

User Authentication

Beyond Passwords (2)

Budi Arief

b.arief@kent.ac.uk

Based on slides by Shujun Li

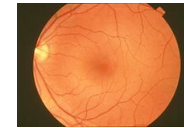
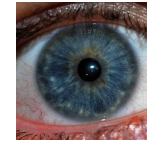
Outline

- Beyond “What You Know”:
 - “Who You Are” (Biometrics)
 - Biometrics: Technical Details
- When Will Passwords Die?
- Summary

Three main classes of biometrics

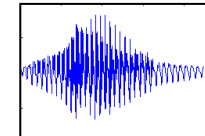
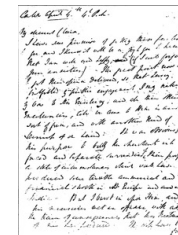
- Physical Biometrics

- Fingerprint, palm, hand geometry, iris, retina, ...



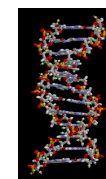
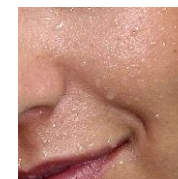
- Behavioural Biometrics

- Handwriting, signature, speech, gait, mouse/keystroke dynamics, ...



- Chemical/Biological Biometrics

- Perspiration, skin luminescence, DNA, body odour, ...



Applications of biometrics

- **User authentication**
- Law enforcement
- Border control
- e-passports and ID cards
- CCTV surveillance
- Customer services
- ...





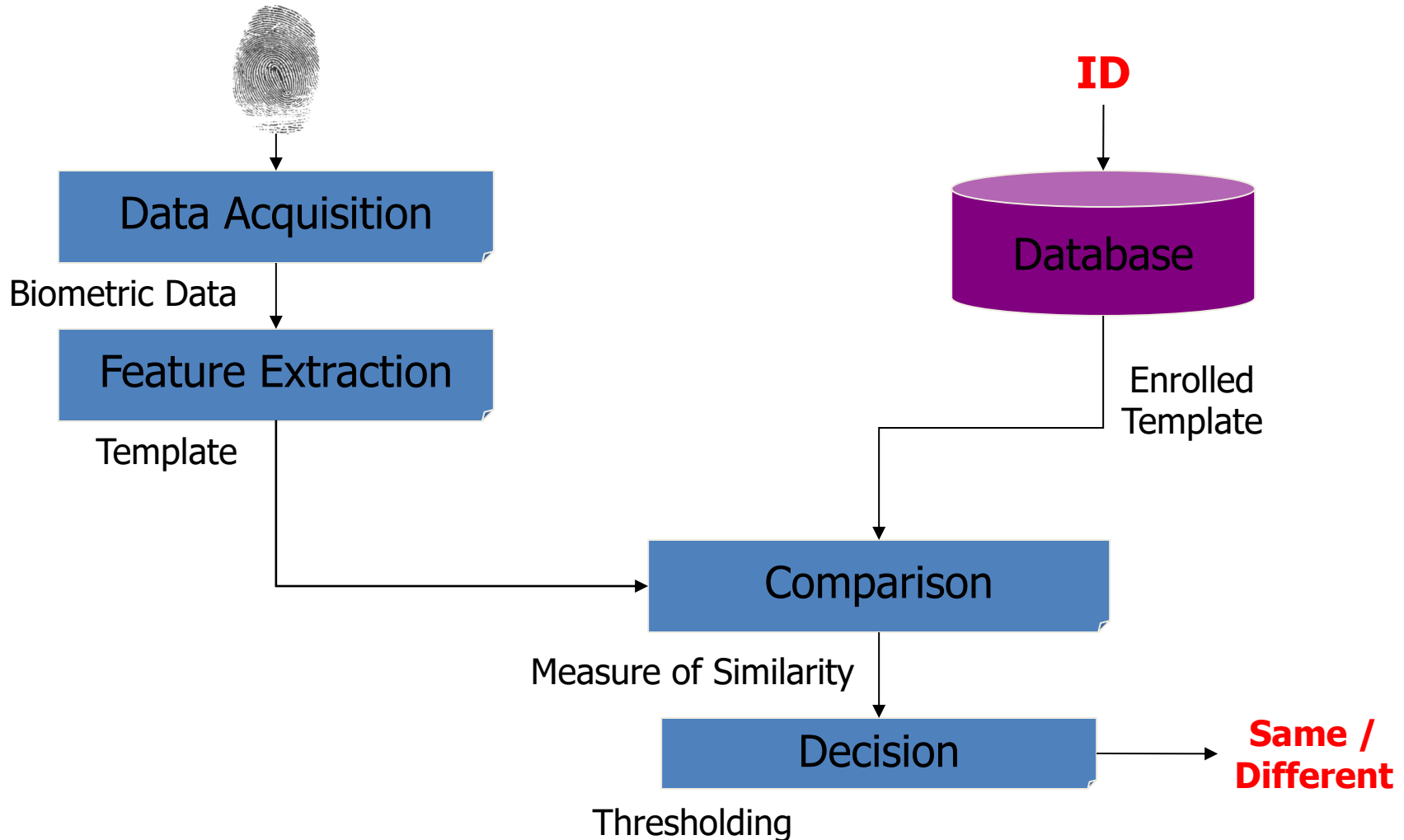
- Can be seen as special cases of **behavioural biometrics**
- Behavioural monitoring \Rightarrow Risk assessment
 - Multiple risk factors around login **behaviours**, including contextual information!
 - Normally used to as the first layer of user authentication, e.g., the following rules may be used:
 - Low risk: no authentication or simpler authentication
 - Medium risk: standard authentication
 - High risk: multi-factor authentication (MFA)
 - Less visible to end users, but widely adopted

