

**Leaked today,  
exploited for life**

Jiri Gogela



This is only an excerpt from Trend Micro whitepaper

# Leaked Today, Exploited for Life

available online at

[https://documents.trendmicro.com/assets/white\\_papers/wp-leaked-today-exploited-for-life.pdf](https://documents.trendmicro.com/assets/white_papers/wp-leaked-today-exploited-for-life.pdf)

---

TL;DR

You can change your password, but not your fingerprint...

# Biometric data

# What are biometric identifiers

---

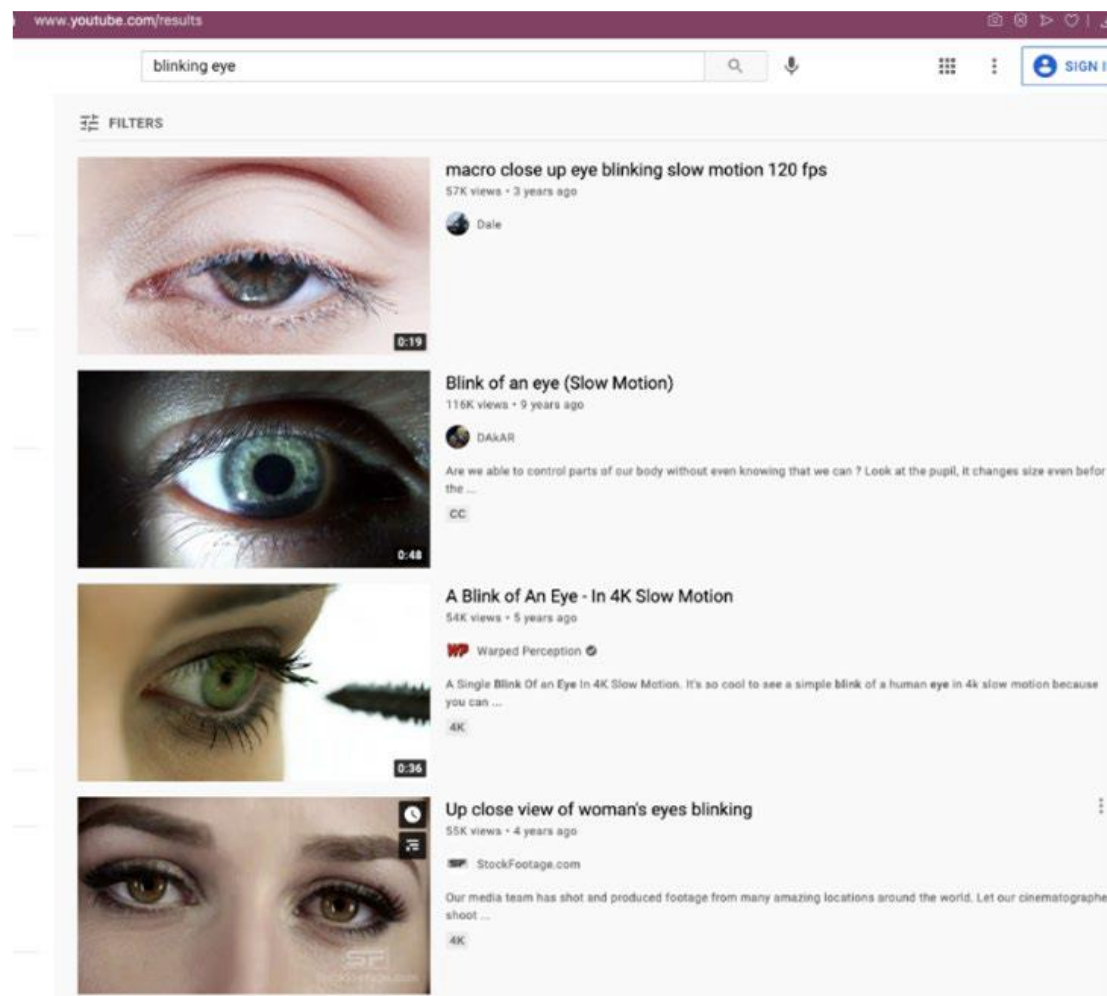
Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals. Biometric identifiers are often categorized as physiological characteristics which are related to the shape of the body. Examples include, but are not limited to [fingerprint](#), palm veins, [face recognition](#), [DNA](#), palm print, [hand geometry](#), [iris recognition](#), [retina](#), odor/scent, voice, shape of ears and gait.

