

James Denahy

Facing the Future

The intricacies, controversies and future
of reading, storing and using your face



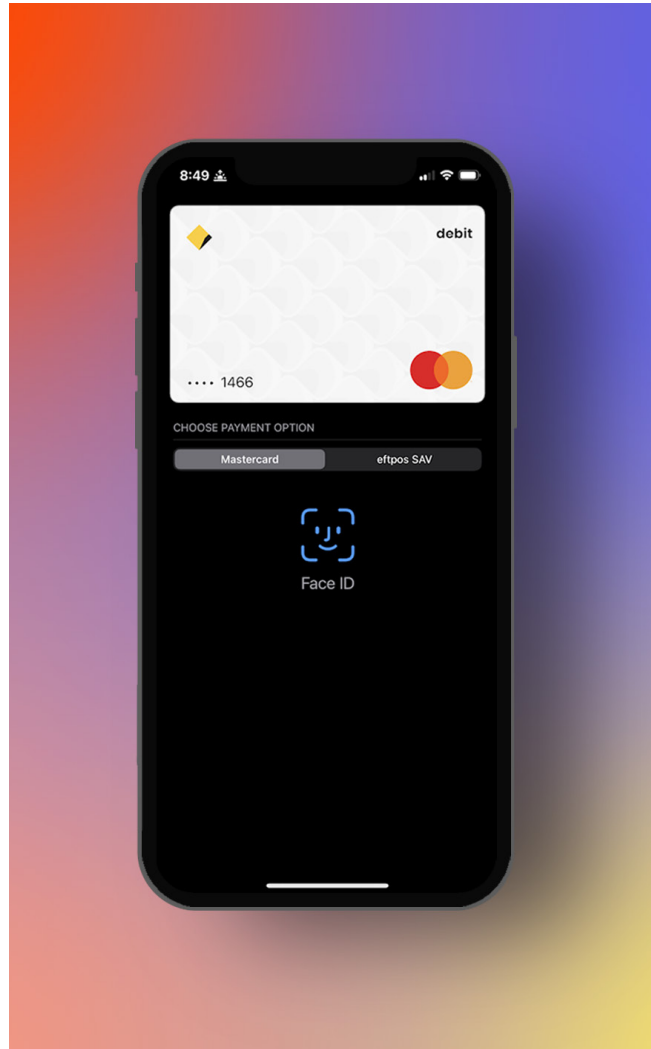
Facing the Future

James Denahy

Face ID is an Apple-designed technology that allows users to unlock and sign into their accounts by using their face as the password.

Many apps, apple owned or otherwise, have given the option to use Face ID to automatically log in, such as Apple Wallet, Commbank and Google Chrome. While its applications are helpful and convenient in many cases Apple will still require you to set a 4 to 6 digit passcode for certain security processes such as updating, erasing or other changes to the device among other things. During Face ID's development, Apple reportedly used over 1 billion images to account for as many facial features and variables as possible such as hair and skin colour, body modifications, hairstyles, accessories and facial structures.

While apple shares facial mapping data with developers which is what allows Instagram and Snapchat to use filters, the actual encrypted mathematical data connected to



the user's face is kept on the phone and not put onto any cloud or online service. Apple has also put a ban on using this data for direct monetary gain or the creation of face profiles. This limitation still allows for the use and recognition of faces to be available to any apps that use this technology, but it can only recognise that there is a face and their expressions, it cannot actually categorise and save this data into individual profiles.