Some basic concepts

- Two phases
 - **Enrollment**: capturing biometric features and add them into the database as a **template**
 - Templates are often encrypted to provide confidentiality
 - **Verification/Identification**: matching an input **live template** against one or all enrolled templates
- Two modes
 - **Verification**: checking if a live template matches the enrolled template corresponding to a given ID
 - **Identification**: checking if a live template matches one enrolled template in the database (no ID is given)

Verification mode = 1:1 matching

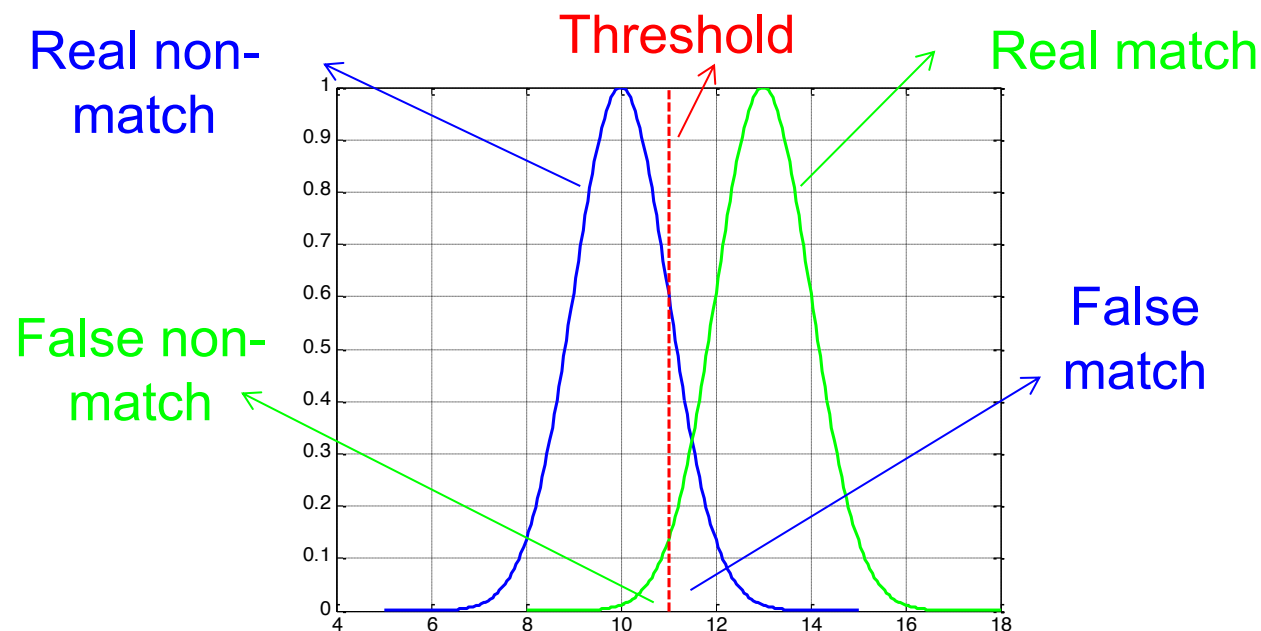
- Input: live template, ID



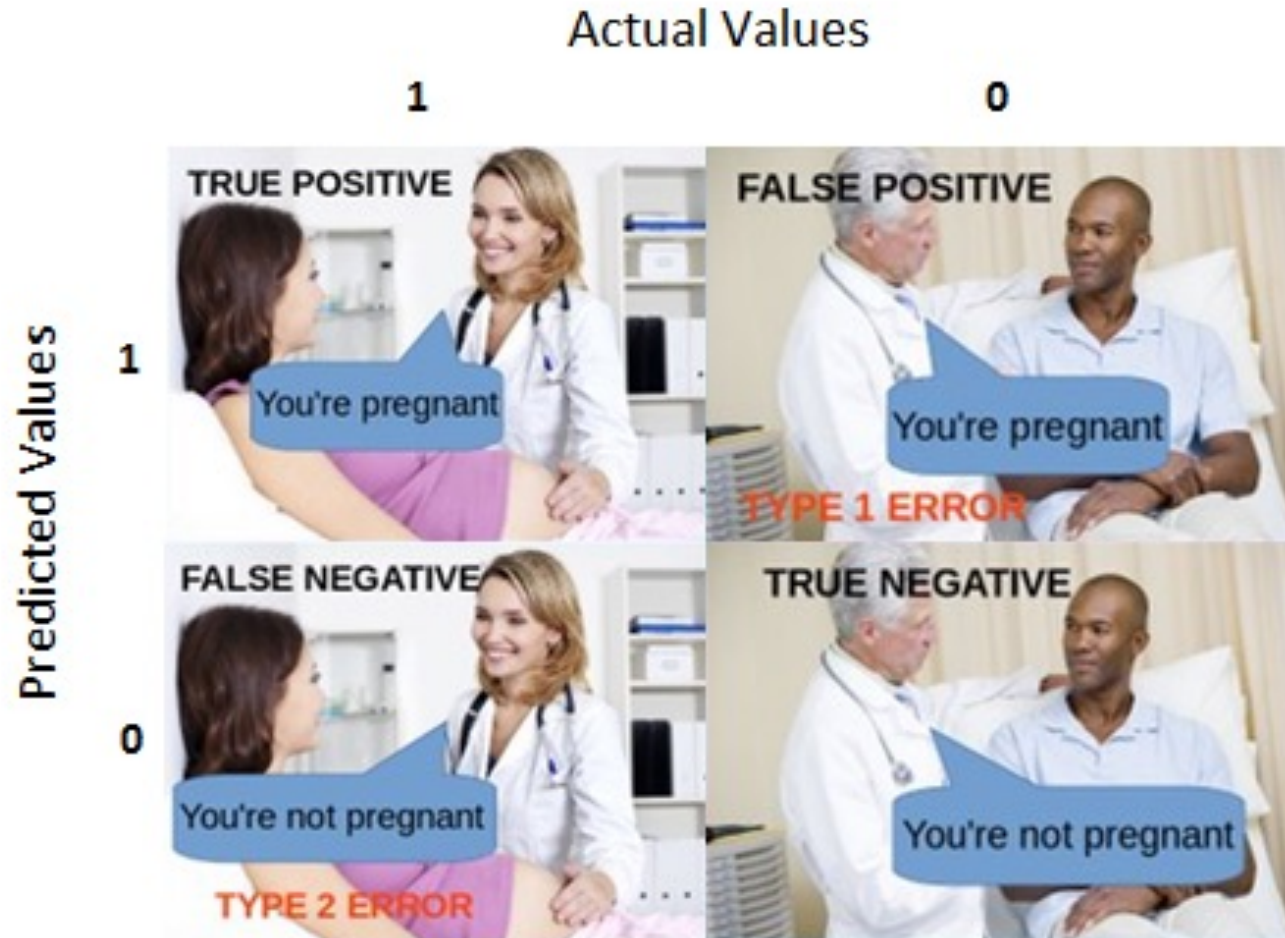
General performance evaluation



- False match rate = **False accept rate (FAR** = False positive rate): User 1 is verified as User 2
- False non-match rate = **False reject rate (FRR** = False negative rate): User 1 is not verified as User 1
- And **failure to enroll (FTE)** rate

