



# Leaked Today, Exploited for Life

## How Social Media Biometric Patterns Affect Your Future

Craig Gibson, Vladimir Kropotov, Philippe Z Lin, Robert McArdle, Fyodor Yarochkin



## TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

**Trend Micro Research**

Written by

**Craig Gibson,  
Vladimir Kropotov,  
Philippe Z Lin,  
Robert McArdle,  
Fyodor Yarochkin**

Trend Micro

Stock image used under license from  
Shutterstock.com

*For Raimund Genes (1963-2017)*

# Contents

5

What is Exposed?

31

How This Affects People: Current  
and Future Attack Scenarios

44

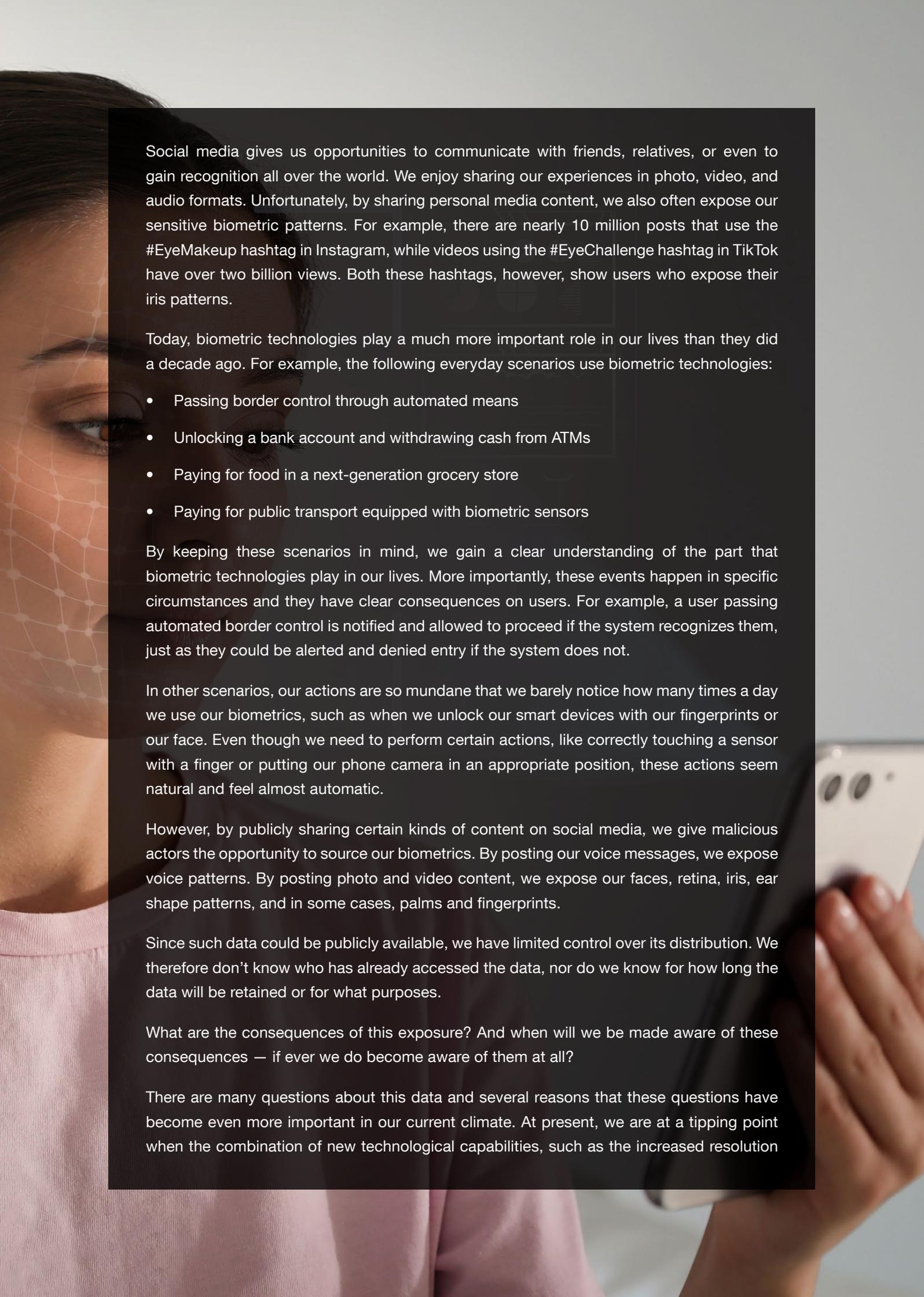
Advice for Readers

48

Conclusion

50

Appendix



Social media gives us opportunities to communicate with friends, relatives, or even to gain recognition all over the world. We enjoy sharing our experiences in photo, video, and audio formats. Unfortunately, by sharing personal media content, we also often expose our sensitive biometric patterns. For example, there are nearly 10 million posts that use the #EyeMakeup hashtag in Instagram, while videos using the #EyeChallenge hashtag in TikTok have over two billion views. Both these hashtags, however, show users who expose their iris patterns.

Today, biometric technologies play a much more important role in our lives than they did a decade ago. For example, the following everyday scenarios use biometric technologies:

- Passing border control through automated means
- Unlocking a bank account and withdrawing cash from ATMs
- Paying for food in a next-generation grocery store
- Paying for public transport equipped with biometric sensors

By keeping these scenarios in mind, we gain a clear understanding of the part that biometric technologies play in our lives. More importantly, these events happen in specific circumstances and they have clear consequences on users. For example, a user passing automated border control is notified and allowed to proceed if the system recognizes them, just as they could be alerted and denied entry if the system does not.

In other scenarios, our actions are so mundane that we barely notice how many times a day we use our biometrics, such as when we unlock our smart devices with our fingerprints or our face. Even though we need to perform certain actions, like correctly touching a sensor with a finger or putting our phone camera in an appropriate position, these actions seem natural and feel almost automatic.

However, by publicly sharing certain kinds of content on social media, we give malicious actors the opportunity to source our biometrics. By posting our voice messages, we expose voice patterns. By posting photo and video content, we expose our faces, retina, iris, ear shape patterns, and in some cases, palms and fingerprints.

Since such data could be publicly available, we have limited control over its distribution. We therefore don't know who has already accessed the data, nor do we know for how long the data will be retained or for what purposes.

What are the consequences of this exposure? And when will we be made aware of these consequences — if ever we do become aware of them at all?

There are many questions about this data and several reasons that these questions have become even more important in our current climate. At present, we are at a tipping point when the combination of new technological capabilities, such as the increased resolution

smartphone cameras, media platform support for 4K videos and high-resolution photos, cloud and data mining, and AI and machine learning (ML) capabilities are bound to change the security risks significantly.

This melting pot of innovations is already starting to lead to niche uses of biometric data. For example, surveillance cameras track individuals based on facial recognition algorithms that are trained with the individual's own data as previously uploaded on social media.<sup>1</sup> Cybercriminals could leverage the same data from social media to launch identity theft attacks or generate deepfakes (especially deepfakes of public figures).

The same social media data could also be leveraged in identity theft attacks, government surveillance, or the generation of deepfakes (especially fakes of public figures). Although the financial criminal use of this data is still low today, the barrier for entry will only continue to fall, and with it the scale of misuse will also increase over time.

At first glance, biometrics seem like an all-in-one solution; they are something unique that can be used for identification and authentication and are always with you. For decades, biometrics have been used for several niche applications: to facilitate criminal investigation and forensics or to access government buildings, for example. Today, the role of biometrics has expanded, and hundreds of millions of people use it on a daily basis. Unfortunately, this also means that the same number of people could fall prey to the vulnerabilities and weaknesses of technologies and processes involved in biometric data processing.

To evaluate the risks, we decided to investigate known use cases that rely on biometrics now or will rely on them in the near future. We also investigated underlying technologies that are used by biometric systems for identification and authentication. Unfortunately, when multimedia content is published, many people are not aware how sensitive this content is. Naturally, it follows that they don't know the current and future risks of such content exposure.

The purpose of this paper is to highlight the important points that users need to know about publishing content on social media, which of their sensitive information might have already been exposed or could still be exposed from their published content, and how the publication of such content can affect not just individual lives but also the day-to-day operations of organizations that use or process biometric data. We also describe current and imminent attack scenarios that use today's exposed biometric features and behavioral data. Lastly, we provide recommendations on how to minimize risks related to the exposure and use of biometric data.

# What is Exposed?

This section focuses on the types of exposed content and variety of social media platforms where such content is exposed. The features that people expose are either static or dynamic. Static features can be taken from a single photo frame and could be enough to expose biometric patterns for malicious intent. Face shape, iris, retina, palm, and fingerprints are examples of such features.

Dynamic features require more time to be captured because they are often leaked in video and voice recordings. Voice patterns or the way that people express emotions are examples of dynamic features. Many of these patterns are exposed when one observes the way people behave, such as the way a person types on a keyboard, navigates browser windows, writes by hand, or signs papers. All these features can be used for both authentication and identification.

Together with the well-known features we have already described, there are other non-biometric unique features that can be used to identify or categorize people. These features include non-detachable (or nearly non-detachable) features like birthmarks or tattoos. Similarly, detachable features like clothes and accessories could be used to profile social status, ethnicity, and age. Cybercriminals could even use designer clothes and accessories like sunglasses, hats, and bags posted on social media to launch attacks on people who upload such content.<sup>2</sup>

This section also covers and highlights the context of content exposure since not all content is exposed intentionally. For example, fingerprints are often exposed in video tutorials on how to cook miniature food, while iris patterns are usually exposed in makeup-related content. These types of content entail many risks that are still unaddressed, which makes it paramount to spread awareness among owners, producers, and hosts of media content as to what situations lead to the risk of exposure.

The considerable difference between the unintended exposure of biometrics a decade ago and exposure now is the quality and resolution of the media content. Quality and resolution have significantly increased, and this allows actors to extract features with higher quality for biometric enrollment and other biometric systems.

# Types of Content

There are currently three types of content that are prevalent in social media: photo, video, and audio recordings. What is important to note here, however, is that metadata, descriptions, comments, and hashtags make such media content searchable, thereby allowing more insights on the context of their exposure. Media content itself or its description often includes information about behavior, mood, and emotions, which can be also used in different attack scenarios.

## Audio Recordings

By posting our voice messages, we expose voice patterns together with our mood, emotions, and background noise. Recording metadata could also provide insights on the time, location, and environment of the recording. More importantly, a collection of these different patterns recorded in different environments can help an attacker bypass security systems that are based on challenge-response. For example, a system can require a user to pronounce a phrase from a given list or a random phrase for authentication, and this requirement could be bypassed by a simulated voice trained from exposed recordings. Voice is often exposed when we send voice messages using messaging platforms or share videos that include an audio track.

## Photos and Videos

In photos and video content, our faces, retina, iris, ear shape patterns, and in some cases, our palms and fingerprints are exposed.

Photos are static, which means they are limited in terms of behavioral information exposure, but they often contain metadata, insights about emotions, time, location, and details about the environment. Videos can be treated as a long sequence of photos that often include an audio track. As a result, they expose nearly everything that photos expose, only on a larger scale. Videos also include patterns exposed in voice messages, except with more detailed behavioral and environmental data.

## 3D Models

3D models of body parts are not exposed at the scale of audio, photo, or video content. Nevertheless, all necessary technologies to extract the details of these 3D models are already in place, making it possible to find 3D scans of faces.<sup>3</sup>

The transition of social media content to the metaverse can lead to the mass appearance of 3D models, which can be printed and potentially used to trick biometric sensors.<sup>4</sup> People will also try to make their metaverse avatars more realistic representations of their real-world selves.

In the near future, with the expansion of surveillance, broadening virtual reality-, augmented reality- and metaverse reality-related technologies, autonomous delivery, military drones using facial recognition,<sup>5</sup> and self-driving cars capable of capturing and consuming biometrics among other similar technologies, the exposure of our physical and behavioral biometric patterns is expected to increase.

# What Social Media Platforms Expose Biometric Content Today?

In this section, we look into the kinds of content exposed by different media platforms. Today, sensitive pieces of content containing biometric features are regularly posted publicly on social media and messaging platforms. It is also possible to find sensitive data on corporate and government portals, where high-resolution portrait photos and interviews with employers are often visible to anyone.

