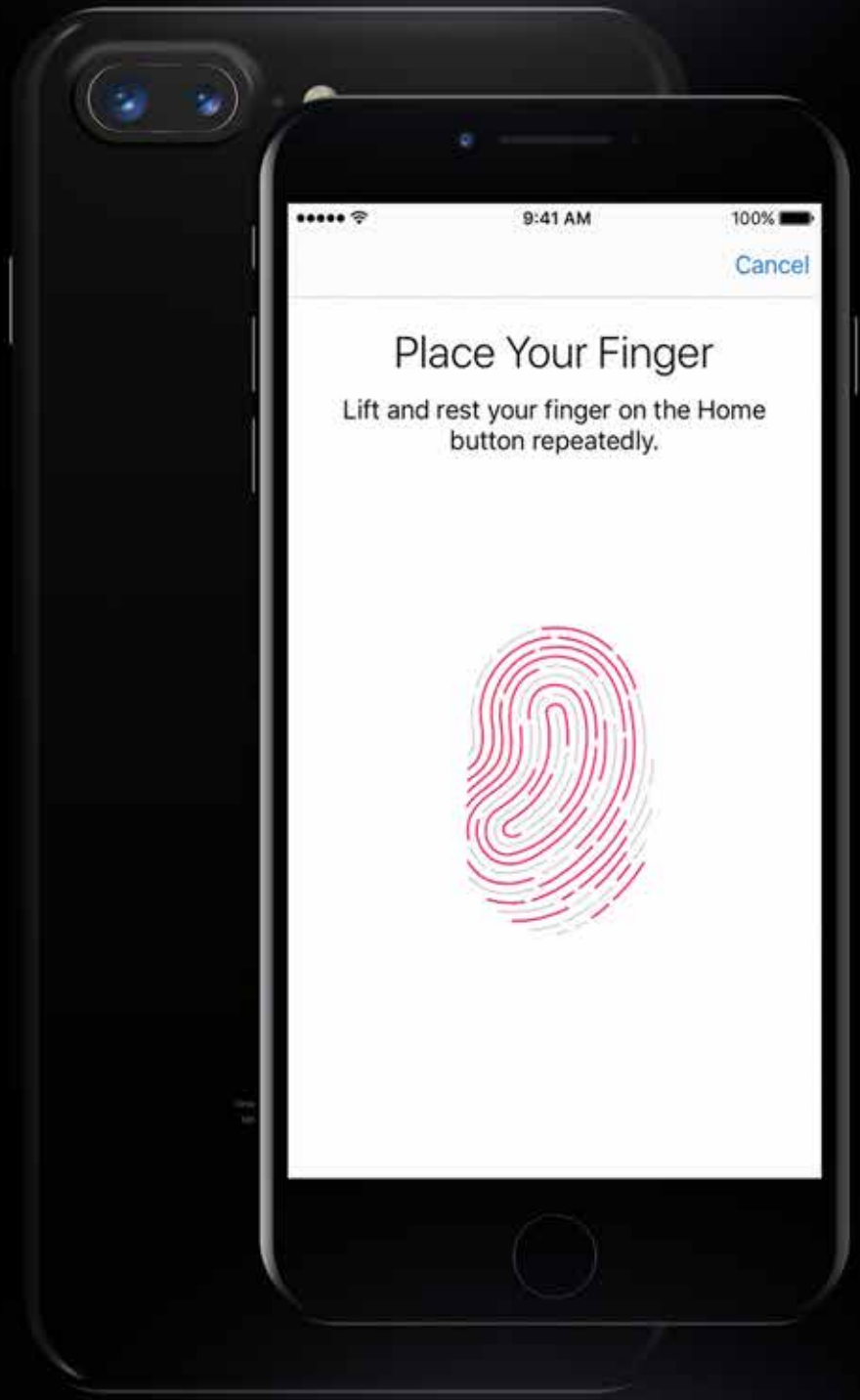
Alex Dunn

Fingerprint Please.....

Is the government storing your personal information?



Fingerprint Please.....