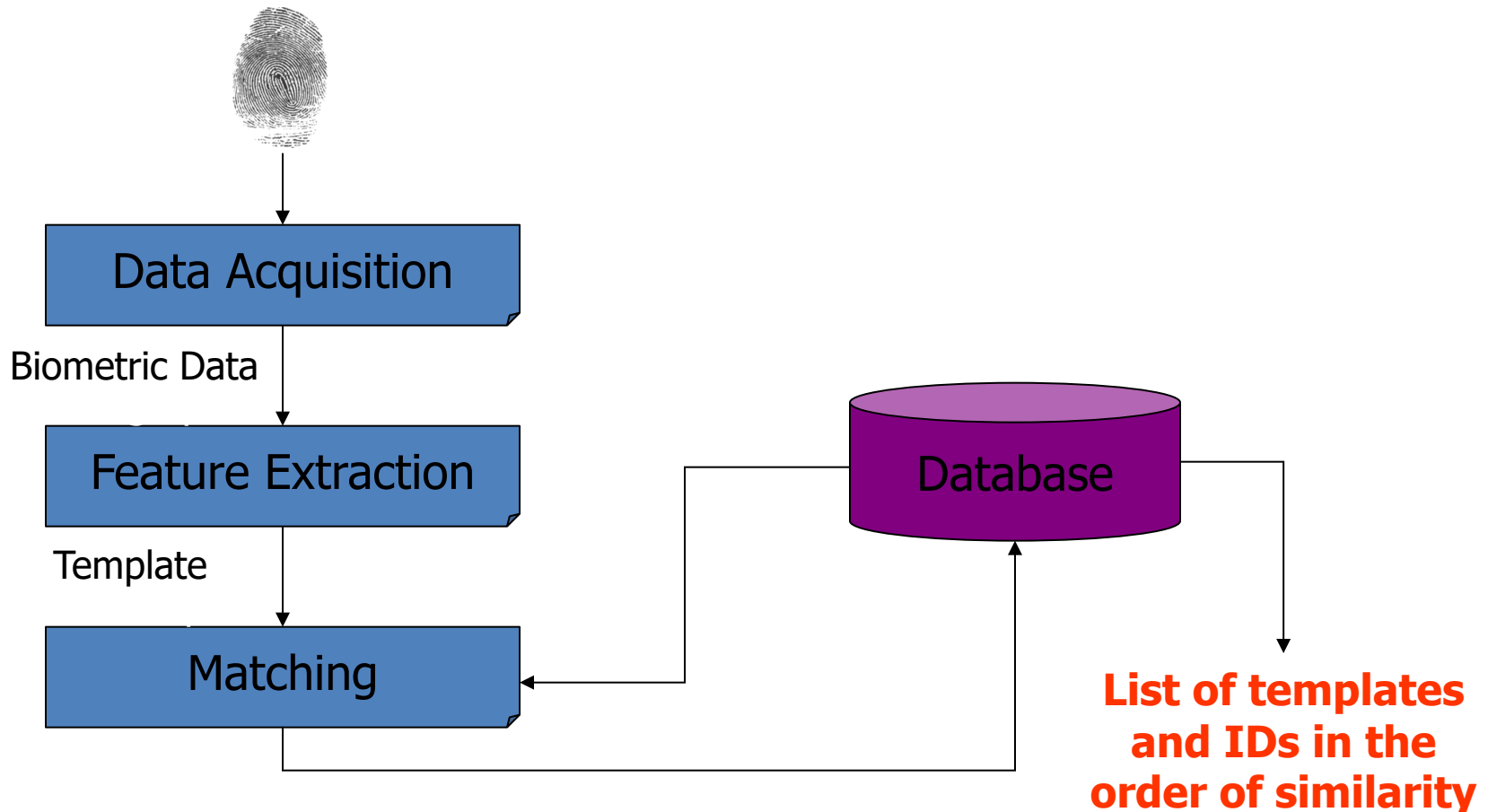


False Positive / False Negative

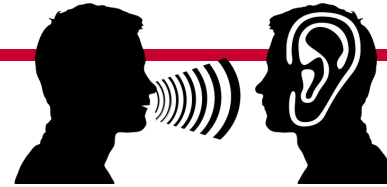


Identification mode = 1:N matching

- Input: live template



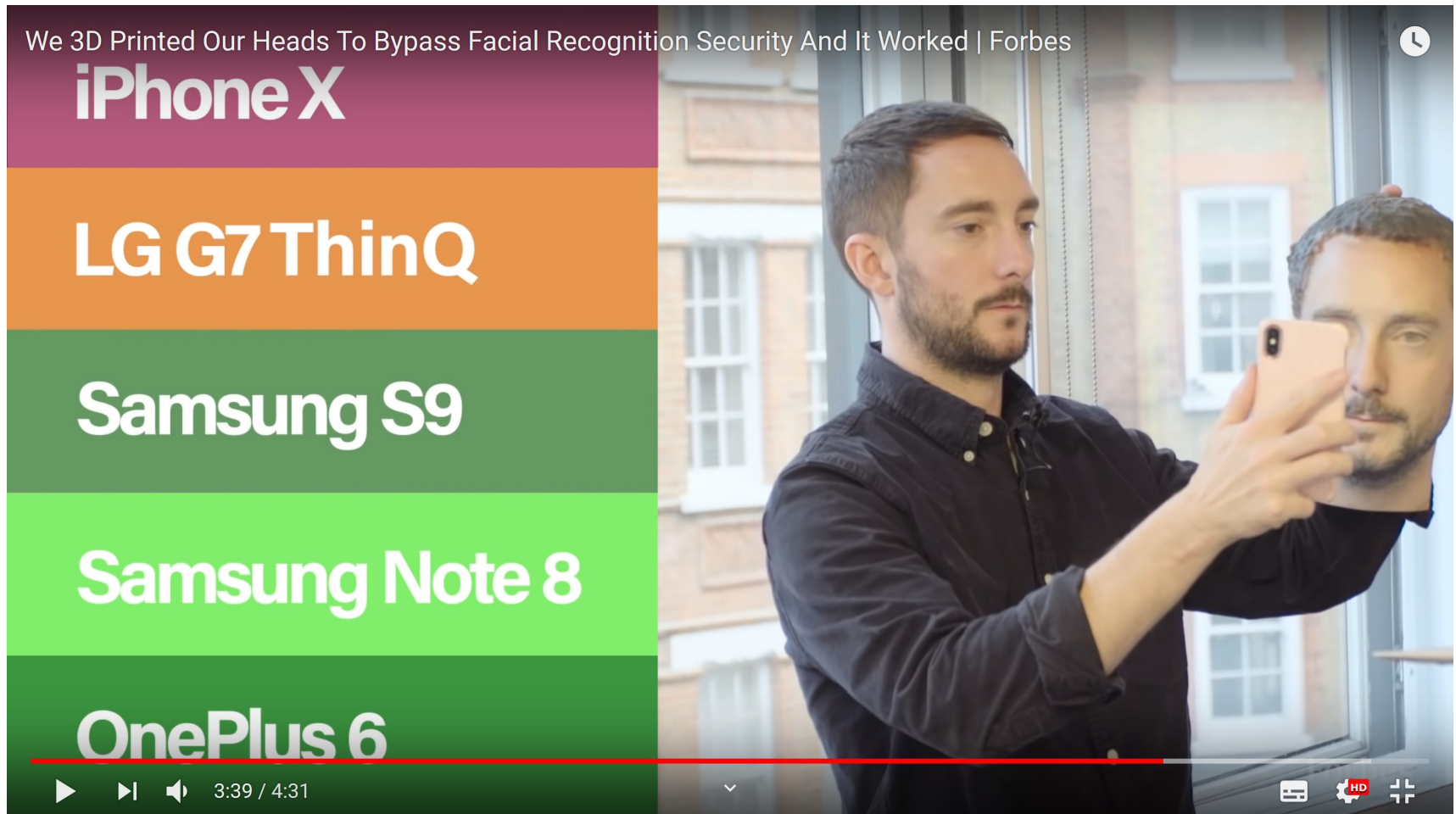
Passive vs Active biometrics



- Passive (covert) biometrics
 - Users do not need to actively submit to data acquisition process
 - Users may even be unaware of the process
 - Main applications: identification – surveillance, customer service, law enforcement, access control, ...
 - Examples: face, speech/voice, gait, mouse/keystroke dynamics, ...

- Active (overt) biometrics
 - Users need to actively submit to data acquisition process
 - Main applications: verification – access control, border control, law enforcement , e-passports and ID cards, ...
 - Examples: fingerprint, iris, hand geometry, retina, ...

Biometrics spoofing



Watch it here: <https://youtu.be/ZwCNG9KFdXs>

A breach in facial recognition!