## Messaging Platforms

Messaging platforms like Viber, Telegram, and WhatsApp were initially used for peer-to-peer communication, but they have now turned into platforms that cater to group interactions. The content of many of these channels and groups is intentionally made public to attract a broader audience. While the number of participants in popular groups could easily reach tens of thousands of people, the most popular channels could reach millions. Alongside text posts, the content in these channels and groups are shared in the form of audio messages, photos, and videos, making the major biometric features from such content susceptible for extraction.

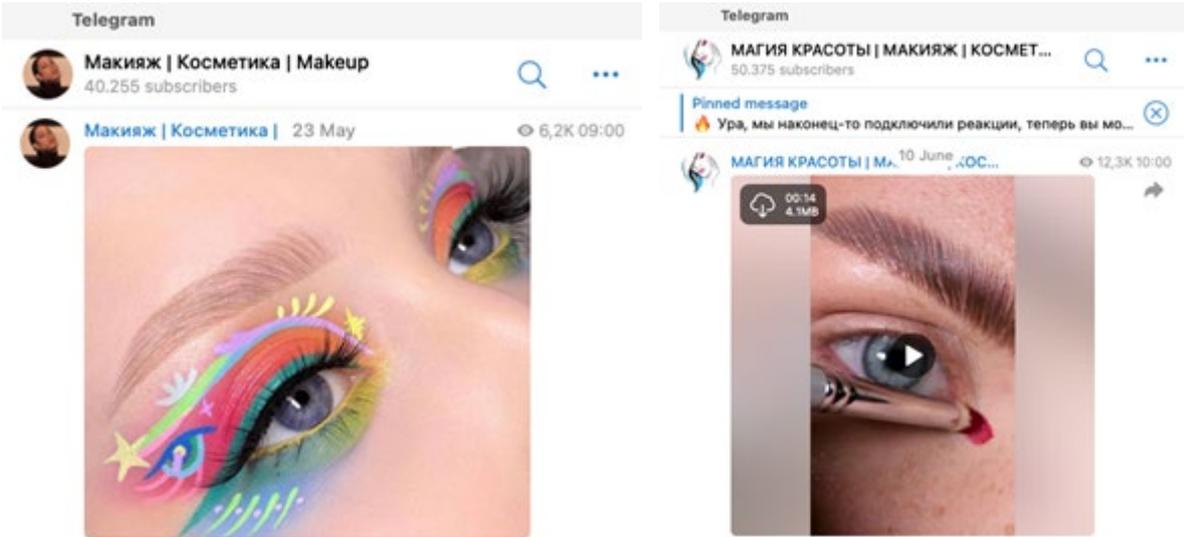


Figure 1. A photo and a video with biometric features exposed on Telegram<sup>6,7</sup>

*Image credit: Makeup | cosmetics and Magic of beauty | make up | cosmetics/Telegram*

# Social Networks

Social media networks such as Facebook, V Kontakte, and OK (popular in Europe) support a variety of multimedia content. Naturally, it follows that such content includes pictures of faces. Iris patterns, ear and palm shapes, fingerprints, and even voice patterns can also often be extracted from such content. To add, extensive environmental information such as places visited at a particular time or home environments could help geolocate and deeply profile a person. It's worth noting that such information is often available and extractable from exposed content as well.

Individuals or groups with malicious intent can also conduct a simple search to find multimedia content that exposes biometric features. When a search for “eye close-up” is conducted on Facebook, Figure 2 shows that results include a clear exposure of eyes and iris patterns.

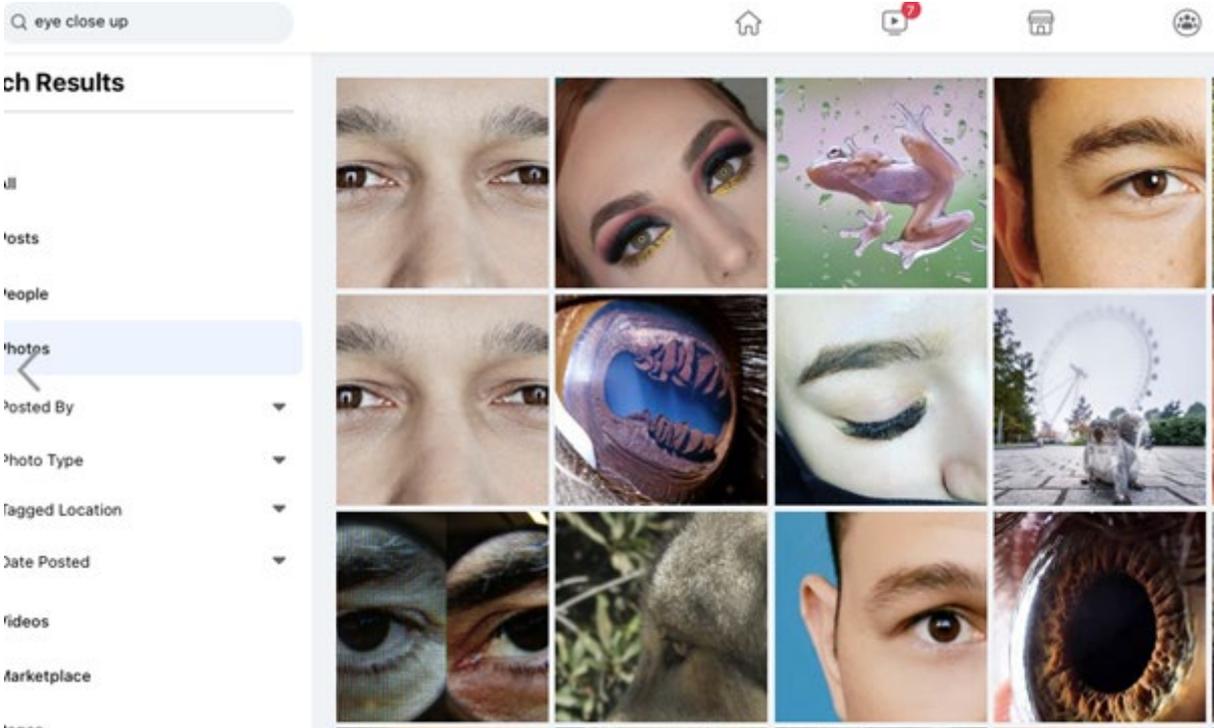


Figure 2. Results returned by Facebook for “eye close-up”

# Instagram

Instagram is a visual media-driven platform where the majority of content shows the activities of individuals. The popularity of profiles is driven by the number of followers, content views, comments, and other forms of engagement. Posts contain hashtags, which can be used to promote and search for similar content. The race for popularity drives profile owners to expose high-quality media content, often produced using professional photo, video, and lighting equipment. Still, the increased quality of such content also means that it would also be easier to use for extracting biometric features in case of exposure.

Figure 3 shows indirect (unintended) ear shape exposure while promoting an example of visual content with the hashtag #Earrings. We discuss both intentional and unintentional exposure of biometric features on these types of social media content in the following sections.

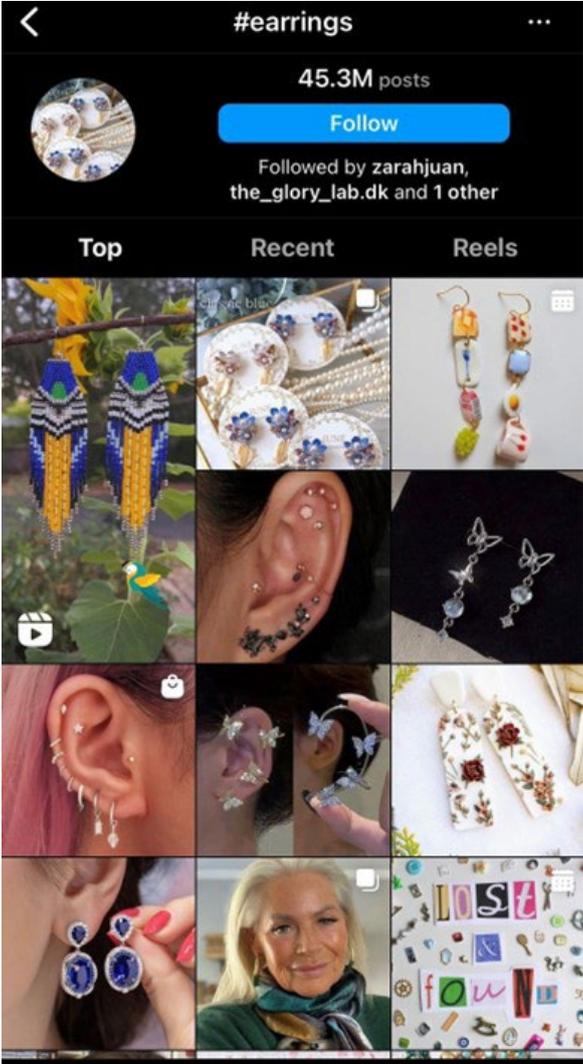


Figure 3. Example of ear shape exposure on Instagram returned by the hashtag #Earrings

## TikTok

TikTok is a video content-driven social media platform where popularity is determined by the number of followers, video views, and engagement. Similar to Instagram, trending posts, audio tracks used for videos, and topics are often determined by hashtags. Users can also rely on professional equipment or high-resolution smartphone cameras to record various content, majority of which is publicly available without registration. As with Instagram, users can also rely on hashtags to find content they are interested in.

Figure 4 features screenshots of hand shapes and fingerprint exposure.

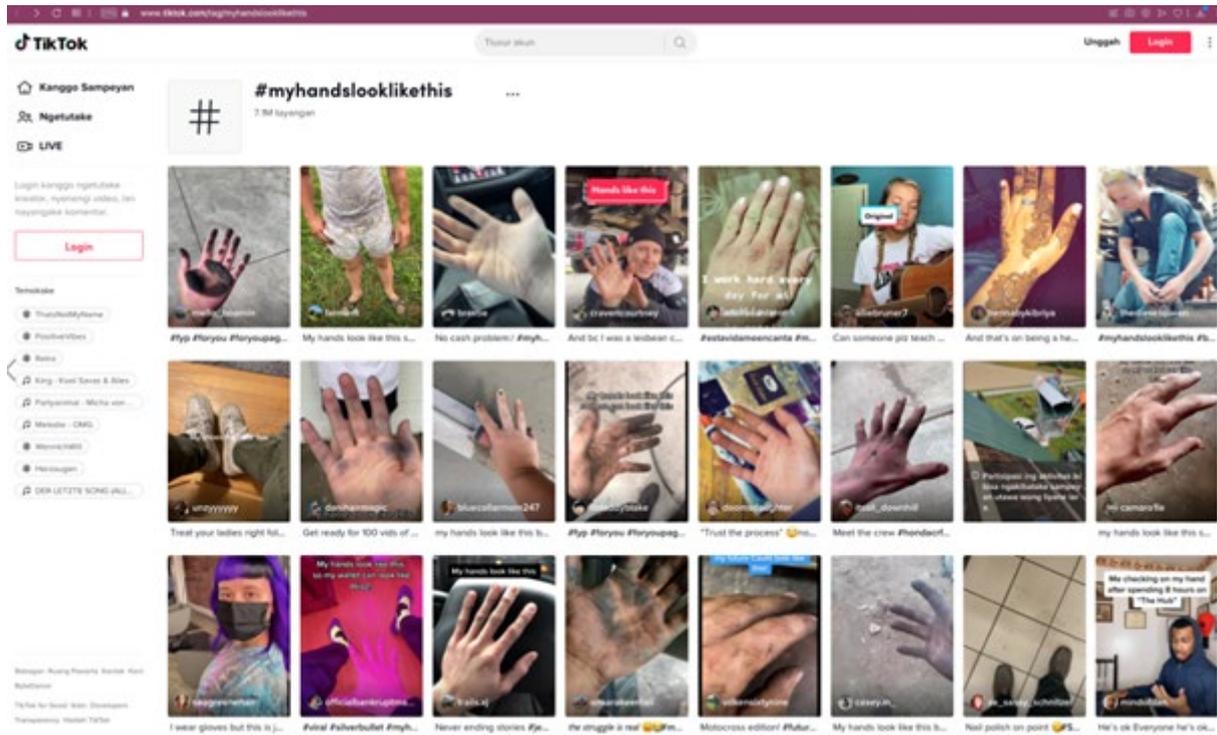


Figure 4. Example of palms with potential palm shape and fingerprint exposure on TikTok using the hashtag #MyHandsLookLikeThis (also called the #JazzHands trend)

## YouTube

YouTube is a video hosting platform with over five billion videos watched per day.<sup>8</sup> There is no dedicated focus for the type of content on this platform, but videos with intentional or non-intentional biometric data exposure are also available here.