[Wikipedia]

# What is exposed?

# Biometric features

- Fingerprints
- Iris patterns,
- Ear shapes
- Palm shapes
- Voice patterns



# Media types

---

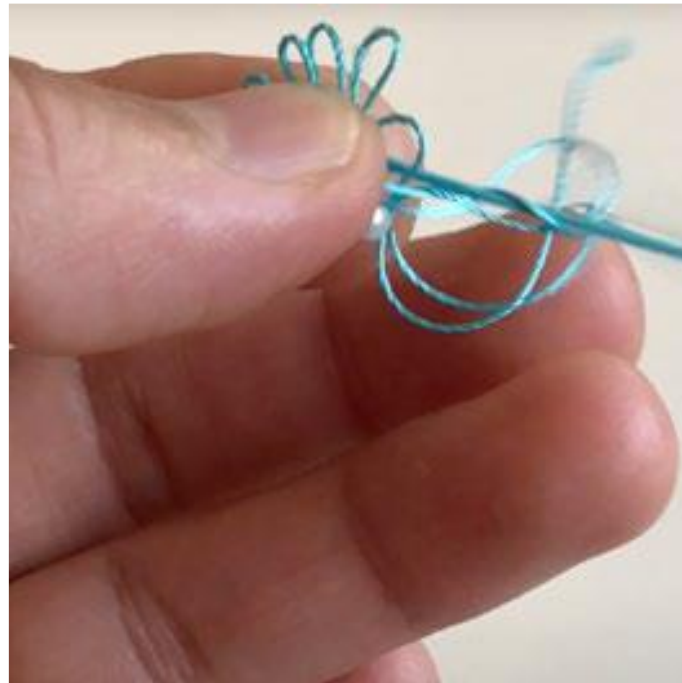
- Photos
- Videos
- Audio recordings
- 3D models



# Where is it exposed?

# Context of the exposure

- Intentional
- Semi-intentional
- Unintentional

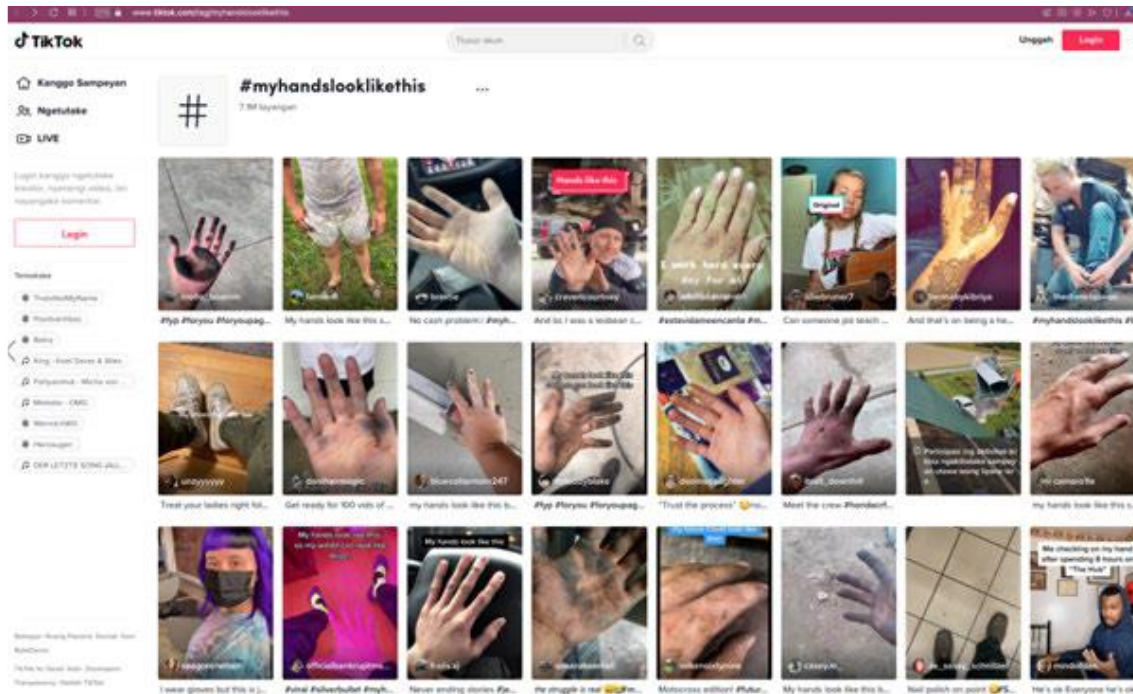


Landlocked Mermaid 🧜‍♀️ @xkrissix · Jan 21  
I got my hair cut (cue dad jokes in 3...2...)



