canada, 2020). Therefore, even the chatbot is developed based on public information, claiming to be someone and make a statement not made by the person him/herself is violating the criminal law of identity fraud. The behavior of the guardian — using a chatbot to simulates Mark Zuckerberg is violating identity fraud which is illegal in Canada (Wong, 2019).

Overall, currently it is both morally and legally wrong to develop a chatbot that simulate someone without permission. The training algorithm may lead to unexpected and unacceptable results because of the pollution from the Internet community. Also, the potential legal risk of violating privacy protection law (PIPEDA) and criminal code for identity fraud makes the developer violates the ACM code of ethics which makes the professionals who do not refuse to develop such chatbot, unethical. However, with the progress of AI technology achieved, the growth

of the need to chat with deceased relatives. Perhaps someday in the future, with the improvement of AI-related laws, it might be allowed that the deceased can give permission to develop a chatbot that simulates him/her by giving his/her consent in his/her testament to ease the pain of bereavement. But no matter under what kind of circumstance, using personal information without permission is wrong.

Word count: 1242

References

Aamoth, D. (2014). Interview with Eugene Goostman, the Fake Kid Who Passed the Turing Test. Retrieved 10 February 2020, from https://time.com/2847900/eugene-goostman-turing-test/

Ermann, M., & Shauf, M. (2003). *Computers, ethics, and society* (3rd ed.). New York: Oxford University Press.

Government of Canada. (2020). Criminal Code. Retrieved 10 February 2020, from https://laws-lois.justice.gc.ca/eng/acts/c-46/section-403.html

Hern, A. (2018). Google's solution to accidental algorithmic racism: ban gorillas. Retrieved 10 February 2020, from https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people

Law Liberary of Congress. (2020). Online Privacy Law: Canada | Law Library of Congress. Retrieved 10 February 2020, from https://www.loc.gov/law/help/online-privacy-law/2012/canada.php

Matei, A. (2017). New technology is forcing us to confront the ethics of bringing people back from the dead. Retrieved 10 February 2020, from https://qz.com/896207/death-technology-will-allow-grieving-people-to-bring-back-their-loved-ones-from-the-dead-digitally/

Wong, J. (2019). 'I am going to say quiet words in your face just like I did with Trump': a

conversation with the Zuckerbot. Retrieved 10 February 2020, from https://www.theguardian.com/technology/2019/dec/22/zuckerbot-mark-zuckerberg-facebook-botnik