Facial recognition

Rob Davies

🐦 @ByRobDavies

Mon 29 Nov 2021 20:18 GMT



US facial recognition firm faces £17m UK fine for 'serious breaches'

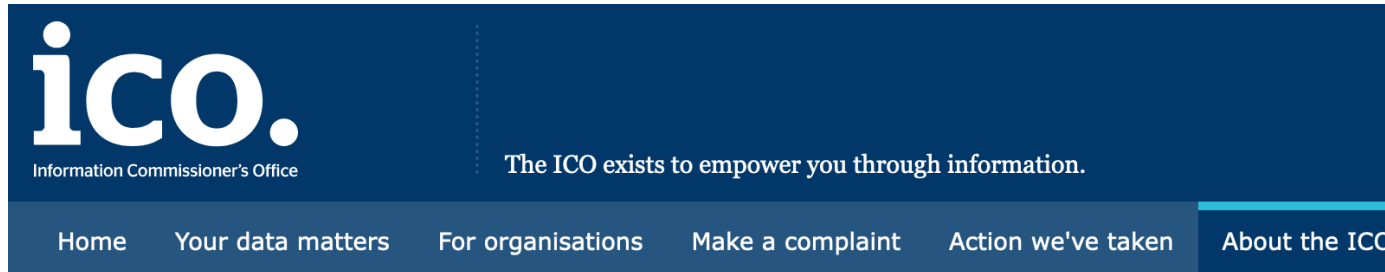
Clearview AI may have gathered data without people's knowledge, says Information Commissioner's Office



📷 Clearview AI is accused of harvesting images from Facebook and other social media sites for use in facial recognition by its clients without people's knowledge. Photograph: Andre M Chang/Zuma Press Wire/Rex/Shutterstock

A US company that gathered photos of people from **Facebook** and other social media sites for use in facial recognition by its clients is facing a £17m fine after the Information Commissioner's Office (ICO) found it had committed "serious breaches" of data protection law.

A breach in facial recognition!



[About the ICO](#) / [Media centre](#) / [News and blogs](#) / [ICO fines facial recognition database company Clearview AI Inc](#)

ICO fines facial recognition database company Clearview AI Inc more than £7.5m and orders UK data to be deleted

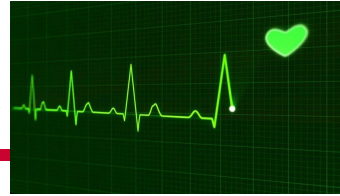
Date **23 May 2022**

Type **News**

The Information Commissioner's Office (ICO) has [fined Clearview AI Inc £7,552,800](#) for using images of people in the UK, and elsewhere, that were collected from the web and social media to create a global online database that could be used for facial recognition.

The ICO has also [issued an enforcement notice](#), ordering the company to stop obtaining and using the personal data of UK residents that is publicly available on the internet, and to delete the data of UK residents from its systems.

The ICO enforcement action comes after a [joint investigation with the Office of the Australian Information Commissioner \(OAIC\)](#), which focused on Clearview AI Inc's use of people's images, data scraping from the internet and the use of biometric data for facial recognition.

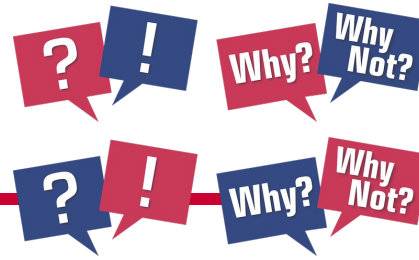


- Liveness detection is about finding solutions to spoofing attacks
- Methods
 - 3D structure (vs. printed 2-D facial images and replayed 2-D video)
 - Natural movement of facial parts (e.g., eyes)
 - Facial expressions and dynamic changes
 - Natural light conditions (e.g., reflection by eyes)
 - Heartbeat detection (via redness detection)
 - ...

Multimodal biometrics

- Use more than one biometric technology
- Can be more accurate than a single biometric technology
 - If used in “AND” mode (pass all)
- Can lower failure to enroll and failure to acquire
 - If one biometric template cannot be measured, switch to the other
 - Increase the population coverage
 - This needs to be under “OR” mode (pass any)
- More difficult to spoof the system
 - If used in “AND” mode (pass all)
- May have to involve multiple capturing interfaces, so more complicated to use, more difficult to manage, and be more costly \Rightarrow Reduced usability

Why biometrics?



- Intrinsic features of human users so no need to create one
- Intrinsic features of human users so cannot be (easily) forgotten or lost
- May be more secure than non-biometric systems?
 - May be more difficult to steal?
 - May be more difficult to forge?
- Accuracy high enough for some biometric modalities and applications (e.g., iris, fingerprint, face)
- Human identification is possible without a given ID
- ...

Why not biometrics?



- **Privacy** issues: misuse of biometric features
 - Private/Anonymous biometrics **may** mitigate this problem
- **Safety** issues
 - Example: in 2005, [Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car](#)
- **Limited security**
 - Many systems are less secure than strong passwords!
- Cannot be easily changed or replaced
 - Cancellable biometric and biometric-based key binding may help solve or relax this problem
- Device dependent
 - Less an issue if only a standard computing device is required

“In-class” exercise



- No biometric system has a 0 error rate!
- Some people cannot even enrol!
 - Non-zero fail-to-enrol rate
- How do current biometrics-based authentication systems address this issue?
 - What would you do?
 - What do real-world systems do?
 - What are the implications?
- Hint: Check how biometrics-based authentication system works on your mobile device

Outline

- Beyond “What You Know”:
 - “Who You Are” (Biometrics)
 - Biometrics: Technical Details
- When Will Passwords Die?
- Summary

General steps of a biometric system

1. Data acquisition (sensing/capturing)

- Passive biometrics vs. Active biometrics
- This step may lead to failure to acquire (e.g., a deaf user cannot have his/her speech captured by a speech biometric system)

2. Live template creation (based on extracted features)

- This step may lead to failure to acquire (e.g., the lighting is so bad that the system cannot take a clear picture of a user's face)

3. Template matching

- Verification vs. Identification: 1:1 matching vs. 1:N matching
- This step causes false reject rate and false accept rate
- Template matching is normally achieved via **pattern recognition** algorithms, so many biometric systems are often called “xxxx recognition systems” (e.g., face recognition systems, fingerprint recognition systems)