# Social media

- Messaging platforms and social networks



# Web pages of institutions

- High resolution media
- Professional quality
- Metadata available

The screenshot displays the European Commission's Audiovisual Service search interface. The left sidebar contains search filters for keywords, type of media (set to Photo), categories, date range, thesaurus (set to Gender Equality), and topic. The main content area shows search results for 53710 items, with a grid of six thumbnails. Each thumbnail includes a small image, the name of the subject, and a 'View full reportage' button. The detailed view on the right shows a large portrait of Helena Dalli, identified as the European Commissioner for Equality. Below the image is a 'Download' button for a 6720 x 4480 JPG file. A metadata sidebar on the far right provides details such as ID (P-041101/00-01), reportage (P-041101), date (20/09/2019), location (Brussels - EC/Charlemagne), tag (von der Leyen Commission), personalities (Helena Dalli), views (1846), co-operators (Photographer: Lukasz Kotus), and source (EC - Audiovisual Service).

# News outlets

- High resolution
- Detailed metadata



Created: Friday, 1. July 2022 at 19:01  
Modified: Friday, 1. July 2022 at 19:01

Stationery pad  
 Locked

▼ More Info:

Keywords: Male; Man; Men  
Business; Financial;  
Finance  
Asia; Asian; Europe  
Title: ANDREW FORMICA  
Dimensions: 2086 x 1565  
Device make: NIKON CORPORATION  
Device model: NIKON D2X  
Color space: RGB  
Color profile: sRGB IEC61966-2.1  
Focal length: 125 mm  
Description: ANDREW FORMICA  
Executive Officer, of  
ANDREW FORMICA  
speaks during a news  
briefing in Singapore, on  
Thursday, September 3rd,  
2009. Photographer:  
ANDREW FORMICA  
Bloomberg News

Alpha channel: No  
Red eye: No  
Metering mode: Pattern  
F number: f/9  
Exposure program: Manual  
Exposure time: 1/60  
Headline: Henderson Group CEO  
Andrew Formica  
City: Singapore  
Region: Singapore

▼ Name & Extension:  
plans-to-step-down-as  
 Hide extension

▼ Comments:

# 'Device leaks'

NEWS

## Military Device Containing Thousands of Peoples' Biometric Data Reportedly Sold on eBay

German Researchers bought the SEEK II device as part of a security study, and found an alarming amount of information on the

By [Lauren Leffer](#) | Updated December 27, 2022 | [Comments \(3\)](#) | [Alerts](#)



<https://gizmodo.com/eBay-military-seek-ii-afghanistan-data-1849930714>

## THE TALIBAN HAVE SEIZED U.S. BIOMETRICS DEVICES

Biometric collection and identification devices were seized last week during the Taliban's offensive.



[Ken Klippenstein](#), [Sara Sirota](#)

August 18 2021, 12:11 a.m.

**THE TALIBAN HAVE** seized U.S. military biometrics devices that could aid in the identification of Afghans who assisted coalition forces, current

<https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/>

# Other sites

---

<http://pf.bigpixel.cn/zh-CN/city/1.html>

# Biometric use cases



# Existing use cases

---

- Access to Own Devices
- Access to Buildings
- Schools
- Healthcare
- Banking
- Critical Events
- Border Crossing and Airport Security
- National Digital Identities and Law Enforcement Biometric Databases

# Future

---

- Contactless Transparent Payment in Next-Generation Shops and Public Transport (Moscow, Dubai – facial recognition)
- Censuses, Polls, and Voting (Nigeria)
- Social Scoring Systems (China, insurance industry)

# Possible attack scenarios

# Data Collection attack scenarios

- Passive Biometric Data Collection
- Active Biometric Data Collection
  - Attacks on Sensors
  - Attacks on Databases
  - Abuse of API and Export Features

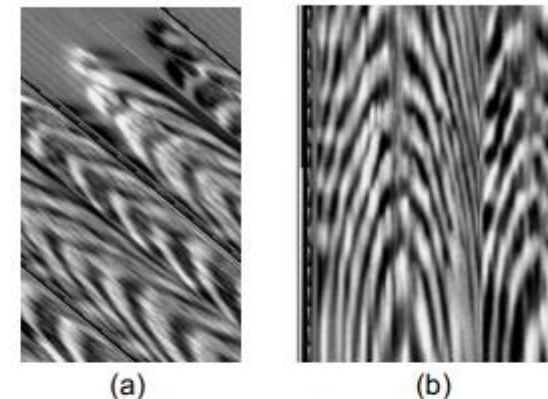


Figure 5: Fingerprint bitmap obtained from HTC One Max. Both the raw b aligned version (b) are shown. We only pasted a small portion of the im fingerprint owner's anonymity.