The quality of uploaded videos on YouTube has been increasing in recent years. Currently, most videos are uploaded with at least full HD resolution, while videos uploaded by professional content creators have ultra HD 4K or even 8K resolution. Notably, although ultra HD resolution videos have higher potential for biometric feature capture, in some scenes where an eye is captured by macro lenses, full HD resolution could be enough to expose biometric features clearly.

The images in Figure 5 are examples of eye exposure. These were the resulting images from a search query for “blinking eye”.

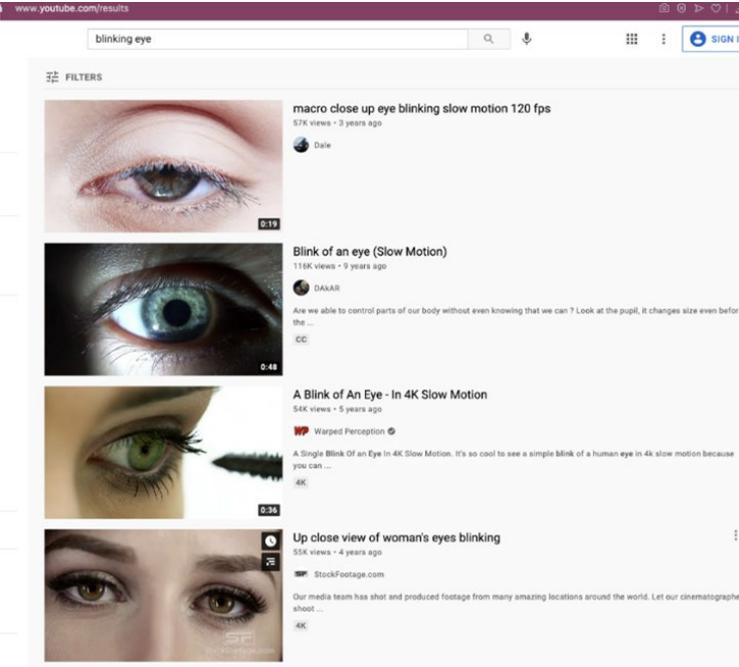


Figure 5. Eyes exposed on YouTube

## Twitter

Twitter is mainly for posting short messages; however, it also supports photo and video attachments. Users can also use hashtags and phrases as search terms on the platform. Such content is normally available without authentication and indexed by search engines. While the quality of media content varies, exposed biometric patterns can still be found on the platform.

The scale of exposure on Twitter is notably not as high as those on other social media platforms, but that does not mean that it is impossible. Figure 6 shows an example of an exposed fingerprint.



Figure 6. Fingerprint exposed on Twitter<sup>9</sup>

*Image credit: SerScience/Twitter*

## Official Corporate and Government portals

Official corporate and government portals are sensitive categories for exposure since the media content on these portals often shows major influencers and decision makers. For example, on the official site of the European Commission, portrait photos of government officials with over 10 MP resolution are available.<sup>10</sup>

If a user conducts a search using keywords, categories, date ranges, and other parameters, they would find that over 50,000 photos and over 120,000 videos of officials are available. Videos are available at several resolutions, while audio tracks from the videos are also available as separate files.

audiovisual.ec.europa.eu/en/search

European Commission

EN English Search our media catalog Search

European Commission > News > Audiovisual Service > Search results

# Audiovisual Service

Home [Headline News](#) [Europe by Satellite](#) [Video](#) [Photo](#) [EU History](#) [Copyright](#)

## Search options

**Keywords** [?](#)

keywords...

**Type of media**

Photo

**Categories**

**From**

**to**

**Thesaurus**

Gender Equality

**Topic**

## Search results (53710)

TYPE OF MEDIA [PHOTO](#) CATEGORIES [Portrait](#)

Showing results 1 to 30 **Sort by** [Date](#) [Relevance](#)

 <p>Janusz Wojciechowski, European Commissioner for Agriculture <b>Date:</b> 17/06/2022</p> <p><a href="#">View full reportage</a></p>	 <p>Ursula von der Leyen <b>Date:</b> 17/06/2022</p> <p><a href="#">View full reportage</a></p>	 <p>Nicolas Schmit, European Commissioner for Jobs and Social Rights <b>Date:</b> 17/06/2022</p> <p><a href="#">View full reportage</a></p>
 <p>Ursula von der Leyen at the podium <b>Date:</b> 17/06/2022</p> <p><a href="#">View full reportage</a></p>	 <p>Ursula von der Leyen <b>Date:</b> 17/06/2022</p> <p><a href="#">View full reportage</a></p>	 <p>Ursula von der Leyen <b>Date:</b> 17/06/2022</p> <p><a href="#">View full reportage</a></p>

Figure 7. Results of a portrait search on the European Commission portal<sup>11</sup>

The media content available has detailed metadata, including time, location, tags, and personalities (names), meaning that for every piece of exposed content, a respective identity is also known.

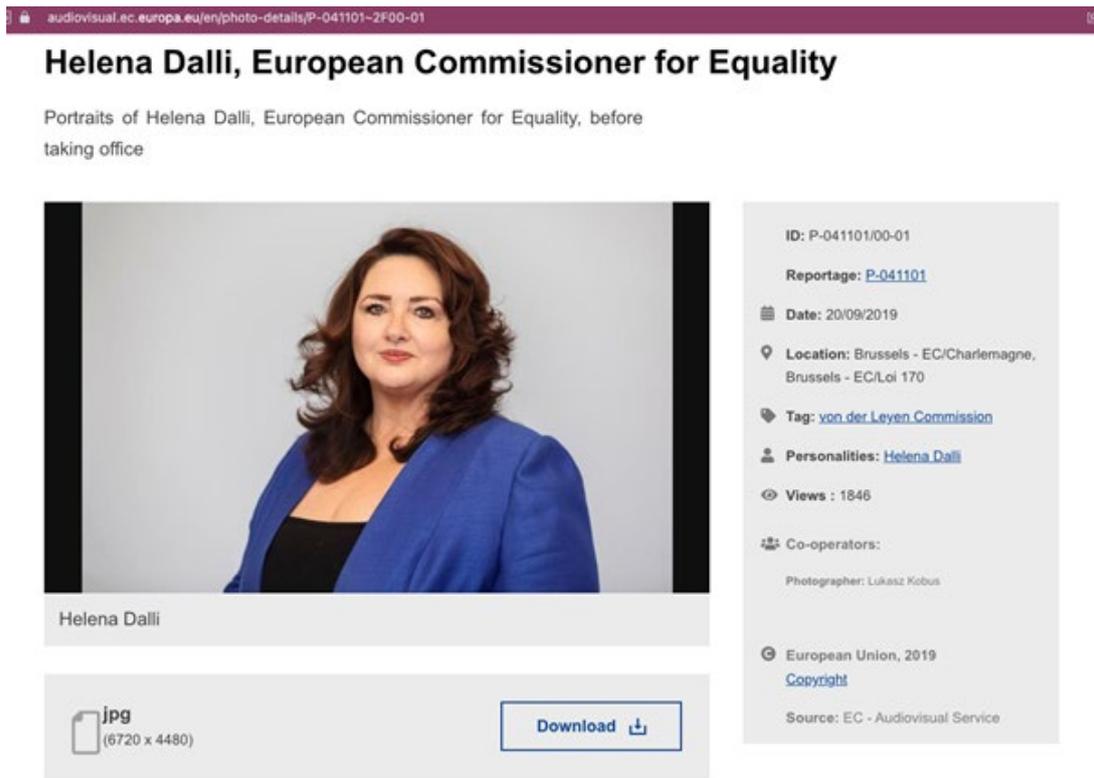


Figure 8. A portrait with 28 MP resolution (6720 by 4480) on the Europa.eu website, complete with detailed metadata and description<sup>12</sup>

*Image credit: European Commission*

Professionals use top-of-the-line equipment to create media content for official government and corporate portals. This means that the quality of the media is therefore so high that exposed biometric features in even just a fragment of an image have resolution high enough for such features to be captured clearly.



Figure 9. The hand shape exposed from the corner of a high-resolution picture from the official European Commission portal<sup>13</sup>

*Image credit: European Commission*

# News and Media Outlets

While navigating news outlets, we can also find high-resolution media that exposes biometrics. As expected, we can find high-quality photos of politicians, CEOs, and celebrities, among others. The photos or content of different articles often provide additional information about a person, time, location, and environment where the photo was taken. The left side of the following figure is a representation of common photos found on news portals and shows the parameters of such photos. The right side of the figure is an example of the extensive metadata usually attached to news images.

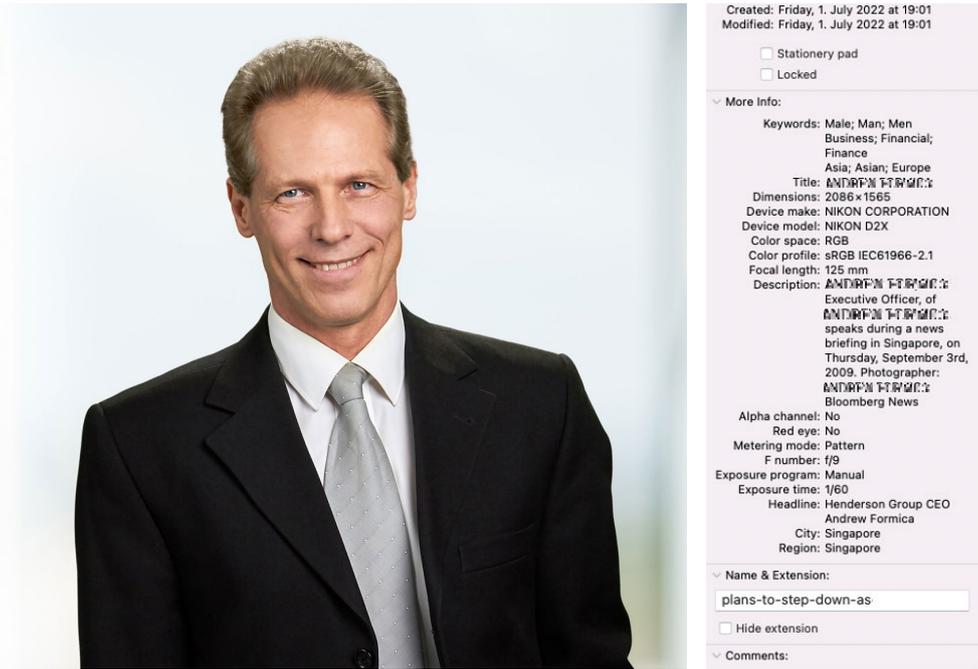


Figure 10. Representation of photos found on news sites like the Bloomberg news portal.<sup>14</sup> Face, ear, and iris pattern are exposed, and metadata can be found attached to the image.

There are specific cases, for example, when an interviewee attempts to be anonymous by sitting aside, staying in the shadow, or wearing a mask. But even in these cases, biometric and personalized features could still be exposed, causing the interviewee to be identified.

Another fact that needs to be considered is that for anonymous interviews, only a handful of people possess the necessary information to give a particular interview. In that case, the identity of the interviewee could be narrowed down according to their perceived age, gender, and height exposed during the interview. At the same time, sensitive features might be exposed unintentionally even if a person used camouflage onscreen or wore a balaclava or a mask.

In the case of online news articles, exposed low-resolution photos in an online article are not too damaging. However, there are often high-resolution photos on the same portal, and these can be extracted by removing or modifying some parts of the URL, like the scale factor.

Figure 11 shows an example of an image that is not clear enough for iris recognition enrollment in a biometric system. However, if we look at a similar image published in The Sunday Times, we see that simple changes to the site reveal high-resolution pictures — in this case, with 20 MP — which can expose enough details to deanonymize the person in the image or be used to impersonate the person. There is an original photo in the article,<sup>15</sup> but the image can be opened in a new tab with about 1.2 MP resolution.<sup>16</sup> It can also be opened in the new tab without a scaling factor with about 20 MP resolution.<sup>17</sup>

In other situations, if an iris pattern has been previously leaked or sourced from an image, it could be deployed in a biometric system at border control or used to gain access to certain buildings.