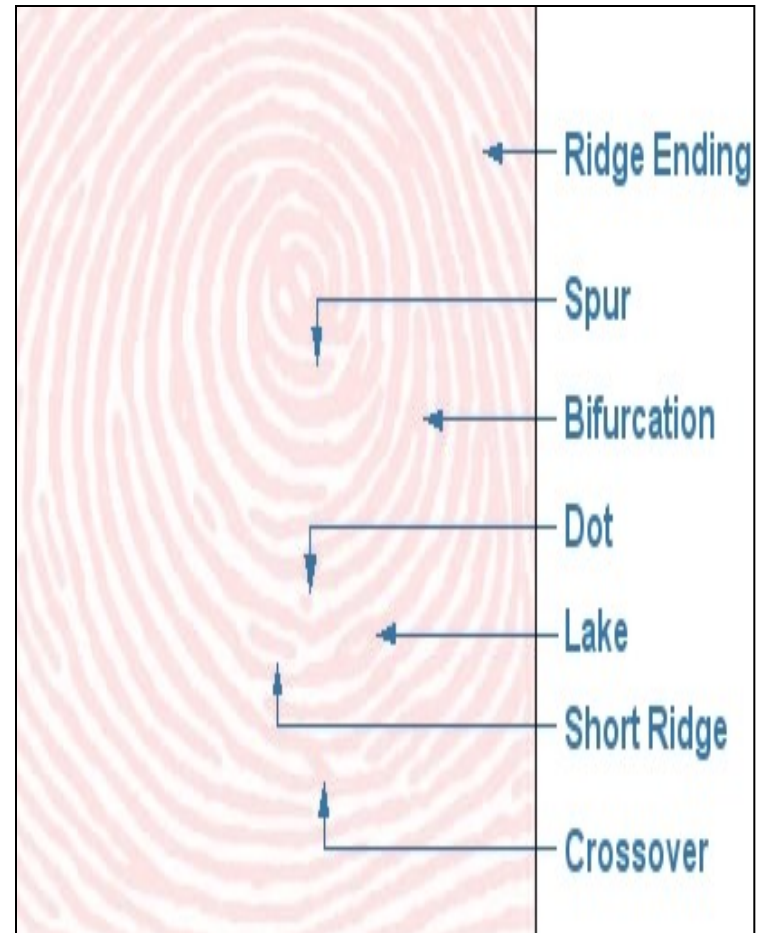
How it works: Fingerprint as an example

- Macro features: global (ridge) patterns
 - Arch (5%): Ridges enter from one side, rise in the center forming an arc and then exit on the other side
 - Loop (60%): Ridges enter from one side and then exit on the same side
 - Whorl (35%): Ridges form circularly around a central point



How it works: Fingerprint as an example

- Micro (local) features: minutiae
 - Position
 - Orientation
 - Curvature
 - Spatial frequency
 - Ridge counts between two minutiae



How it works: Fingerprint as an example

- Typical process of global ridge pattern extraction



Gray-scale image

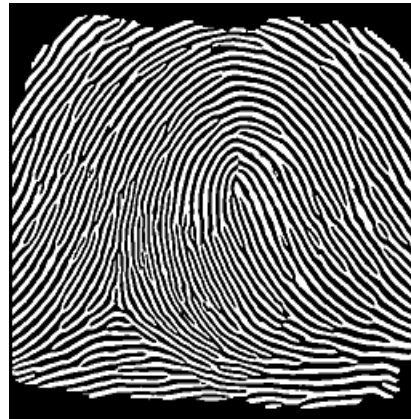
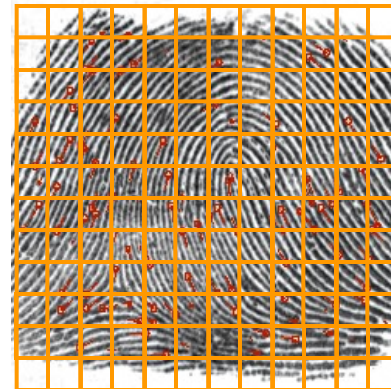
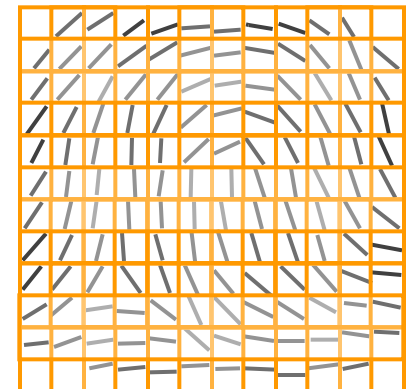


Image Skeleton



Cell definition



Pattern features

How it works: Fingerprint as an example

- Typical process of minutiae extraction



High quality
Gray-Scale Image

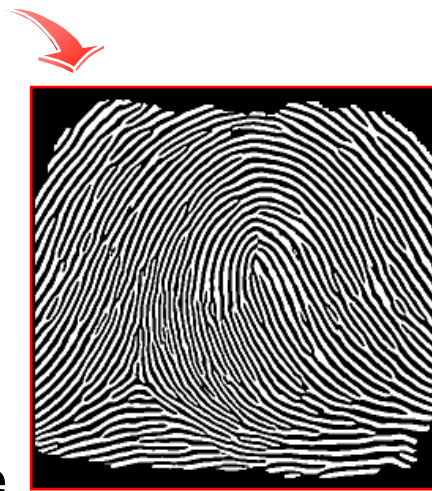
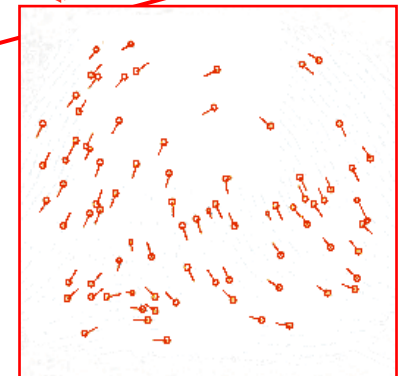
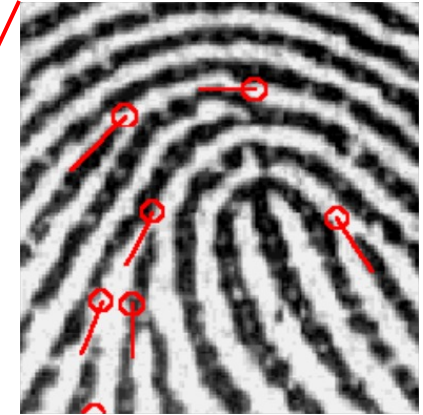