Alex Dunn

Touch ID is a recognition feature which requires the finger being scanned. This allows users to unlock their device, make purchases, and use it as authentication for apps. The feature was first introduced in 2013, and was developed for two main reasons, a stronger security wall (making it harder for hackers) and easier access. This feature paved the way for innovation and technology.

Touch ID works by having sensors placed underneath the home button by which when your finger is placed, scan's your fingerprint. The software, detects the scan by using a 360 degree angle, analysing the layers of skin and categorising them into 3 main sections - *Arch*, *Loop* or *Whorl*.

Arches, are the ridges of the finger which run continuous from one side of the finger to the other with no recurving. *Loops* are ridges which make a backward turn but do not twist. This backward turn, or loop, is differentiated by how the *loop* flows on the hand. *Whorl* are patterns which have two or more deltas (point on a friction ridge at or nearest to the point of divergence of two type lines.) and there exists a recurve preceding each delta.

The software then stores the data allowing the phone to remember the print. In many peoples eyes, **Touch ID** raises many questions on whether the software is secure or not.

1. The most obvious concern is that the system may not work as well as people expect. There were claims in 2013 that **Touch ID** would also perform 3D analysis to avoid being tricked by images of lifted fingerprints. Such claims obviously did not hold up to hackers. Time will also tell how significantly inaccuracy impacts people leveraging the new technology in general, fingerprint based authentication suffers from a problem that either legitimate users are going to occasionally be denied access, or inappropriate users are going to sometimes gain unauthorised access.

2. In many jurisdictions, if you secure your phone with a fingerprint police have the right (without any warrant) to force you to unlock your phone and let them inspect

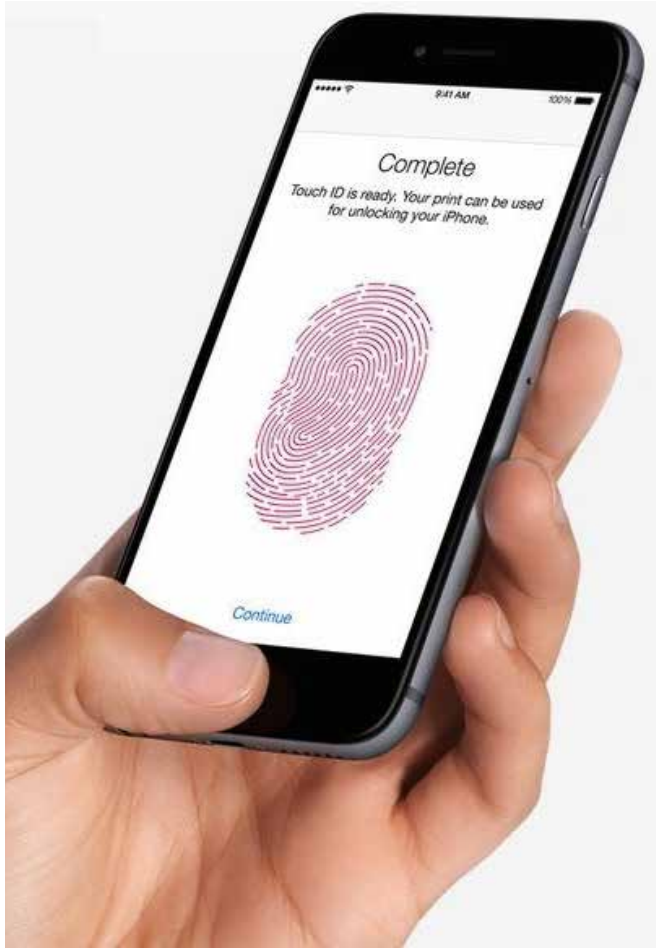
it’s contents, but if you secure your phone with a password law enforcement has no such right.

3. Despite assurances that collected fingerprint data is never actually transmitted from the phone and is processed only in an area separate from the operating system, there remains the risk that criminals may find ways to get to the data. Unlike passwords, fingerprints cannot be reset if a criminal obtains a fingerprint along with the user’s identification information he can potentially use it to steal the user’s identity and commit crimes for decades, evildoers certainly have the incentive to look for ways to steal this information, and will likely invest in technology to do so. Once people are conditioned to trust a phone fingerprint reader, for example, couldn’t criminals potentially sell slightly modified internally devices on the secondary market and capture actual fingerprints?