Figure 11. A representation of an image from The Sunday Times showing potential unique face details and eye exposure

Another example is the series of photos in Figure 12. It shows representations of common images seen in news coverage of rallies and protests. We see that a person wearing a mask can effectively hide their iris pattern and their face shape but at the same time can also expose their ear shape, partial palm shape, and tattoos. Taken separately or in combination, these exposed features can significantly improve the chances of deanonymization. This is especially true if the task is to identify a single person from a particular known group where several individuals have already been identified. It should be noted that even if the camera position was set to focus mostly on the back of a person's head, some angles can still expose their ear shape and tattoos.



Figure 12. Potential ear shape and tattoo exposure even if an individual's face is hidden. Images represent photos typically used in news coverage.<sup>18</sup>

The identification of such individuals from an image is not a trivial task. However, a combination of different possible sources, such as telecom network data about people who were present in an area or social media posts that expose the same unique patterns, would increase the probability significantly compared to a situation where these features were not exposed during the event.

## Search Engines

Search engines normally index content, allowing cross correlations across media published in different sources. For example, they can tag a person on a picture and find similar pictures with higher resolutions that contain biometric features.

Google, Bing, Yahoo, Yandex, and Baidu are universal search engines. However, there are also specific search engines that narrow the scope to a particular social media or messenger network, such as *tgstat.ru*. There are also engines that allow users to search social media platforms like *social-searcher.com*. While search engines are normally not responsible for content exposure, therefore, they can still be used to search or match one piece of content with others that have the exposed biometric features of a particular person.

## Future Scenarios Involving VR, AR, and Metaverse

In the near future, we expect the advent of more internet-of-things (IoT) and industrial internet-of-things (IIoT) devices capable of directly and indirectly capturing biometric features. The use of visual reality (VR) and augmented reality (AR) technologies, the shift to the metaverse<sup>19</sup> from classic social networks, and the extensive use of devices with embedded audio, video, and biometric capabilities in daily life will

lead to nearly permanent user exposure. In fact, HoloLens 2 (a mixed reality headset) already has iris authentication with user management function. Similarly, other VR platforms already have plans to use iris recognition for authentication.

Even now, if we compare uploads of video content with live streaming, there are different exposure risks. Videos can be reviewed and edited, while streaming exposes sensitive features immediately and directly. We already have mobile sensors and applications that are capable of capturing 3D objects, including capturing the 3D shape of a face, which has key benefits for VR and metaverse users. This means that in the near future, malicious actors could bypass more advanced facial recognition technologies at scale.

In the next decade, we also expect the mass appearance of self-driving cars on roads. These cars, if considered as IIoT devices with cameras, sensors, and computation capabilities, are also perfect for biometric collection. Access to such data should be restricted by vendors, but a sophisticated attacker<sup>20</sup> could still compromise and use such devices as their adoption increases.

It is also important to consider the infrastructure and back-end areas of multimedia content-processing services. Today, we are witnessing a variety of breaches related to personally identifiable information (PII) and financial information. In the future, we expect more frequent breaches that expose biometric databases or raw captured content of multimedia services instead of processed content. Similarly, media content that is considered private or restricted (only shared to specific people) will be exposed for public access in such cases. The impact of such exposures can be critical. As with all biometrics, once the features are exposed even for a single instance, it is hard to mitigate the malicious use of these features in the future.

## A Summary of Content Exposure by Different Services

To summarize our findings, we created a table that compares the exposure of major biometric features depending on the type of content and where it can be found. Content location includes major hubs like messaging apps, social media platforms, and several major news outlets (we go into further detail in succeeding sections).

We classified the type of content as audio, photo, or video. We also highlight what kind of features are mostly exposed in the content of each platform.

Content location	Audio	Photo	Video	Context / Description	Hashtags	Search capabilities	What is prevalent?
Government/ Corporate portals	Medium	High	Medium	High	Low	Low	
Messenger platforms	Medium	High	Medium	Low	High	Medium	
Facebook	Medium	High	High	High	High	High	
Instagram	Medium	High	Medium	Medium	High	Medium	
TikTok	Low	Low	High	Medium	High	High	
YouTube	High	Low	High	High	Medium	High	
Twitter	Low	Medium	Low	Medium	High	Medium	
News outlets	High*	High*	High*	Low	Low	Low	
Misconfigurations, breaches, and leaks	High	High	High	High	Low	High	 

Table 1. Heatmap of content exposure on certain platforms and applications

It is evident from the table that majority of the portals have either medium or high exposure, while for some features there is no straightforward way to find biometric features at scale, especially for fingerprints. Instead, it is necessary to think about the context in which the features can be exposed. We can therefore categorize exposure as intentional, semi-intentional, and unintentional. The succeeding section looks into context in more detail.

## Context of the Content

One of the problems with biometric data is that, unlike a password, once it is exposed, it is nearly impossible to change. In some cases, people expose biometrics intentionally, but unintentional biometrics exposure is more dangerous and has more potential to be abused at scale.

## What People Show Intentionally

In some cases, people clearly understand what they are doing while exposing certain features such as fingerprints. For instance, there are scientific articles and videos on the topic of fingerprint exposure.

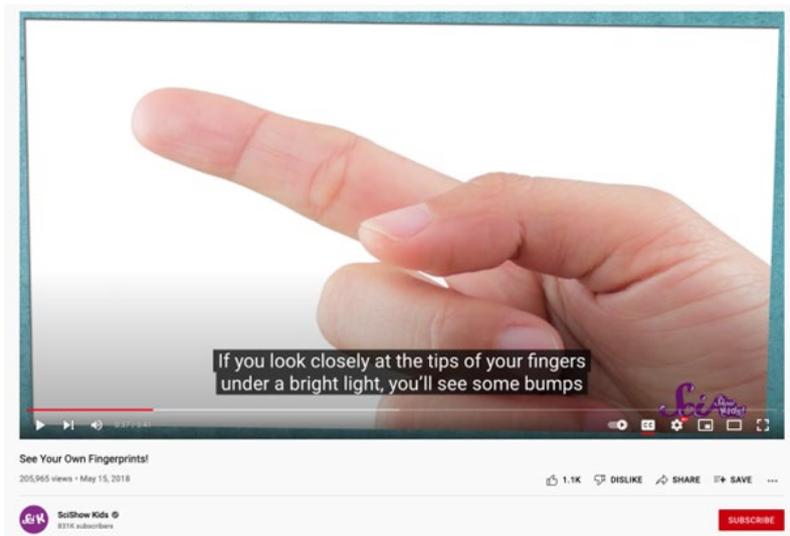


Figure 13. Exposure of fingerprints from a video on the topic<sup>21</sup>

*Image credit: SciShow Kids/YouTube*

In contrast, the search results for direct tags like #Fingerprint contain a lot of noise and do not suggest the mass exposure of biometric features. The exposure in such cases happens either semi-intentionally or unintentionally.

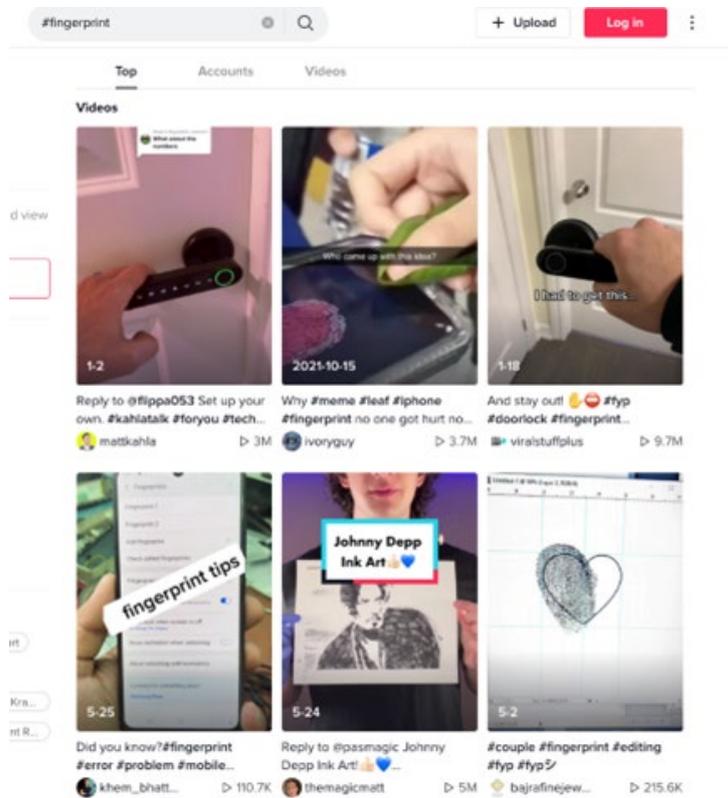


Figure 14. Results for the hashtag #Fingerprint on TikTok don't indicate mass fingerprint exposure.

# Semi-Intentional Content Exposure

Semi-intentional exposure means that authors of the content expose either voice recordings or photo and video content related to the parts of the body that also include biometric patterns. In such cases, the authors probably do not consider that such posts lead to exposure.

For example, by posting a high-quality portrait photo, face patterns are exposed. By posting a picture or a video of an eye, very often iris pattern is also exposed.

We see this type of exposure on a moderate scale. For example, there are trending topics and terms on social media like the phrase “beautiful eyes”. A search query for this phrase revealed a significant volume of exposed relevant content.

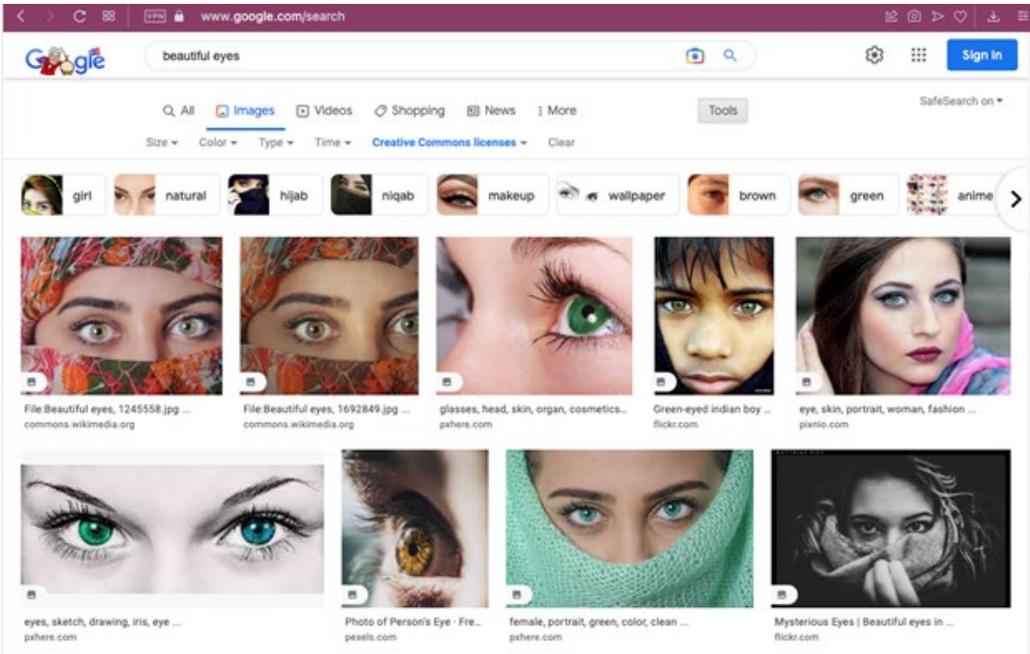


Figure 15. Search results for “beautiful eyes”

# Unintentionally Exposed Content

Unintentionally exposed content refers to content with major biometric pattern exposure. This means that the major topic of the post is not related to biometric features or parts of the body that expose biometric features. However, at the same time, unknown exposure takes place, and it is this category in particular that merits increased awareness.

One example is this picture of a wine glass. By zooming in, we can spot the exposure of fingerprints on the glass. However, it is clear that fingerprints are not the topic of this post and that the exposure is unintentional.

