**Explore – Impact of Computing Innovations  
Written Response Submission Template**

**Computational Artifact**

2a) The computing innovation that I selected is facial recognition. My computational artifact shows the steps that facial recognition software takes while scanning someone's face. The intended purpose of facial recognition software is to help computers recognize who someone is. The computer can then use the recognized face and match it with a database to be able to verify someone's identity to unlock a device or even track them.

2b) To create my computing artifact I used google slides. To add text to the powerpoint I used the text tool and created text boxes. I then added arrows to allow the reader to understand the progression of what direction to read to text from and the process facial recognition takes when detecting someone's face

**Computing Innovation**

2c) One beneficial effect of facial recognition on society is that it allows security to do their jobs better. One case of facial recognition helping out security is when “Recently, at the Washington Dulles Airport, facial recognition technology caught an imposter trying to enter United States on a fake passport”(Newman). Without facial recognition these airport security workers would not be able to have caught the man with his fake passport. This would have allowed for a potentially dangerous person to get into the U.S. A harmful effect of facial recognition is that it can be used by governments or private institutions to allow people to be tracked easily. Facial recognition cameras can be set up in public and store the faces of everyone who passes by and follow their movements across a city gathering data for the city or a company. This is harmful to society because it can be an invasion of privacy for people if they do not consent to be tracked across a city or in a store or other building. One company “to enter this territory was IBM, which in January released a collection of nearly a million photos [that were taken from the photo hosting site Flickr](https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/) and coded to describe the subjects’ appearance”(Solon). No one was told that IBM was using their faces to train their AI’s until they released the thousands of photos with scanned data. This is a clear invasion of privacy and could have been extremely harmful to society.

2d) The data that my computing innovation uses is data from a camera, a library of human facial features and a database of pre-existing faces. The innovation consumes the data from the camera after a photo is taken. The photo provided from the camera is then analyzed alongside the data from the human facial feature library. After these two data points are analyzed the software then puts different points along the picture of the face where the prominent features of the face are. This marked up photo known as “Your facial signature - mathematical formula - is compared to a database of known faces”(Symanovich). The software then produces the transformed data, which is the face that matched your facial signature, into an answer for the user. This answer is usually if the face matches another face to unlock a device or if the face matches a face on record and give the name of the face on record. One data security concern is that the software or computers holding the data of the scanned faces can be leaked to the public and used by malicious entities to track people through cameras or their own phones if they have access to them.These faces that could be stolen, could also be used to create programs or models of a face to spoof facial recognition into unlocking a device that should be secured.

**References**

2e)

Works Cited

[1] Brandom, Russel. "HOW SHOULD WE REGULATE FACIAL RECOGNITION?" *The Verge*, 29 Aug. 2018, [www.theverge.com/2018/8/29/17792976/facial-recognition-regulation-rules](http://www.theverge.com/2018/8/29/17792976/facial-recognition-regulation-rules). Accessed 13 Mar. 2019.

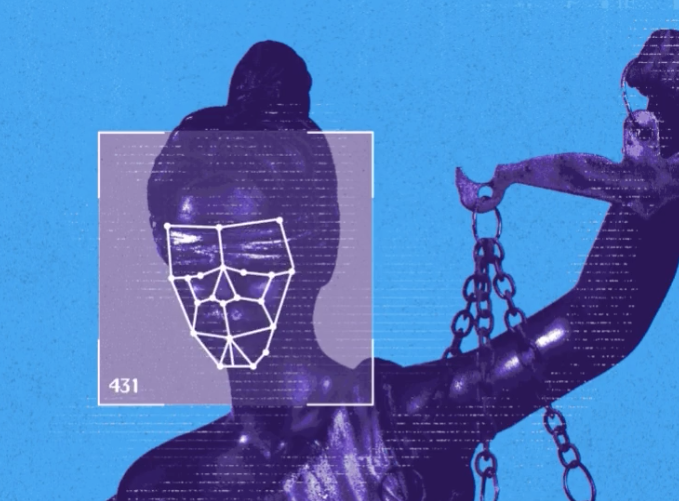
[2] Newman, Daniel. "Facial Recognition Software: The Future Is Here." *Forbes*, CMO Network, 18 Sept. 2018, [www.forbes.com/sites/danielnewman/2018/09/18/facial-recognition-software-the-future-is-here/#61667ab1299d](http://www.forbes.com/sites/danielnewman/2018/09/18/facial-recognition-software-the-future-is-here/#61667ab1299d). Accessed 13 Mar. 2019.

