Chloe Bowen and Wendy Xayalith

PeekaBoo! iSeeYou!

Is Face ID truly safe to use?

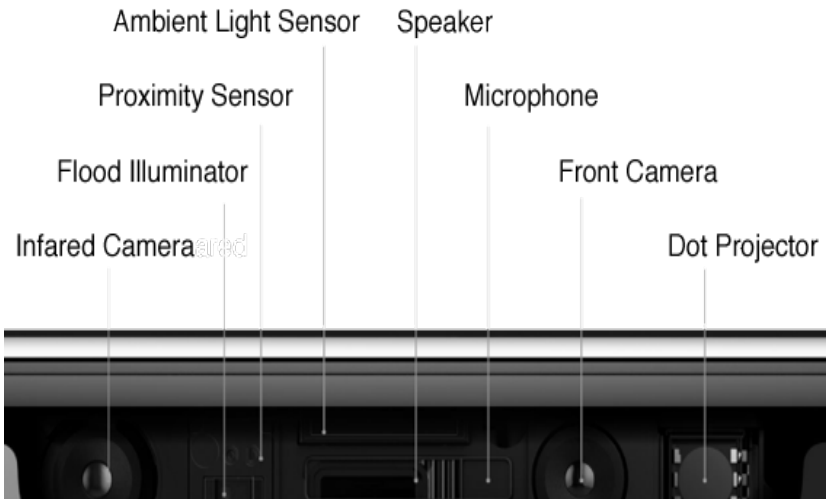
PeekaBoo! iSeeYou!

By Wendy Xayalith and Chloe Bowen

The evolution of the iPhone has changed dramatically ever since its first launch in 2007, with a 2MP camera, and a camera hole measured up to 4.5mm, allowing for the user to capture photos with 1600 x 1200 resolution. This received worldwide attention from the media, thus the iPhones journey set sailed. Fast forward to the present, 2019, their latest model iPhone 11 and iPhone 11 Pro, the evolution within the iPhone has evolved, unlocking many features, such as taking photos from wide to ultrawide, with not one but three cameras on the one phone. What changed overtime the most though is the method of accessing your phone. Originally the only way to unlock your device is by a text-based passcode, this however changed overtime with the installation of using your own fingerprint, to now, your own face, officially referred to as Face ID.

Face ID, the new method of unlocking your phone, uses the TrueDepth camera system. This means that every time you look at your phone, the camera system will be able to detect your face with a flood illuminator in any light setting. Additionally, there is an infrared camera which uses a dot projector to project approximately 30 000 invisible dots onto your face, when you take a picture. The dots will then be sent through a process of neural networks to create a mathematical model of your face. With this invention, Apple too has established new applications and opportunities. This includes Animoji, which was introduced for the iPhone X during 2017, an emoji application that uses facial motion capture to animate.

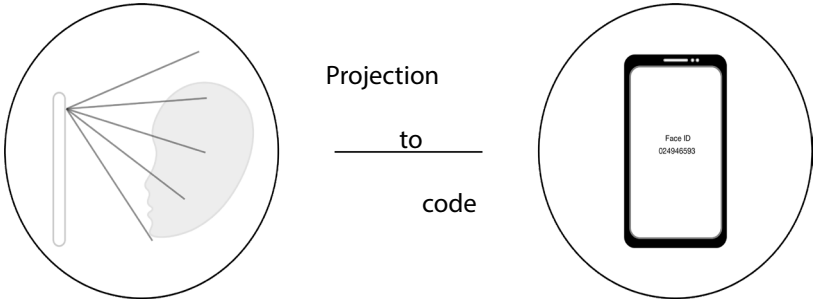
Apple's TrueDepth Camera



With the new installation of Face ID, there are also fears of its security from hackers. Due to security being a very important aspect, Apple had to place protection for privacy. Face ID uses TrueDepth camera and machine learning for a solid authentication solution. Face ID data, which includes mathematical representations of your face, with a key available only to the Secure Enclave. The "Secure Enclave" is one of the iPhone's chips that's devoted directly to securing sensitive data, and also where your fingerprints are stored. The way it works in order to make Face ID protected is that, when the device completes scanning your face, your facial scan is not actually kept on your iPhone. Instead, it is then converted into a number that represents the scan. This means that even if a hacker is attempting to get into your iPhone's Secure Enclave, they would only find a number, not a facial scan of your face. This means that they cannot use the data for another facial recognition system. With this in mind, the possibility of a stranger unlocking your phone using Face ID is approximately 1 in 1 000 000 with a single registered appearance. To further improve the security, Face ID allows only up to five unsuccessful match attempts before the facial passcode is required.

Even though the security on Face ID is well protected, the potential consequences with Face ID is unavoidable. Such circumstances can be considered as cybersecurity paranoia, where many were concerned about the security following the announcement of this new technology. However, Apple's cutting-edge technology is more promising in this circumstance. Additionally, a consequence that has been brought up is its effectivity for everyday life. Whilst reviewing several articles and posts, there was evidence that people did struggle when using facial recognition in their everyday lives. People found that the component was not functioning as it should be. Apple proposed many steps that could help solve this issue. These steps included checking for updates, checking the Face ID settings, checking there is nothing obstructing the TrueDepth camera and nothing is covering the user's face.

Overall, Face ID technology has demonstrated the advanced growth of Apple over the past decade and furthermore the high-level protection they ensure to their consumers. Due to this, it is really no surprise that in the near future, this technology will become more progressive and will be used to the fullest in their products.



References:

Apple. (2019). About Face ID advanced technology. Retrieved from https://support.apple.com/en-au/HT208108

Cipriani, J. (2018, October 26). Apple Face ID: Everything you need to know. CNet. Retrieved from https://www.cnet.com/how-to/apple-face-id-everything-you-need-to-know/

Cipriani, J. (2017, November 7). Here's what you need to know about animoji. CNet. Retrieved from https://www.cnet.com/how-to/getting-started-with-the-iphone-x-animoji-apple/

Guiness, H. (2018, October 23). How Secure Are Face ID and Touch ID? How-To-Geek. Retrieved from https://www.howtogeek.com/350676/how-secure-are-face-id-and-touch-id/

Apple. (2017, November). Face ID Security. Retrieved from https://www.apple.com/business/docs/site/FaceID_Security_Guide.pdf

Nachreiner, C. (n.d.). Apple's Face ID: No match for multifactor security. TechBeacon. Retrieved from https://techbeacon.com/security/apples-face-id-no-match-multifactor-security

Bud, A. (2018, January). Facing the future: the impact of Apple FaceID. Biometric Technology Today, Volume 2018, Issue 1, Pages 5-7. Retrieved from https://www.sciencedirect.com/science/article/pii/S0969476518300109

Mainenti, D. (2017, December). User Perceptions of Apple's Face ID. Information Science: Human Computer Interaction. Pages 1-16. Retrieved from https://www.researchgate.net/profile/David_Mainenti/publication/321795099_User_Perceptions_of_Apple's_Face_ID/links/5a31f871458515afb6d97834/User-Perceptions-of-Apples-Face-ID.pdf

A Step-by-Step Guide to Using Face ID