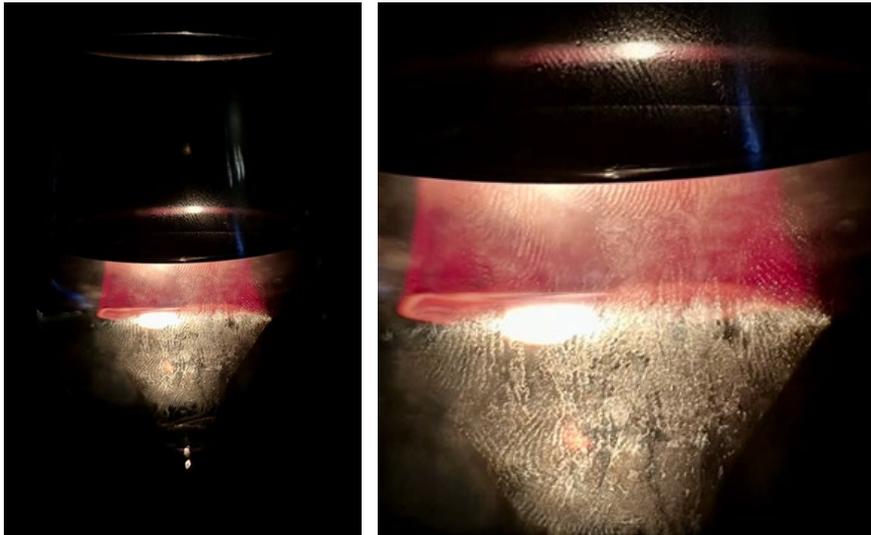


Figure 16. A series of fingerprints exposed on a picture of a wine glass

There are dozens of scenarios like this and without knowledge of exposure risks, it is nearly impossible to spot such exposure. After all, do we think about eye makeup pictures and video in relation to iris exposure? We can also ask the same about photos of bracelets, which often show the palm with exposed fingerprints.

Etsy goods, wedding rings, small gifts, videos about hand care, miniature food cooking, needlework — media content related to such topics do not look suspicious at first glance. However, albeit unintentionally, they expose biometric patterns. At the same time, many of these photos and videos have hundreds and thousands of views.

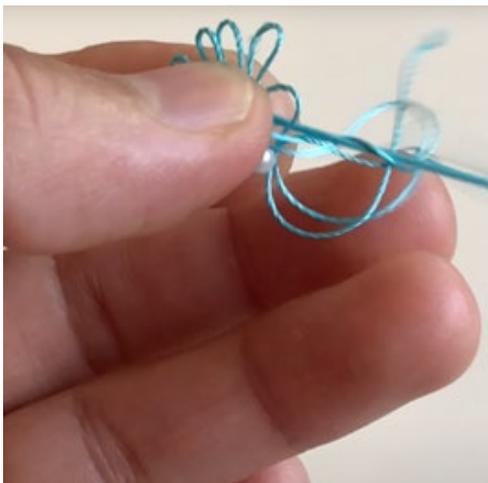




Figure 17. Examples of unintended fingerprint exposure on YouTube

Similar to a physical fingerprint collection where environmental variables like temperature can significantly affect the quality of the fingerprints,<sup>22</sup> lighting conditions and equipment quality can affect a digital collection of fingerprints. Collected fingerprints could even be used to plant evidence at crime scenes.<sup>23</sup>

## Examples of Hashtags and Pivots Used to Find Exposed Content

Search terms	Face	Iris	Palm, fingerprints	Ear
Messaging platforms	Makeup News	Makeup	Manicure	Haircut
Facebook	Makeup	Eye close-up	Manicure	Earrings, haircut
TikTok	#Face #Makeup #MyMakeup #NoMakeup	#EyeTransition #EyeZoom #EyeChallenge #Inverted #Eyes	#HandTrend, #FingerChallenge, #MyHandsLookLikeThis #Etsy #Braslet #WeddingRing	#EarTok #Earrings #EarCheck
YouTube	Interview Makeup Hairstyle News	eye zoom, eye zoom in, zoom macro, eye close up, blinking eye	Finger tattoo, Needlework, Miniature food	Earrings
Twitter	#Hairstyle #Haircut	#Hairstyle #Haircut	#Manicure #Fingerprint	#Hairstyle #Haircut
Instagram	#Makeup #Hairstyle #Haircut	#MyEye #EyePhotography #EyePhoto #EyeyMakeup #MacroEye	#Fingers #MyHand #HandPicture #HandCloseUp #TodayOnMyhand	#Hairstyle #Haircut

Table 2. Examples of search terms and relevance of results on different media platforms

Table 2 provides some examples of search terms we found that exposed biometric information. Some terms exposed three to five biometric features at the same time. While it is easy to find faces, irises, palms, and ears exposed together on makeup- and haircut-related videos, news articles also often expose faces, palms and ears, as do many other platforms.

## Different Biometric Patterns People Typically Leak Depending on Media, Length, and Scenario of Multimedia Files

In this section, we outline scenarios involving exposure within typical media content as simple examples. This will give additional context to the information in preceding sections.

The first scenario is a press conference where a C-level executive or politician walks onto a stage, waves their hand, and says hello to the audience. During the speech, to keep the attention of the audience, they use gestures and turn slightly to the left and right. They also periodically drink a bit of water from a glass. This means that their face, iris, ear, hand, and fingerprint patterns have already been potentially exposed for several minutes. If there are press cameras and an audience with smartphones present at the conference, capturing those features is almost guaranteed. The quality of the images depends mostly on the equipment, distance, and the lighting conditions.

The second scenario involves cooking miniature food. Here, the creator presents themselves, exposing their face and probably iris patterns. When they turn to pick up something, they expose their ear pattern. While holding a spoon or fork, they also partially expose their fingerprints, and while presenting the result of their cooking, they expose their palm pattern.

There are many other video scenarios that expose two to three biometric features in a very short period. TikTok videos, for example, are often only 15 seconds long, but these expose nearly every feature discussed in the paper.

In sum, static pictures and videos that show a feature for several seconds can expose sensitive data, making it paramount to keep those risks in mind when publishing media content.

## Biometrics Use Cases

For years, biometrics have been used for identification and authentication; however, there are other applications for biometrics. Behavioral biometrics are used to profile people or their habits, like their driving style.<sup>24</sup> These can also be used for user context recognition.<sup>25</sup> To understand the risks and potential attack vectors of exposed biometric data, it is important to know where, when, and how biometrics are used. This section will describe typical current and future use cases for biometrics.

## Access to Own Devices

Most modern smartphones and tablets have the capability to authenticate the owner by using one or several biometric features. Currently, fingerprint or facial recognition are two of the most widely used methods. Many laptops are also equipped with fingerprint scanners or have facial recognition capabilities.

Biometrics are not just used to unlock the device but also to authenticate a user during purchases and software installation, or to confirm sensitive actions inside different applications. In 2020, an estimated 41% of smartphone owners used biometrics, and according to forecasts, by 2024 that percentage will grow to about 66%.<sup>26</sup> Considering that in 2020 the number of smartphones users already numbered more than five billion,<sup>27</sup> we can estimate that more than two billion smartphones process biometric features. Accessing these devices is, for now, the major use case where biometrics are used on a daily basis.

## Access to Buildings

Accessing buildings, especially those in locations where sensitive information is processed such as government or research institutions, is one obvious use cases for biometric-based access control.<sup>28</sup> Fingerprint, facial, iris, and palm recognition sensors are the most widely used for physical access control. The data from access control sensors are often also used to calculate working hours and make correlations between access control sensors and secure IT assets (usually accessible only from the building to enforce defense-in-depth strategies).

Access control can be deployed as supervised or not supervised. Biometric identification can also be combined with other methods to enforce security.

## Schools

An obvious use case for biometrics in schools is to restrict access to buildings to only authorized persons like students and teachers. In the UK, biometrics are also used for cashless catering, library registration, photocopying, locker access, vending machines, and laptop access.<sup>29</sup>

In some cases, biometrics can minimize the risks of the abuse of government-sponsored programs in schools. One example is the National Home-Grown School Feeding Programme (NHGSFP) that provides meals to children in Nigeria. As part of its operations, fingerprints and photos of children as young as five are collected to provide government compensation to children who have not received food. Biometrics also help guarantee effectiveness, transparency, and accountability.<sup>30</sup>

## Healthcare

In healthcare, biometrics are used to ensure precise verification of a patient's identity. The use cases vary from remote diagnostics, donor's authentication, determining identity, and obtaining the medical records of a patient who arrives in an unconscious state.

One of the most obvious potential misuses of exposed biometric data is the abuse of electronic prescriptions systems.

## Banking

Biometrics is already widely used in banking to authenticate individuals and confirm financial transactions. There are several use case scenarios: remote and local, supervised and non-supervised:

- The authentication can be local and supervised when the biometric sensor is controlled by a bank and a bank employer ensures that the authentication process is done properly. The confirmation of a money transfer in a specific branch or office of a bank is one example.
- Another case involves cash withdrawal from an ATM that supports biometric authentication.<sup>31</sup> In this case, the sensor is controlled by the bank, while authentication is not supervised. Non-supervised authentication gives more options for an attacker to bypass security mechanisms. Depending on the model of the ATM, fingerprints, facial recognition, or iris recognition can be used for authentication. Some ATM deployments in other countries like Brazil also permit cash withdrawal using biometrics in lieu of a debit or credit card.<sup>32</sup>
- Another scenario is local enrollment using remote authentication. Here the enrollment is done with a supervisor in the bank office or through a trusted partner, after which biometrics are used to authenticate or confirm remote transactions. In this scenario, malicious actors could use leaked biometric data to bypass security mechanisms. For this to happen, the victim's account must support biometric authentication.
- We also have cases of remote enrollment with remote authentication. In this scenario, leaked biometric data can be used to enroll and authenticate a user. If an attack succeeds, the owner of the biometrics is unaware that there is a bank account under their name that could be used to initiate financial activities.

## Critical Events

Critical events are similar to critical infrastructures but have limited lifespans. Biometrics can play a crucial role in such events to minimize risks for participants or attendees.

For example, the German Olympic team<sup>33</sup> used biometric-based access control to restrict access to their facilities against unauthorized persons. Verification of identity and vaccination status checks are also used together to permit access to sport events.<sup>34</sup>

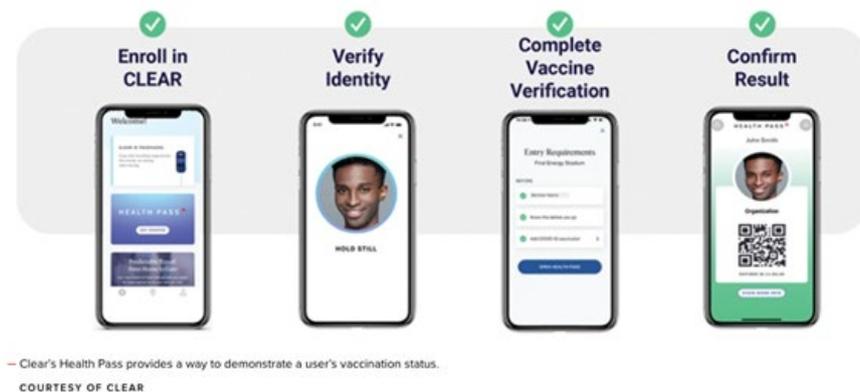


Figure 18. An application that verifies identity and checks vaccination status before permitting entry to a sports event

*Image credit: Clear application*

## Border Crossing and Airport Security

Biometrics are being used increasingly for international border crossing and airport security. There are several use cases for this, such as the frequent recording and verification of fingerprints and faces during border control procedures.

Based on typical travel experience, both customized sensors and full HD web cameras are used during those procedures. This means a wider or more limited attack surface depending on the quality or cost of the equipment. Indeed, options for crossing the border that do not require direct interaction with personnel are already implemented in major airport hubs. In addition to border crossing, some airports already use biometric-based check-in and boarding processes. In Frankfurt, Vienna, Munich, and Hamburg, airport facial recognition is available for Star Alliance flights.<sup>35</sup>

Due to the pandemic and masks requirements, iris-based authentication has turned into one of most preferred methods for authentication. Service providers that provide airport and event authentication, such as Clear, now allow eye-only authentication as a result of the global health crisis.<sup>36</sup>

## National Digital Identities and Law Enforcement Biometric Databases

For years, law enforcement agencies used fingerprint databases, like Integrated Automated Fingerprint Identification System (IAFIS) in their investigations. The current trend is to integrate several types of biometric features into these databases to be able to match identities based on face, fingerprints, iris, and other biometric features.<sup>37</sup>

Together with law enforcement databases, national digital identity and national biometric registers have been introduced in many countries. This means government and commercial organizations can use these

centralized databanks for authentication and identification. These databanks are often integrated into government, financial, and healthcare services and can be used for identification and authentication of hundreds of government and private sector services, including banks, fintech, telecom operations, and IT services. There are many implementations of such programs, including India’s Aadhaar Card<sup>38</sup> project and the UAE Pass.<sup>39</sup>

## Future Use Cases

In the near future, biometrics will play a more significant role because of the following factors:

- The number of devices that include biometric sensors or biometric capabilities are growing. Over 80% of new mobile devices that are shipped today have biometric capabilities.<sup>40</sup>
- There is now an increased availability of algorithms<sup>41</sup> and APIs,<sup>42</sup> especially for face recognition.
- Bigger players are stepping into native support of biometrics in their products and services.
- Updates that explicitly involve facial recognition in the terms of service of big media services like YouTube are indirect signs of biometrics’ increased importance. At the same time, while these updates might restrict the collection of biometric data, there are still many other biometric features that can be extracted from media content.