4. Could the government be asking phone manufactures to create backdoors allowing them to store or send fingerprint information, and to lie to the public about such “ideas”.

There’s always risks when storing credentials anywhere.

Security implications raises questions as it has been fairly easy to trick fingerprint scanning information.



References:

Hall, Z. (2018, September 4). 9TO5MAC. i*Phone won’t embed Touch ID in the display anytime soon. Retrieved from https://9to5mac.com/guides/touch-id/#posts.*

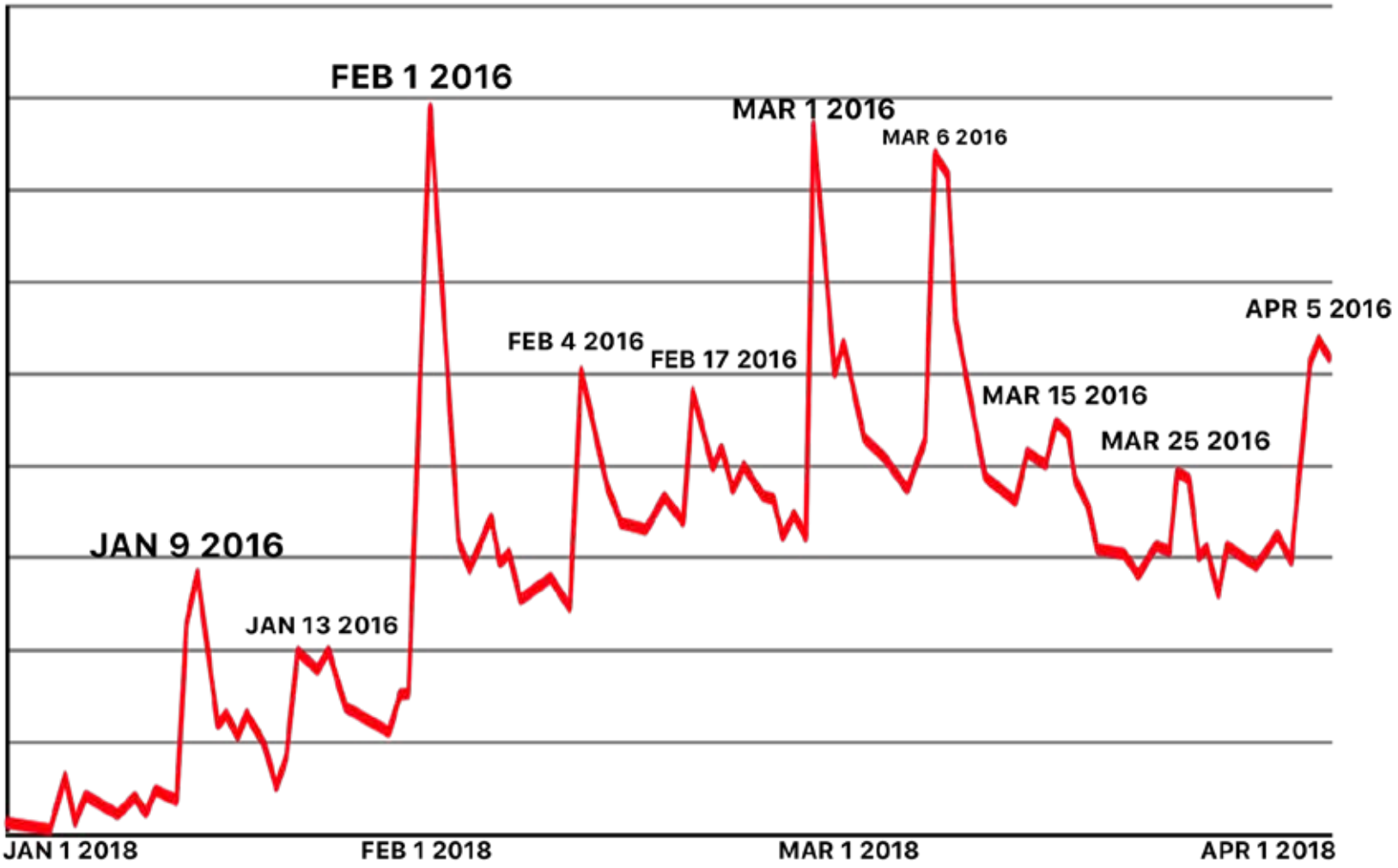
Bump, P. (2013, September 10). The Atlantic: If It Wants Your Fingerprint, the Government Won’t Need Your New iPhone. Retrieved from https://www.theatlantic.com/politics/archive/2013/09/government-has-better-ways-getting-your-fingerprint-your-new-iphone-guys/311232/.