<https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf>

# Identity Theft and Impersonation Attacks

---

- Deepfakes
  - Criminal Monetization of Deepfake Technology
  - Attacks Using Deepfakes During Critical Events
- Abuse of Smart Devices
- Tricking Tech Support to Take Over Accounts
- Faking the Presence of a Person at a Particular Place or Event
- Abuse of Reputation Using Impersonation Attacks
- Abuse of Social Scoring Systems

## NEWS

 Xinmei Shen · 27 Nov 2018 · 2 min read

### **Businesswoman in China caught ‘jaywalking’ because her face was on a bus**

Chinese cities have widely deployed facial recognition systems on their streets

# Attacks With Identification

- Tracking and Automated Identification of a Person and Their Habits
- Identification of Communities Where People Communicate
- Creating Contexts for Extortion or Manipulating Public Opinion Based on Exposed Media
- Identification of People at Critical Events



<https://edition.cnn.com/2021/05/25/uk/drug-dealer-cheese-sentenced-scli-gbr-intl/index.html>

# Attacks on Authentication

- Abusing Local Authentication Mechanisms
  - Unlocking a Laptop, Phone, and Other Gadgets
  - Opening a Biometric Door Lock
  - Next-Generation Retail, Public Transport Payments, and Cash Withdrawal



Figure 22. An array of high-precision fake fingers modeled from index, middle, and thumb fingers from 20 subjects<sup>101</sup>

<https://www.ndss-symposium.org/wp-content/uploads/2022-82-paper.pdf>

# Suggestions



# General Suggestions

---

- Minimize exposure of biometric patterns.
- Minimize reliance on biometric factors that are commonly publicly exposed or have a high possibility of exposure.
- Minimize the quality of exposed media or the parts of exposed media that potentially contain biometric features.
- For users who are widely seen in public media and are recorded in high resolution, assume that all meaningful biometric data is already exposed or at very high risk of exposure.

# Suggestions for Organizations Handling Biometrics

---

- Use separate security processes for trusted and untrusted environments. Trusted environments are those that are supervised and controlled by an organization or trusted partner sensors, while untrusted environments are sensors or environments controlled by the individual who submitted the biometric features.
- Use biometrics for single-factor authentication for non-critical assets and tasks only, or use it as just one factor in MFA based on “something you know” and not just “something you are.” This should be considered specifically for untrusted environments.
- Ensure the security of storage, processing, and the whole life cycle of business processes that rely on biometrics.
- Secure biometric patterns in a way that minimizes the consequences of potential data breaches. Increase awareness about the existence of deepfakes, specifically focusing on real-time implementations that can be adopted for conference calls.

# How to Handle Your Own Biometrics

---

- Be aware of each major biometric data type at risk of exposure: face, voice, fingerprint, palm, and iris.
- Limit exposure of all biometric features, especially fingerprint, palm, and iris patterns.
- Minimize the quality of exposed media and modify sensitive areas of posted media.
- Review media carefully before sharing anything online for intended exposure.
- Control and manage access rights on media platforms properly.
- Regularly conduct a media search of your own image and check the context in which the images appear. Reverse image search tools such as Google Images are useful for this. This is a form of reputation management that can mitigate any misuse of your personal image and minimize reputational damage. For example, malicious actors might misuse real images of you, or they might create and abuse deepfakes of you.

# Additional considerations

---

- For the use of biometrics, one option is to use a strategy similar to network segmentation. Separate the potential use of biometrics into segments like government service usage, finance, building access, and so on. Prioritize biometric features according to how easily each can be sourced publicly. Face and voice, for example, are easy to source, while fingerprints and iris patterns are more challenging. Use less exposed features depending on the sensitivity of the account or service you are authenticating.
- For the purpose of identification, use what is potentially publicly exposed. For authentication, use what is not publicly exposed.
- Use what is potentially not exposed for single-factor biometric authentication. If there is no other choice, use potentially exposed biometrics as part of MFA, not as a single factor. If fingerprints are required for several types of services, use different fingers for different services, or alternate between each hand.
- Separate requirements and expectations for remote and local authentication, as well as for supervised and not supervised authentication. If you are passing border control, you may use a picture to authenticate yourself. If, however, you are authenticating a login from your home to a remote network, then it is a completely different scenario.
- Be very careful when exposing your biometrics to new types of services and technologies. Newly launched technology often means zero or a low level of regulation. There is a higher probability that exposed data will be abused and misused.
- When creating media content, especially using professional equipment, use the equipment itself to minimize exposure. This is exactly the case for political figures, CEOs, and celebrities, especially in live-streaming scenarios. (For example, distributed and multiple sources of light can lead to multiple reflections on the iris and minimize the exposed area. The use of a single point of light, which is reflected in the middle of your pupil, increases the chance of successfully capturing the iris from exposed media.)

# Full document

---

Available at:

<https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/leaked-today-exploited-for-life-how-social-media-biometric-patterns-affect-your-future>