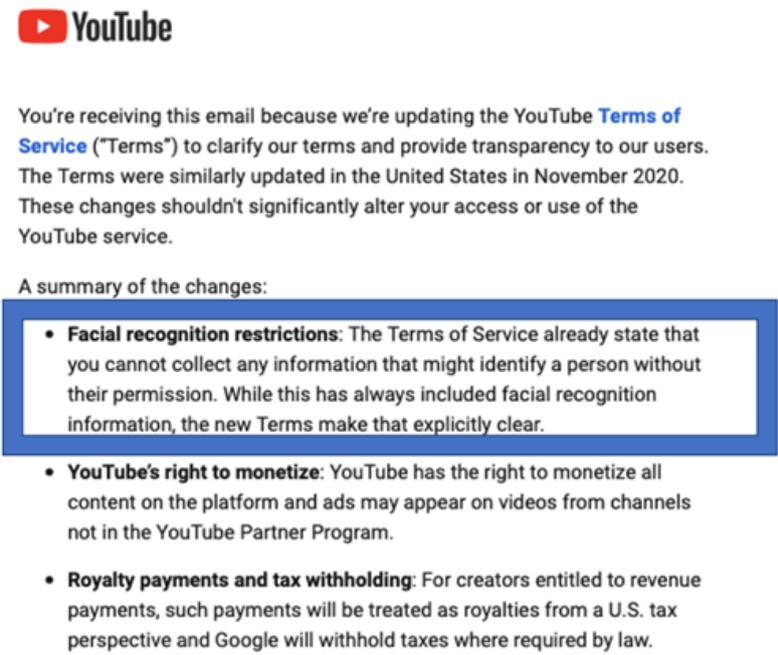


Figure 19. YouTube updated its terms of service to restrict the explicit inclusion of facial recognition in the US. The update was enforced within the US in November 2020 and outside the US starting June 2021.<sup>43</sup>

*Image credit: YouTube Help/Google*

There are several scenarios we expect to emerge where biometrics will play an important role. These are scenarios for which there are proofs of concept, or scenarios that have already been deployed, such as next-generation retail.<sup>44</sup> We expect that these technologies will be scaled to other countries and regions in the future.

## **Contactless Transparent Payment in Next-Generation Shops and Public Transport**

The next-generation retail<sup>45</sup> concept considers a variety of capabilities, including smart shelves and the extensive use of robotization, as well as means of payment that do not require cash or credit cards as their key features. In some cases, special applications provided by retailers and used at store entrances generate QR codes. In other cases, the process is even more transparent and a registered customer with enrolled biometrics is automatically recognized and tracked inside the shop. Biometric features are also used to initiate payments when the customer is leaving the shop. Together with usability, therefore, the technology also brings tracking concerns.<sup>46</sup>

Another similar use case is transparent payments in public transport using biometrics. These technologies recently became available in megapolises like Moscow<sup>47</sup> and Dubai.<sup>48</sup>

## **Censuses, Polls, and Voting**

In a 2002 symposium, the UN discussed the use of biometric technologies together with other innovations in censuses, including population censuses.<sup>49</sup>

Now, more and more countries have introduced biometric voter systems. In these circumstances, biometrics could play an important role in avoiding shared authentication credentials that would allow votes to be placed on behalf of several people at the same time.<sup>50</sup> In fact, there are already confirmed cases of biometric voter systems detecting anomalies. In Nigeria, over one million invalid entries, including double registrations, were detected.<sup>51</sup>

As for internet polls and petitions, there are a variety of attack vectors to manipulate the outcomes.<sup>52</sup> Biometric technologies can significantly improve the integrity of internet polls and petitions in the near future.

## **Social Scoring Systems**

A social scoring system has already been available in China for years, although it is still under active development.<sup>53</sup> Many other countries already have the technological capability to launch similar systems, but in Europe there are many privacy concerns about the implementation of these systems on a country-wide scale. Some industries, like insurance<sup>54</sup> or law enforcement agencies,<sup>55</sup> are already adopting these technologies. We expect that soon, there will be more industries using the results of these social scoring systems in some sense.

Biometrics, especially facial recognition, will play an important role in this process. Overall, capabilities to trace people's behavior and habits is expected to significantly increase during the transition from 5G to 6G communication technologies. This expectation comes from the increased number and types of sensors that will be capable of tracing human behavior.

There are already known cases when an AI system mistook an image of a model's face on a bus advertisement for someone jaywalking on the street. This in turn automatically affected the model's reputation in the scoring system until it was later manually corrected.<sup>56</sup>

# How This Affects People: Current and Future Attack Scenarios

This section covers current and future attack scenarios. Current attack scenarios are those that can be easily implemented now and at scale. Future attack scenarios cover the technologies that are already available but not used at scale, or scenarios for which prototypes and concepts of technologies are already present and for which we expect the appearance of attack enablers in the future.

The purpose of this section is to increase awareness on the risks that could appear after biometric features are exposed.

Attack scenarios		Face		Fingerprint		Iris	
		NOW	FUTURE	NOW	FUTURE	NOW	FUTURE
Biometric collection	Passive biometric collection	High	High	Low	Medium	Low	High
	Active biometric collection	High	High	Medium	High	Medium	High
Identity theft and impersonation attacks	Deepfakes	High	High	Low	Low	Low	High
	Abuse of smart devices	Low	High	Low	Low	Low	Medium
	Account takeover by tricking tech support	Medium	High	Low	Medium	Low	Medium
	Faking the presence of a person	Low	High	Low	Medium	Low	Medium
	Abuse of social scoring system	Low	High	Low	Low	Low	Medium
Attacks with identification	Tracking and automated identification of a person and their habits	High	High	Low	Low	Low	Medium
	Identification of communities where people communicate	High	High	Low	Low	Low	Medium
	Creation of context suitable for extortion	High	High	Medium	High	Low	Medium
	Identification of people presented at critical events	High	High	Low	Low	Low	Low

Attack scenarios		Face		Fingerprint		Iris	
		NOW	FUTURE	NOW	FUTURE	NOW	FUTURE
Attacks on authentication	Unlocking laptop, phone, and other gadgets	High	High	High	High	Low	High
	Next-gen retail, public transport payments, and cash withdrawal	High	High	Medium	High	Low	High
	Confirming account and financial transactions using biometric gadgets	High	High	Medium	High	Low	High
	Future devices	Low	High	Low	Medium	Low	High

Attack scenarios		Voice		Palm		Ear	
		NOW	FUTURE	NOW	FUTURE	NOW	FUTURE
Biometric collection	Passive biometric collection	High	High	Low	Medium	Low	Low
	Active biometric collection	High	High	Low	Medium	Low	Low
Identity theft and impersonation attacks	Deepfakes	High	High	Low	Medium		
	Abuse of smart devices	High	High	Low	Medium	Low	Low
	Account takeover by tricking tech support	High	High	Low	Low	Low	Low
	Faking the presence of a person	Low	High	Low	Low	Low	Low
	Abuse of social scoring system	Low	Medium	Low	Low	Low	Low
Attacks with identification	Tracking and automated identification of a person and their habits	Medium	High	Low	Low	Low	Low
	Identification of communities where people communicate	Medium	High	Low	Low	Low	Low
	Creation of context suitable for extortion	Low	Medium	Low	Low	Low	Low
	Identification of people presented at critical events	Low	Medium	Low	Low	Low	Low

Attack scenarios		Voice		Palm		Ear	
		NOW	FUTURE	NOW	FUTURE	NOW	FUTURE
Attacks on authentication	Unlocking laptop, phone, and other gadgets	Low	Low	Low	Low	Low	Low
	Next-gen retail, public transport payments, and cash withdrawal	Low	Medium	Low	Low	Low	Low
	Confirming account and financial transactions using biometric gadgets	Low	Medium	Low	Low	Low	Low
	Future devices	Low	Medium	Low	Low	Low	Low

Table 3. A heatmap of the use of biometric features in different attack scenarios and comparing current and projected future usage

# Biometric Data Collection and Connected Attacks

Attackers need to collect or intercept biometric features to use them. The collection of features can be passive or active. “Passive” means that the collection will not be visible to the owner of the features or the organization that stores or processes biometric data. “Active” means that the collection process is known to the owner of the features or organization that stores or processes biometric data.

## Passive Biometric Data Collection

Passive collection is mostly related to the publicly exposed features that were previously described in this paper. The major sources for such information are social media and messaging networks, news outlets, and official government and corporate portals. FindFace<sup>57</sup> is one of the services that process photos from social media network vk[.]com at scale to identify people based on their face patterns.

## Active Biometric Data Collection

By “active biometric collection,” we mean attacks that aim to collect biometric features. Notably, no such active engagement is necessary for passive collection. In addition to the main focus of this paper on passive biometric leakage in social media, it is also worth listing the sources of biometric data that are available for an active attacker.

In this section, we walk through several attack scenarios related to active biometric data collection.

## Attacks on Biometric Ecosystems

The simplest case scenario of a biometric ecosystem is a standalone implementation, which means that patterns are stored on a sensor or on a host directly connected to the sensor. Those implementations are mostly related to the small office, small home (SOHO) and small-and-medium-sized business (SMB) segments where access to a single asset, like an entrance door to the gym, is controlled by a biometric sensor.

Implementations connecting several distributed sensors already require more complex architecture. The deployment often includes biometric sensors, a cloud or centralized database, and APIs for integration with different authentication services. Any of these components can be used to extract biometric patterns if there are configuration errors, exploitable vulnerabilities, or insider threats present. Since third-party biometric service vendors often possess sensitive personal, government, or corporate data and information on business processes, they are therefore potential lucrative targets and serve as an important link in the supply chain.

### Attacks on Sensors

Sensors (hardware biometric sensors, not normal mobile phones) can be installed, controlled, or modified by an attacker. The attacks in this scenario are similar to skimmer attacks on ATMs that allow sensor output interception. In many cases, they can be easily implemented.

Few would be surprised, for example, if an extra camera is attached to an ATM or if fingerprint scanners appear on an ATM. This is similar to how contactless payment devices are now in many stores. However, an attacker can compromise the equipment or credentials used for controlling and managing cash or payment.

The software supply chain can be also broken in several places, especially if third-party libraries, APIs, or software development kits (SDKs) are used.<sup>58</sup> There are also precedents in other industries, such as criminal underground sales of modified applications for taxi drivers that are capable of faking GPS data and charging customers for longer journeys.<sup>59</sup> In short, all necessary technologies for such attacks are already in place, and it will just be a matter of time until the issue becomes visible and at scale.

### Attacks on Databases

In this current climate, data breaches happen regularly. While we hear a lot about breaches exposing PII on the news, it's worth noting that misconfigurations or other incidents that expose biometric data also happen.<sup>60, 61</sup> Additionally, while breaches tend to be public in nature, in some cases they are covert, as attackers could compromise databases and back-end infrastructure supporting biometric data storage without public exposure.

## Abuse of API and Export Features

To provide interoperability to many, biometric ecosystems (especially distributed ones) need the capability to export patterns or raw biometric feature captures. This capability is often a part of compliance requirements. The exchange format of the data is standardized, and the ISO/IEC 19794 – Biometric data interchange formats series or ANSI/NIST-ITL 1 is one example of such standards. The attacker can exploit or abuse such features to obtain biometric data related to accounts enrolled in the system.

APIs related to biometrics can also be used to extract biometric patterns or raw data captured by sensors. This fact is confirmed by research published in recent years. For example, a report on the usage of fingerprint API in Android<sup>62</sup> discusses security issues of Android APIs related to biometrics. Some Android-based devices are also vulnerable to biometric feature extraction through API. There are also published reports of a vulnerability in the API that allowed for the extraction of fingerprints from a phone.<sup>63</sup>

APIs related to distributed biometric systems can be also exploited,<sup>64</sup> which opens another path for criminals to monetize existing access to infrastructures.<sup>65</sup> For example, if a compromised organization integrates biometric identification and authentication in some of their processes, then criminals could exploit their access for ill gain.