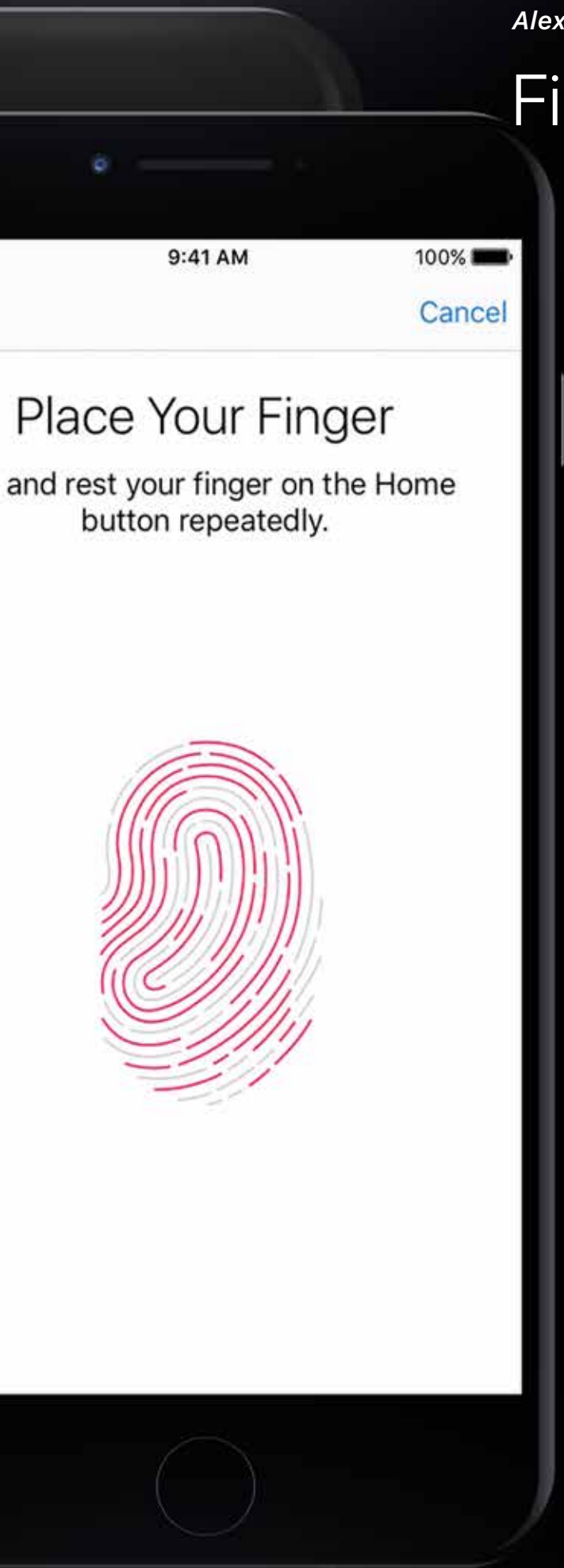
Daniel Matthew L. Biometric Fingerprint System, *Global Health Sciene and Practices. 2015. Vol. 3, No. 1.*

Hamilton, *M. Winton, R. (2016, April 30).* LATimes: *The government wants your fingerprint to unlock your phone. Should that be allowed? Retrieved from: http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html*

Cappelli, R. Ferrara, M. Maltoni, D. SpringerLink, *The Quality of Fingerprint Scanners and Its Impact on the Accuracy of Fingerprint Recognition Algorithms.* 2006. Vol 4105, (Unknown), pg 10-11.