Image Skeleton



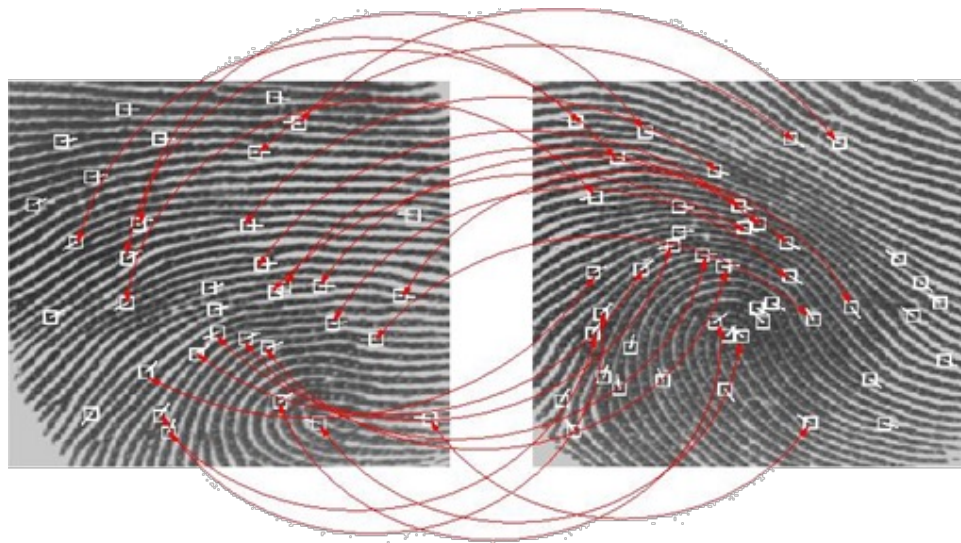
Extraction of
Minutiae



Minutia features

How it works: Fingerprint as an example

- Feature matching
 - Matching should be “elastic” to handle mis-alignment, deformation and missing/noisy minutiae
 - Registration is done by using reference points
 - Number of matched minutiae is usually used as a similarity score




Further readings

- Paul Reid, ***Biometrics for Network Security***, Prentice Hall PTR, 2003
- John D. Woodward, Jr., Nicholas M. Orlans and Peter T. Higgins, ***Biometrics***, McGraw-Hill, 2003
- Stan Z. Li (editor), ***Encyclopedia of Biometrics***, Springer, 2009
- Peter Gregory and Michael A. Simon, ***Biometrics For Dummies***[®], Wiley Publishing, Inc., 2008
- Christian Rathgeb and Andreas Uhl, **A survey on biometric cryptosystems and cancelable biometrics**, *EURASIP Journal on Information Security*, 2011:3, online: <https://jis-urasipjournals.springeropen.com/track/pdf/10.1186/1687-417X-2011-3.pdf>

- Beyond “What You Know”:
 - “Who You Are” (Biometrics)
 - Biometrics: Technical Aspects
- **When Will Passwords Die?**
- Summary

“Passwords will die”? – 2004

- Bill Gates, keynote speech at RSA 2004, 24 February 2004
 - ***“There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don’t meet the challenge for anything you really want to secure.”***
- Many media and people quoted the above like ...
 - Munir Kotadia, “[Gates predicts death of the password](#),” CNET, 25 February 2004



“Passwords will die!” –



- **“You will never need a password again.”***
 - *“You will no longer need to create, track or remember multiple passwords for various log-ins.”* ⇒ Biometrics
 - More [here](#) (texts) and [here](#)* (a YouTube video, from 1:10)



* Note: these links have disappeared (or they have been made private);
Use “Wayback Machine” if you are curious.

“Passwords will die”? – 2017

- Eric Jacksch, “[Practical password policy](#)*,” *IT in Canada Online*, 14 February 2017
 - “Speaking at the **2004** RSA Conference, Bill Gates predicted the demise of passwords saying ...”
 - “In **2011**, IBM predicted that within five years, ‘you will never need a password again.’”
 - “The death of passwords has been predicted by many people.”
 - **“And they are all wrong.”**