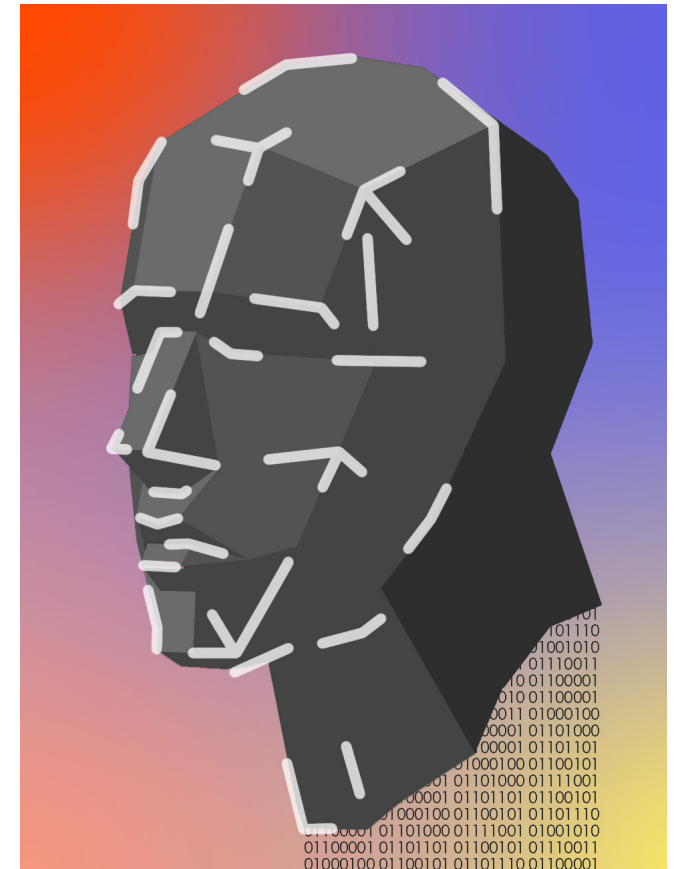
While Apple in the past has remained solid in their security and making any violators accountable this decision has still raised eyebrows as in order to actually crack down on violators they need to catch them first which may allow any existing assailants to go undetected for an unknown amount of times before they're caught. The efficacy of the system seems to vary throughout its multiple updates. Many news outlets have attempted to 'hack' the security system by creating realistic Hollywood-level masks impersonating the would-be victim but to no avail. This is

contrasted with identical twins being able to unlock each other's phones and even a son being able to unlock his mother's phone. This was discovered to be a lighting problem as when the mother registered her face in a low light setting her son could also unlock her phone, but when she registered her face in proper lighting the son was unable to.

The Way Face ID works is Apple's TrueDepth camera projects thousands of invisible dots onto your face which creates a sort of mesh map of your face. This is then coupled with infrared images to create a mathematical representation of your face. This data is then encrypted and stored on the device. Then whenever you go to use face ID it compares the face that is attempting to unlock your phone to this data to determine whether it's the correct face or not. Face ID is also built to adapt to your appearance, if there are small detectable changes such as a hat, glasses or a piercing it will adapt its data to consider

these new parameters. If there is a drastic difference such as shaving your head or facial hair it will ask you to enter your passcode first before updating your data. Thanks to the use of infrared cameras to confirm your identity, Face ID can work in complete darkness.

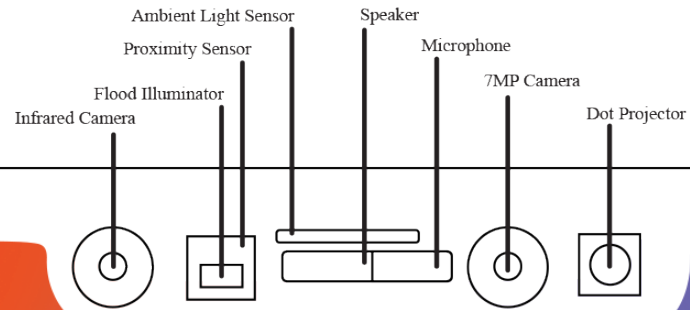
When comparing the built-in TrueDepth camera within Apple devices to an industry-grade 3D scanner such as the Artec Space Spider the advantages and disadvantages become clear. While Apple devices had more deviations in results and had trouble picking up certain colours, specifically black, the low cost and widespread nature of this technology are far too advantageous to ignore. We've seen this happen before as what is considered to be 'industry standard technology' constantly becomes cheaper and more intuitive, then put into the hands of consumers.



References:

Apple. (2022, May 13). Face ID, Touch ID, passcodes and passwords. Apple Support. <https://support.apple.com/en-au/guide/security/sec9479035f1/1/web/1>
Deahl, D. (2017, November 14). This 10-year-old was able to unlock his mom's iPhone using Face ID. The Verge. <https://www.theverge.com/2017/11/14/16650394/10-year-old-unlock-mom-iphone-face-id>
Lomas, N. (2017, October 17). Apple responds to Senator Franken's Face ID privacy concerns.