[3] Shankland, Stephan. "IBM stirs controversy by sharing photos for AI facial recognition." *c net*, 12 Mar. 2019, [www.cnet.com/news/ibm-stirs-controversy-by-sharing-photos-for-ai-facial-recognition/](http://www.cnet.com/news/ibm-stirs-controversy-by-sharing-photos-for-ai-facial-recognition/). Accessed 13 Mar. 2019.

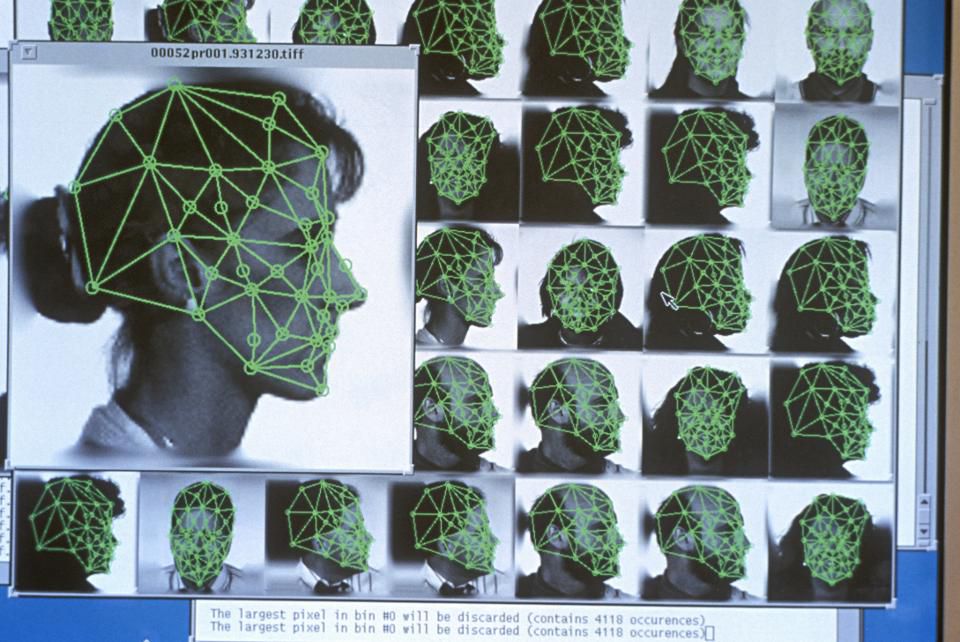
[4] Solon, Olivia. Facial recognition's 'dirty little secret': Millions of online photos scraped without consent. *NBC News*, 12 Mar. 2019, [www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921](http://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921). Accessed 13 Mar. 2019.

[5] Symanovich, Steve. "How does facial recognition work?" *Norton*, Symantec, [us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html](http://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html). Accessed 13 Mar. 2019.

[6] Yang, Wencheng, and Song Wang. "Fingerprint and face scanners aren't as secure as we think they are." *The Conversation*, 5 Mar. 2019, [theconversation.com/fingerprint-and-face-scanners-arent-as-secure-as-we-think-they-are-112414](http://theconversation.com/fingerprint-and-face-scanners-arent-as-secure-as-we-think-they-are-112414) . Accessed 13 Mar. 2019.

Image Courtesy of:

[www.theverge.com/2018/8/29/17792976/facial-recognition-regulation-rules](http://www.theverge.com/2018/8/29/17792976/facial-recognition-regulation-rules)

Image Courtesy of: 

<https://www.forbes.com/sites/danielnewman/2018/09/18/facial-recognition-software-the-future-is-here/#5b49c27299d7>