TOUCH ID GLITCH/TAMPERING REPORT





Alex Dunn

Fingerprint Please.....

Is the government storing your personal information?

Fingerprint Please.....

Alex Dunn

Touch ID is a recognition feature which requires the finger being scanned. This allows users to unlock their device, make purchases, and use it as authentication for apps. The feature was first introduced in 2013, and was developed for two main reasons, a stronger security wall (making it harder for hackers)

and easier access. This feature paved the way for innovation and technology.

Touch ID works by having sensors placed underneath the home button by which when your finger is placed, scan's your fingerprint. The software, detects the scan by using a 360 degree angle, analysing the layers of skin and categorising them into 3 main sections - *Arch*, *Loop* or *Whorl*.

Arches, are the ridges of the finger which run continuous from one side of the finger to the other with no recurving. *Loops* are ridges which make a backward turn but do not twist. This backward turn, or loop, is differentiated by how the *loop* flows on the hand. *Whorl* are patterns which have two or more deltas (point on a friction ridge at or nearest to the point of divergence of two type lines.) and there exists a recurve preceding each delta.

The software then stores the data allowing the phone to remember the print. In many peoples eyes, **Touch ID** raises many questions on whether the software is secure or not.

1. The most obvious concern is that the system may not work as well as people expect. There were claims in 2013 that **Touch ID** would also perform 3D analysis to avoid being tricked by images of lifted fingerprints. Such claims obviously did not hold up to hackers. Time will also tell how significantly inaccuracy impacts people leveraging the new technology in general, fingerprint based authentication suffers from a problem that either legitimate users are going to occasionally be denied access, or inappropriate users are going to sometimes gain unauthorised access.

2. In many jurisdictions, if you secure your phone with a fingerprint police have the right (without any warrant) to force you to unlock your phone and let them inspect it's contents, but if you secure your phone with a password law enforcement has no such right.

3. Despite assurances that collected fingerprint data is never actually transmitted from the phone and is processed only in an area separate from the operating system, there remains the risk that criminals may find ways to get to the data. Unlike passwords, fingerprints cannot be reset if a criminal obtains a fingerprint along with the user's identification information he can potentially

use it to steal the user's identity and commit crimes for decades, evildoers certainly have the incentive to look for ways to steal this information, and will likely invest in technology to do so. Once people are conditioned to trust a phone fingerprint reader, for example, couldn't criminals potentially sell slightly modified internally devices on the secondary market and capture actual fingerprints?

4. Could the government be asking phone manufactures to create backdoors allowing them to store or send fingerprint information, and to lie to the public about such "ideas".

There's always risks when storing credentials anywhere.

Security implications raises questions as it has been fairly easy to trick fingerprint scanning information.

References:

Hall, Z. (2018, September 4). 9TO5MAC. i*Phone won't embed Touch ID in the display anytime soon. Retrieved from https://9to5mac.com/guides/touch-id/#posts.*

Bump, P. (2013, September 10). The Atlantic: If It Wants Your Fingerprint, the Government Won't Need Your New iPhone. Retrieved from https://www.theatlantic.com/politics/archive/2013/09/government-has-better-ways-getting-your-fingerprint-your-new-iphone-guys/311232/.

Daniel Matthew L. Biometric Fingerprint System, *Global Health Sciene and Practices. 2015. Vol. 3, No. 1.*

Hamilton, *M. Winton, R. (2016, April 30).* LATimes: *The government wants your fingerprint to unlock your phone. Should that be allowed? Retrieved from: http://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html*

Cappelli, R. Ferrara, M. Maltoni, D. SpringerLink, *The Quality of Fingerprint Scanners and Its Impact on the Accuracy of Fingerprint Recognition Algorithms.* 2006. Vol 4105, (Unknown), pg 10-11.

TOUCH ID GLITCH/TAMPERING REPORT