Due to interoperability, the captured data can be imported to the other biometric systems without user permission or injected into a system on behalf of compromised or attacker-controlled sensors.

## Attacks on Raw Data and Media-Processing Algorithms to Extract Biometric Features

With global internet connectivity, it is hard to control the full supply chain related to media services, especially if media content is stored unencrypted, streamed, downloaded, or uploaded using unsecure connections. Media traffic could also go through different jurisdictions. That means that at any intermediate point, additional media-processing algorithms could be deployed and biometrics extracted and processed without our control.

## Attacks on Surveillance Systems to Extract Biometrics

Surveillance systems are a gold mine for collecting biometric features (mostly face images), but in some cases they could also include voice, palm, and ear patterns. This is the case in both China<sup>66</sup> and Russia<sup>67</sup> where systems that use facial recognitions are already centralized.

In other locations, this equipment could still be used to capture biometric patterns. There are numerous cases of surveillance systems being publicly exposed, and these systems can be categorized by location or type of content. In previous research, we discussed the sale of access to surveillance systems as part of established business models in the cyber underground.<sup>68</sup>

# Identity Theft and Impersonation Attacks

Digital identity already plays an important role in our life. In some countries, one's digital identity is linked to a SIM card or mobile app that requires biometric enrollment to unlock an application or authenticate transactions. Usually, this means that there are procedures to initiate a trusted relationship between normal print or plastic IDs and a digital identity, after which an individual can use their digital identity for many activities without physically providing a traditional ID.

Right from the stage of establishing a trusted relationship, the compromise, takeover, or cloning of these new kinds of IDs could lead to serious real-life consequences. Among the possibilities, account takeovers, including accounts on government portals and accounts related to financial institutions, could happen. Malicious actors could even use accounts to fabricate evidence by placing an individual in a particular place in specific circumstances.

## Deepfakes

Deepfakes can leave critical damage on the reputation of people who have influence in a country or a particular industry, which means that public figures are automatically potential targets. More importantly, these are the people who almost definitely have already had their static and behavioral biometric features exposed at scale via media content. Unfortunately, this exposure would allow someone to train deepfake models — something we already see regularly with political figures.<sup>69, 70</sup>

The same activities on a bigger scale can lead to a significant impact on the owner of the biometric features or assets, as criminals are already adopting technologies to target private companies using deepfakes of CEOs.<sup>71</sup> Trend Micro previously explored this at length in a collaborative research with Europol and the United Nations Interregional Crime and Justice Research Institute (UNICRI).<sup>72</sup>

There are existing proofs of concept showing how deepfakes can bypass the security mechanisms of financial institutions, specifically biometric liveness checks done through videos.<sup>73</sup> One key risk here, however, is that cybercriminals and state-sponsored groups might also use these technologies.

## Criminal Monetization of Deepfake Technology

The use of deepfakes for financial scams and other malicious activities has been discussed in underground forums in recent years. Not surprisingly, technology capable of significantly improving the success and monetization rate of a variety of cyberattacks piqued the interest of underground users since the early days of its appearance.<sup>74</sup> Deepfakes can revolutionize and empower existing attacks like business email compromise (BEC), messaging and tech supports scams, making accounts for money laundering, and taking over accounts in financial institutions.

## Attacks Using Deepfakes During Critical Events

Some scenarios, like the use of a deepfake to mimic a country leader or a government representative making important statements at an inappropriate time, could lead to serious consequences. For example, if a deepfake of a government representative from a country with limited independent journalists makes a potentially damaging statement, this can trigger grave consequences inside the country, affect diplomatic activities, or leave an impact on the stock market. The effects of these fakes could therefore be considerably significant in critical scenarios.

A more specific example would be a deepfake video suspending the exportation of a particular material, piece of technology, or good. If the country involved has a significant or near-monopoly market share, many areas could be affected by such a statement.

Deepfakes also have the potential to create or amplify unrest in a particular region or for a particular social group.

## Abuse of Smart Devices

Smart speakers and voice assistants can be tricked and abused using publicly available media content. They can take commands based on reproduced voice messages and messages replayed by other nearby devices.<sup>75</sup> In some cases, this attack method can be used for innocent pranks, but some smart home devices can also initiate purchases, so this attack could create a financial impact for the person that owns these devices, thereby highlighting a specific risk involving devices that rely on voice recognition for authentication.

## Tricking Tech Support to Take Over Accounts

Tech support calls might require some media content to recover accounts in so-called Know Your Customer or KYC processes. These could require a user to take a selfie in a particular position where exposed media can be reused, or to take a selfie during a call. However, since modern equipment is capable of creating filters that can be applied to a video or audio stream in real time, someone can mimic a target's appearance or voice based on leaked biometrics that have been gathered by an attacker.

The same strategy can be applied by an attacker to target services that are deliverable through call centers. In this scenario, an attacker would use voice biometrics in real time. It's important to note that this kind of technology has been available for over a decade and is often used by financial institutions.<sup>76</sup>

## Faking the Presence of a Person at a Particular Place or Event

There are a few scenarios that involve faking the presence of a person in a place or at an event. For example, an attacker can trigger matches in surveillance systems equipped with facial identification capabilities, or they can implement biometric-based payment transactions (in public transport, for example) using biometric features collected from exposed media content.

Depending on the location chosen for the attack and the sensitivities around it, these malicious activities can trigger significant real-world consequences for the owner of the biometric features. There are simple and obvious scenarios where the consequences are visible.

To illustrate, we can take the example of a car-sharing service application that uses biometrics. If an attacker successfully abuses a user's biometrics, they can authenticate an account and then steal a vehicle under the user's name. The owner of the biometrics will probably be investigated and blamed for the crime. It's worth reiterating that this might be more relevant today because we are seeing more and more car-sharing applications with biometric authentication options available. We described a similar scenario involving stolen identities linked to mobile phones in a previously published paper.<sup>77</sup>

In another possible scenario, an attacker can plant evidence fabricating the presence of an individual at a suspicious place. In this scenario, knowing that a criminal group meets at a particular place, the attacker can trigger surveillance systems at the crime scene while also initiating payments to known money-laundering criminal accounts using an account tied to the biometric data of their target. Essentially, the attacker can frame their target for suspicious activity using biometric data.

These actions could lead to law enforcement investigations, additional background checks, and articles in the press, all of which can affect the biometric owner's reputation.

## Abuse of Reputation Using Impersonation Attacks

Impersonation attacks using exposed biometrics can be leveraged to affect the reputation of a person. The objective could be extortion, scams, or political and corporate advantages. An attacker can use photo, audio, and video recordings and post any of these with another description, in a different time, or with alternative context. They can also send voice messages to relatives or friends using messaging platforms for extortion purposes or scams.

There are more and more developments related to biometric-based identification<sup>78</sup> and authentication in social media networks.<sup>79</sup> We can map this to a previous paper, where we discuss how biometric sensors and processing algorithms can be bypassed and attackers can obtain access to a device with a certain social media application or social media account.<sup>80</sup> In this case, an attacker can initiate posts, comments, engagement, and join groups that can negatively affect the reputation of the person who owns the biometric data.

## Abuse of Social Scoring Systems

A social scoring system can be enforced country-wide or be limited to particular verticals. The ability to impersonate a person either on the streets or in the digital world can significantly affect a person's life if a social scoring system is deployed in their jurisdiction. For example, the cost of an individual's car insurance could significantly depend on their driving style.<sup>81</sup> This means that the impersonation of such an individual, or even the impersonation of the digital identity linked to such an individual, could significantly leave an impact on many aspects of their life beyond their insurance rates.

As for triggering a city surveillance system, for example in case of a virus outbreak and a subsequent lockdown, or in the case of an illegal street protest, the triggered system could lead to financial or criminal charges. For some, it might also mean a disruption of their career.

We expect that more and more methods for targeting both reputation and social scoring systems will be available for attackers in the near future. We also expect that any exposure of media content with biometric data will decrease the cost of implementing such attacks.

## Attacks With Identification

Exposure of biometric features at scale, especially those with geolocation information, also provides opportunities to trace people's activities at scale. For such attacks, due to the scale of exposure and recognition capabilities, face-based identification is the most typical scenario, while in some cases voice identification can be used.

There are a variety of attacks with regard to identification, and we will highlight several privacy-related scenarios in this section.

## Tracking and Automated Identification of a Person and Their Habits

Facial exposure together with real names can be used as a training dataset to train surveillance cameras with facial recognition capabilities. Governments, financial institutions, or private companies (which normally ask for written consent for collecting biometric features) can do this, but a malicious actor who has access to this type of data can do it as well.

An attacker that has access to a series of cameras can obtain data that can be used to trace the detailed location of a person at a particular time. By identifying the background environment in media content, they can also track a person's habits and weaknesses. This data can be used in other attack scenarios like extortion, preparation of individual phishing emails, attacks on reputation, and the manipulation of public opinion. Knowing that a person likes a particular food or is eager to attend events on a particular topic can significantly increase the success of phishing attacks if an attacker uses such information

Considering that connectivity of sensors will increase in the near future, especially during the transition to 5G and 6G, data collected by such sensors could also be used to trace location and habits with even more precision. It must also be stressed that risks related to connectivity would increase because legal requirements are so far very limited — something that we witness often whenever new technologies appear. Normally, there is a gap of several years after new technologies are abused and before legal regulations take shape, a kind of “wild west” period, if you will.

At present, we already see new companies selling face and emotion recognition models that have been trained on data exposed on social media networks. We also see very precise advertising related to our recent social media posts or discussions, even though data on our habits is supposedly anonymized. Combining this data gives a potential attacker precise and powerful fuel for a variety of psychological operations — from commercial scams to nationwide plots.

## Identification of Communities Where People Communicate

Faces on group photos and videos can be recognized and mapped to their social media profiles, including professional ones, to determine an individual’s employer, position, location, time of the event, and many other parameters. Several online services today provide this sort of accurate facial reverse image search, either for free or for a price.

Appearing with a controversial person at a particular time or in a certain context could also significantly affect the reputation or even political career of someone. If such an appearance is presented at the right time and to the right audience with the appropriate reach, the revelation can be very damaging. This scenario could lead to a political figure having to resign after a drunken incident or to apologize for an appearance at a celebrity gathering during quarantine. Both are realistic scenarios, and we have already witnessed such occurrences in recent news.

## Creating Contexts for Extortion or Manipulating Public Opinion Based on Exposed Media

Today, videos and photos can be published in the context of one event even if they were initially published in another context. This type of media can significantly change an audience’s understanding of a situation.

For example, let us say that a video identifying a person in military training some years ago is published to appear like the person is at present actively involved in ongoing military activities. Such posts can easily end up in news outlets before the person is aware of it and can take action. The publication can lead to significant reputational damage, affect ongoing negotiations, or even cause serious tension between several countries.

Unfortunately, even if the long-term effect of such a malicious activity is debunked, the short-term impact can do all the damage that the attacker hoped to achieve. Exposed biometrics can also expand capabilities of the so-called human flesh search (HFS)<sup>82</sup> and increase potential damage for the victims of such attacks.

## Identification of People at Critical Events

A critical event is a limited-time public or private event with higher risks and impact of incidents compared to a normal event. Examples include sports events like the Olympic games or World Cup, political events like elections, meetings involving a president or a prime minister, public speeches, strikes, natural disasters, and so on. Media exposure of the presence of a person at such an event can lead to positive and negative consequences.

Nevertheless, there are some personal scenarios that could lead to awkward situations or even extortion attempts. For instance, a person might appear at a football match while claiming to be sick and unable to go to the office, or someone might claim to be on a business trip only to be revealed at a nice beach after their face is recognized via a social media network. To add, friends and relatives might be asked to verify if the correct individual was tagged. Another scenario involves appearances at illegal street protests, which could lead to arrests and legal consequences in particular jurisdictions.

As long as media content is exposed, there are a dozen ways the content can be monetized or leveraged against a particular person in attack scenarios. What is also clear is that new technologies give more and more opportunities for an attacker to do that.

## Attacks on Authentication

For authentication-based attack scenarios, face, iris, fingerprint, and voice are the major features that are used. We can consider local and remote authentication and, in this section, will cover several use cases for both scenarios.