TechCrunch. <https://techcrunch.com/2017/10/17/apple-responds-to-senator-frankens-face-id-privacy-concerns/>
Staff, W. (2017, November 3). Beating the iPhone X Face ID Is Hard. We Know, Because We Tried. WIRED; WIRED. <https://www.wired.com/story/tried-to-beat-face-id-and-failed-so-far/>
Statt, N. (2017, November 2). Apple will share face mapping data from the iPhone X with third-party app developers. The Verge. <https://www.theverge.com/2017/11/2/16599592/apple-iphone-x-face-id-data-share-app-developers-privacy>

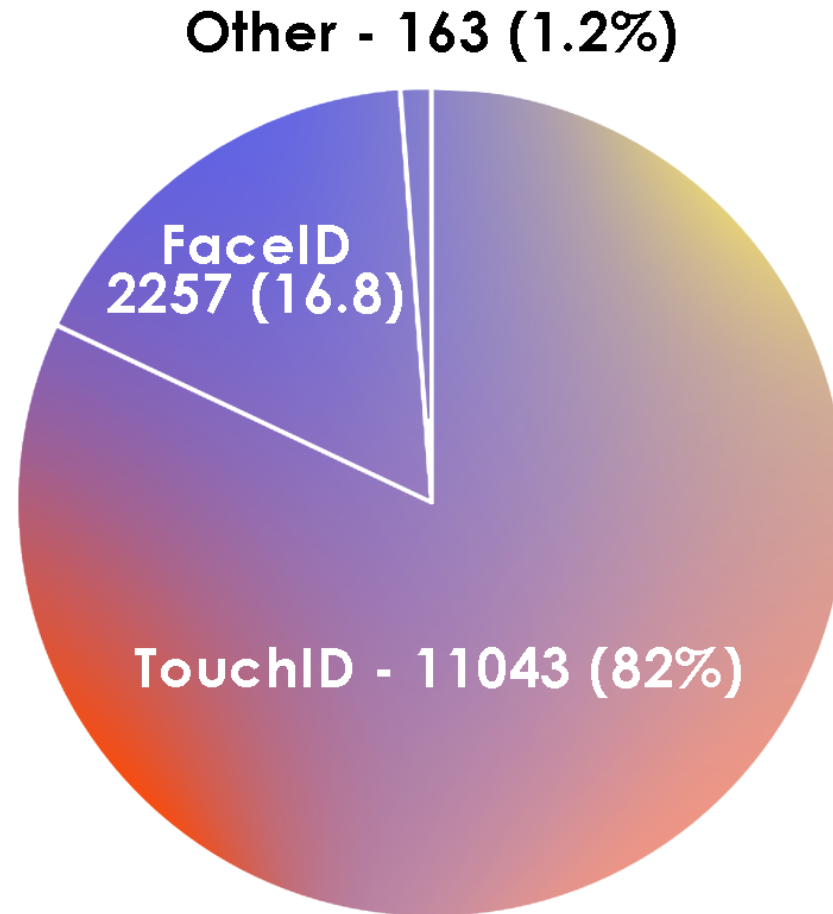


Determined position and profile tolerance values of seen different coloured Lego bricks scanned by Artec Spider

| Target-Actual Comparison | Value 1 | Value 2 | Value 3 | Mean | Standard Deviation | Variation |
|--------------------------|---------|---------|---------|--------|--------------------|-----------|
| Position | 0.5mm | 0.37mm | 0.41m | 0.43mm | 0.067mm | 0.004mm |
| Profile of Surface | 0.6mm | 0.78mm | 0.67mm | 0.68mm | 0.091mm | 0.008mm |
| Profile of a line | 4.63mm | 4.24mm | 4.67mm | 4.51mm | 0.238mm | 0.056mm |

Determined position and profile tolerance values of seen different coloured Lego bricks scanned by the iPad Pro (2020) using TrueDepth

| Target-Actual Comparison | Value 1 | Value 2 | Value 3 | Mean | Standard Deviation | Variation |
|--------------------------|---------|---------|---------|--------|--------------------|-----------|
| Position | 1.10mm | 0.88mm | 1.10mm | 1.03mm | 0.127mm | 0.016mm |
| Profile of Surface | 1.25mm | 1.58mm | 0.57mm | 1.13mm | 0.515mm | 0.265mm |
| Profile of a line | 4.51mm | 5.04mm | 5.2mm | 4.92mm | 0.361mm | 0.130mm |



FaceID vs TouchID