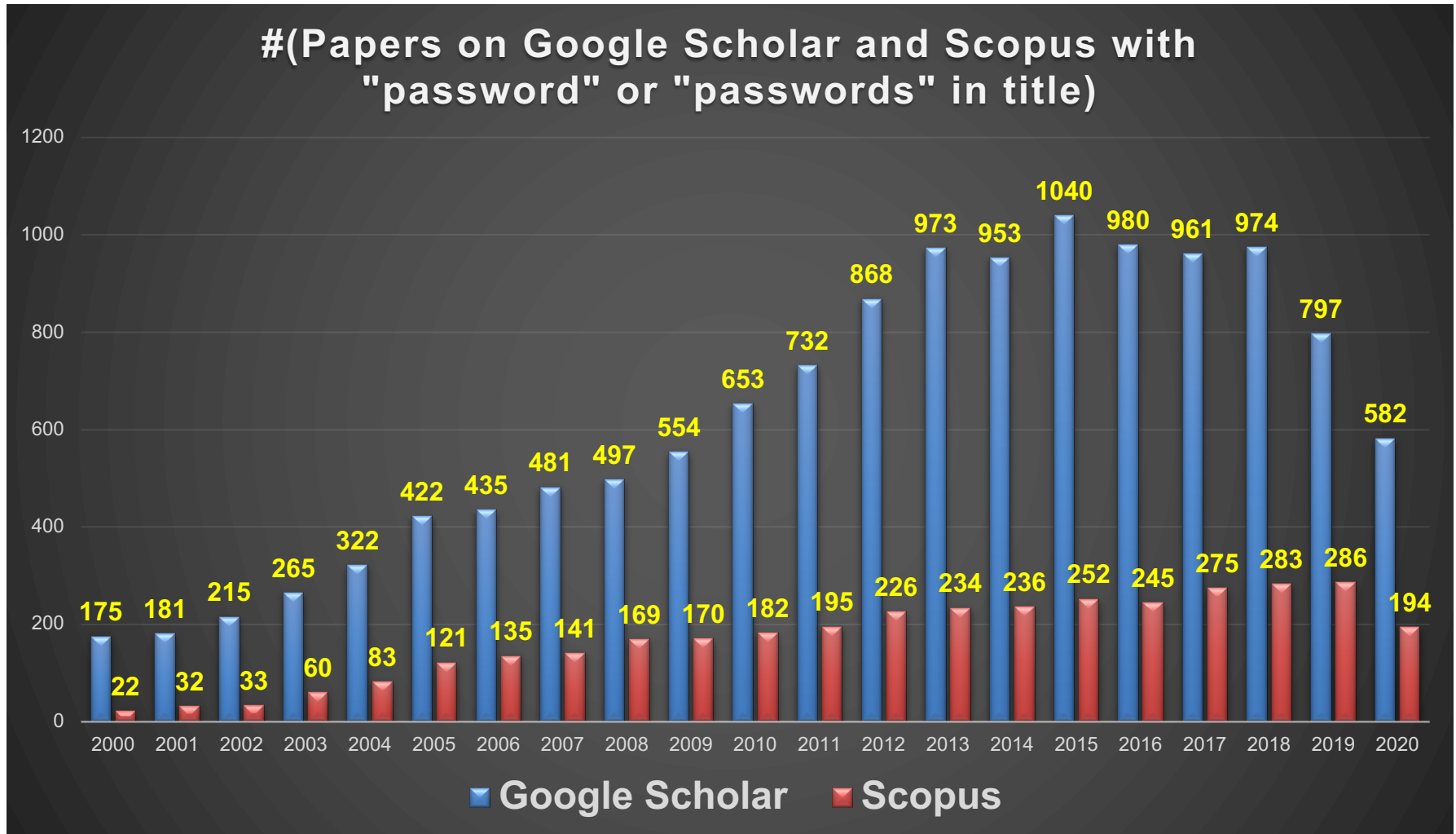


COLUMNIST

ERIC JACKSCH

* Note: this link has completely disappeared, not even on “Wayback Machine”. 33

“Passwords will die”? – 2020



“Passwords will die”? – 10/10/2023



The Keyword

Latest stories

Product updates ▾

Company news ▾



Subscribe

SAFETY & SECURITY

Passwordless by default: Make the switch to passkeys

For Cybersecurity Awareness Month we're making it even easier for users to get started with passkeys

Oct 10, 2023 · 2 min read

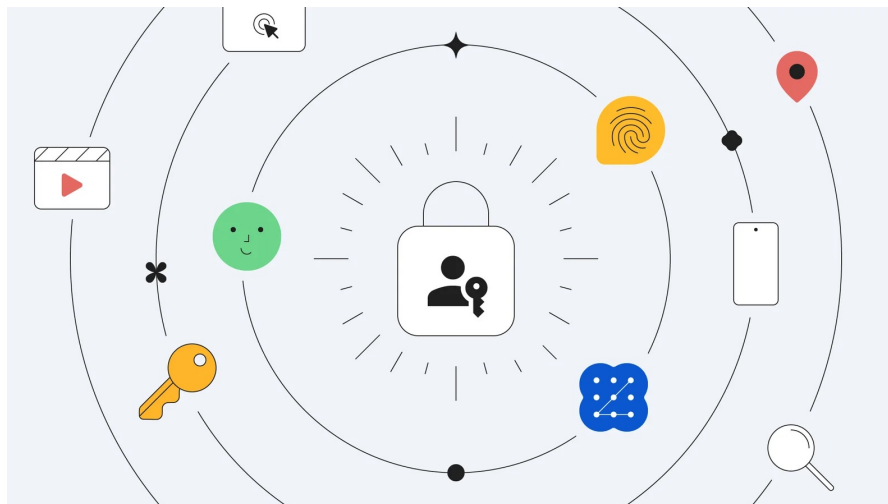


Sriram Karra
Senior Product Manager



Christiaan Brand
Group Product Manager

Share



<https://blog.google/technology/safety-security/passkeys-default-google-accounts/>

Outline

- Beyond “What You Know”:
 - “Who You Are” (Biometrics)
 - Biometrics: Technical Aspects
- When Will Passwords Die?
- **Summary**

Summary

- Biometric is a very useful authentication technique
 - Potentially less effort on the user's side
 - But it is not perfect!
 - Some issues, such as error rates or privacy concerns
- Password is here to stay – at least for now!
- Next week:
 - Non-user authentication
 - Starting on Access Control and Authorisation