### Abusing Local Authentication Mechanisms

Local authentication mechanisms mean close positioning between the sensor and the asset to which access is provided. In other words, if biometric-based authentication provides access to an asset located in the proximity of a biometric sensor, we consider the scenario as local.

This is why payment in public transport or next-generation retail falls under a local authentication category.<sup>83</sup> In many of these cases, pattern databases are stored in the sensor (like for some fingerprint-based door locks). The database could also be located in a smartphone or in a computer also located locally.

## Unlocking a Laptop, Phone, and Other Gadgets

Many modern gadgets, including phones, tablets, and laptops have embedded biometric sensors in some form. Unlocking these gadgets using biometrics is the use case scenario most applied in daily life, and attacks in this area have been widely publicized. When attacks do happen, the evidence of unlocking is recorded in local logs. However, further investigation capabilities are limited in these commercial gadgets compared to enterprise-grade biometric systems. This is due to the local nature of the authentication.

The reasons for device-unlocking attacks using exposed biometrics can vary, and they are significantly dependent on the role of the device owner in society. Political figures or C-level executives are plausible targets in state-sponsored attacks, whereas an ordinary person could fall prey to different criminal monetization strategies.

## Opening a Biometric Door Lock

Biometric locks are widely used in celebrities' private homes and executive apartments. These locks allow access without a physical key to a predefined list of people.<sup>84</sup> Being able to trick such locks using previously exposed biometric patterns can lead to an extensive attack surface, which could expand to physical access to the property.

The consequences of such access range from extortion to reputational damage and monetization-based scenarios. One of the most obvious is burglary and theft, especially in the case of influencers who regularly show off the internal surroundings (and wealth) of their home while simultaneously exposing all the biometric details needed to bypass their security setup.

## Next-Generation Retail, Public Transport Payments, and Cash Withdrawal

Next-generation retail services<sup>85</sup> and biometric-based payment systems in public transport are already in production or available as prototypes in several countries. Successful attacks on biometric-based authentication could lead to a victim who has been impersonated to be charged with shopping purchases or the cost of a public transport ticket. In some cases, the financial impact will not be significant, but the side effect of this is that the possibility of the case being investigated by law enforcement would be low. Due to successful attacks in that category, in some cases they could be classified as a new variation of the salami slicing attack.<sup>86</sup>

We see that more and more ATMs are being equipped with biometric features. If these features allow cash withdrawal without providing a bank card, successful authentication using exposed biometric features could lead to direct financial impact for the owner of the bank account.

## Abusing Remote Authentication Mechanisms

Remote authentication mechanisms allow access to a remotely located asset. Access to a bank account using online banking or access to cloud storage that requires biometric authentication are good examples of this.

The key feature of remote authentication mechanisms (compared to local mechanisms) is that the authenticating party has limited control and visibility on sensor integrity and sensor environment. When a person accesses a building, the chance of a sensor being controlled is much higher compared to a sensor installed in an attacker-controlled environment that is used to access remote assets.

Attackers can, for example, choose lighting conditions, use artificial copies of fingers, and inject and fake sensor output — all before this data is sent to the back end for authentication. However, this also means that the attack surface for remote authentication scenarios is normally bigger compared to a local one.

The major use cases for remote authentication are account authentication and confirmation of transactions. There are known vulnerabilities for biometrics that help bypass two-factor authentication (2FA) and can be used by an attacker, for example, to gain access to iCloud accounts of victims.<sup>87</sup> Studies have also been carried out on remote fingerprint authentication.<sup>88</sup>

## Confirming Account and Financial Transactions Using Embedded Gadget Features

Many financial applications or applications capable of initiating financial transactions provide access or confirm transactions using embedded biometric-capture features in the gadget. For example, many mobile bank applications allow the confirmation of transactions using embedded fingerprint scanners or facial recognition capabilities instead of initiating standard 2FA procedures. Successfully bypassing biometric authentication could directly leave a financial impact on the impersonated victim.

A second use case is the confirmation of sensitive actions on the device, like installing software from stores and even untrusted sources, adding accounts to the host, or editing sensitive documents.

## Future Devices

We expect that more and more IoT and IIoT devices will have biometric capture and processing capabilities. For example, virtual and augmented reality devices will have more biometric authentication capabilities.<sup>89</sup> If such devices are tricked, attackers can gain access to a variety of digital assets in the metaverse, games, or even get additional spying capabilities if the devices are used in high-tech production.

Physical assets like next-generation cars could also be affected in the near future. With biometric-based keyless car access, which is expected to be available at scale soon,<sup>90</sup> the consequences of successful attacks on biometric algorithms can affect valuable physical assets.

# Advice for Readers

In recent years, society has raised many questions about the exposure of personal information. Many jurisdictions have already gone a step further and accepted laws like the General Data Protection Regulation (GDPR),<sup>91</sup> which clarifies rules on personal information processing and other regulatory guidelines<sup>92</sup> on some use cases of biometric data processing. The big issue is that these laws and regulations are linked to a particular jurisdiction, while the content is exposed globally. As a side effect of that global exposure, in the near future organizations and individuals will be capable of processing biometric data and monetizing it.

In this section, we provide recommendations to help decrease the risks and consequences of biometric pattern exposure. The section also gives suggestions for the general audience, together with suggestions for specific groups who own, handle, process, or use biometrics.

## What Makes Biometrics Different From Other Authentication and Identification Methods

Biometric features like an individual's face, fingerprints, and iris pattern cannot be changed as easily as a password. If any of these are leaked, it can trigger consequences for a decade or even longer.<sup>93</sup>

In some cases, an unintentional biometric leak that happened in your teens can follow you for your entire life. Behavioral biometrics such as how people interact with a device, their typing cadence, or the angle they hold a device, meanwhile, have more flexibility. However, if their device is compromised, these traits can be profiled and substituted at the telemetry level.

People should realize that while their biometric features will never leave them, once lost they can still be replicated and uncontrollably distributed just like any other exposed digital asset. At the same time, an incident of biometric exposure has much more limited avenues for mitigation compared to other sensitive assets like passwords or exposed credit card data.

# General Suggestions

We recommend the following best practices to the general public:

- **Minimize exposure of biometric patterns.** With modern life, it is understandably very hard to keep face and voice patterns from exposure. However, a degree of control over other biometric patterns such as fingerprints or iris patterns can still be kept to a minimum for most internet users.
- **Minimize reliance on biometric factors that are commonly publicly exposed or have a high possibility of exposure.** Using facial recognition for authentication to confirm remote banking transactions can be riskier compared to using less exposed biometric factors.
- **Minimize the quality of exposed media or the parts of exposed media that potentially contain biometric features.** Alternatively, consider transparent manipulation of this data in random ways that are imperceptible to a human but drastically different to a computer. For example, modifying an iris pattern in a photo will create a perceptible difference only to a computer.
- **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.** For these individuals, it is better to adopt a risk profile where biometrics should always already be assumed as compromised and should only be used as part of two-factor methods for any authentication. For privacy purposes, they should also assume that any media recording featuring them in which they are supposedly anonymous could still likely be tied to their real identity with increasing ease in the coming years.

## 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

For common advice to stick to, we have six golden recommendations:

- 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<sup>94</sup> and Yandex Images<sup>95</sup> 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.

In addition to our general suggestions, we also ask the reader to consider the following:

- 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.



Figure 20. Reflections from several sources of light (left) versus a single source on a public YouTube video (right)<sup>96</sup>

*Image credit: Jazmin Castro/YouTube*

# Conclusion

Biometric data should be treated like a password that never expires. Even though currently criminals can't reliably use this information to mount attacks at scale, that does not mean that this will always be so.

In some recent cases, we've seen that an attacker needs access to physical devices such as a phone or a laptop belonging to a victim to plan and push through with attacks that use leaked data. This is a worrying scenario in a range of coercive control scenarios, but this too will change with the increasing use of biometrics in society.

For years, people have both intentionally and unintentionally exposed their sensitive biometric data on the internet. Still, unintentional exposure can be more damaging than intentional because the person sharing is not aware that exposure has occurred.

As users, we are losing control of such data, and its future uses and the risks from the platforms we use every day are not understood well by the common user. Indeed, data from social media networks are already being used by governments and even startups to extract biometrics and build identification models for surveillance cameras.<sup>97</sup>

The same data is or will be used in the most sensitive parts of our lives, both now and in the future. For example, it will be used when we access our banking accounts, use cashless payments for public transport and next-generation shops, cross borders, choose keyless driving, or if part of the police force, when we investigate a crime. The specifics of biometric data mean that every individual has a limited number of biometric features (like fingerprints, face, voice, iris, retina, or palm) that they cannot change, unlike passwords.

The fact that our biometric data cannot be changed means that in the future, having such a treasure trove of data will be increasingly useful for criminals. Whether that future is five or 20 years ahead, the data is available now. We owe it to our future selves to take precautions today to protect ourselves in the world of tomorrow.

Together with that the availability of data, developments in data-mining technologies, artificial intelligence, and the existence of data breaches with PII significantly increases the attack surface of exposed biometric data. This can affect nearly every person on the planet in the future.

In this paper, we highlighted key risks that stem from biometric features that are already exposed in social media and messaging platforms at scale. Malicious actors could use collected data to bypass identification and authentication for sensitive financial and government services, not to mention to access restricted areas that require biometric authentication, commit digital identity theft, abuse reputation and social scoring systems, create deepfakes, and even trigger alerts for law enforcement.

The problem of exposed biometric data is a hard one for humanity to address. We recommend the following measures:

- Minimize the unintended exposure of high-quality media.
- Prioritize the use of less exposed biometric patterns for access to sensitive areas, especially for remote authentication.
- Use a combination of static and behavioral biometrics and other methods for authentication.
- Tackle the problem at scale through significant policy changes that address the use of current and previously exposed biometric data for both present and future activities.

We hope that increased awareness and our suggestions will help readers minimize additional security risks related to exposed biometrics for ordinary people as well as for organizations who use or provide biometric-based technologies. The way that the world will develop solutions to tackle the difficult problems of identification and authentication of its inhabitants for a variety of services will continue to evolve and move forward. It is our hope that some of the concerns raised in this work will help inform more detailed conversations and encourage better overall solutions for society.

# Appendix

## Testing Exposed Data Against Real-World Devices

We investigated scenarios related to the three types of features that are widely used for authentication: fingerprints, face, and iris. For all cases, in either our own research or in external reputable sources, we found confirmation of the existence of the threats and risks we are trying to evaluate.

We tried to answer questions such as is it possible to use unintentionally leaked fingerprints to identify a person based on a photo exposed on social media? Can a camera with facial recognition capabilities be tricked by a non-sophisticated attacker? Can algorithms of a hardware iris sensor be tricked using other objects? Is the resolution of the media content exposed on social media enough to enroll or authenticate a person on an iris sensor?

In this section, we focus on the technologies and capabilities that allow someone to process, attack, and trick biometric systems, or to make decisions based on exposed fingerprints, faces, and irises.

### Fingerprints

Fingerprints are normally acquired in an 8-bit-per-pixel grayscale format with recommended resolution greater than or equal to 500 pixels per inch or greater than 197 pixels per centimeter.<sup>98</sup> The acquisition area can be between 12.8 and 25.4 mm in width and 16.5 and 24.5 mm in height for most standards. That means that an image of a fingerprint starting from 252 by 325 pixels can be enough to identify a person.



**Table 1.** A comparison of PIV, PassDEÜV and CNIPA-A/B/C requirements for the main quality parameters.

Parameter	Requirement				
	PIV IQS [4] [9]	PassDEÜV IQS [13]	CNIPA		
			IQS A	IQS B	IQS C
Acquisition area	w ≥ 12.8mm h ≥ 16.5mm	w ≥ 16.0mm h ≥ 20.0mm	w ≥ 25.4mm h ≥ 25.4mm	w ≥ 15.0mm h ≥ 20.0mm	w ≥ 12.8mm h ≥ 16.5mm
Native resolution	R <sub>N</sub> ≥ 500ppi				
Output resolution	R <sub>N</sub> ± 2%	R <sub>N</sub> ± 1%	R <sub>N</sub> ± 1%	R <sub>N</sub> ± 1.5%	R <sub>N</sub> ± 2%
Gray-level quantization	256 gray-levels (8 bpp)				
Geometric accuracy	In 99% of the tests: D <sub>AC</sub> ≤ max{0.0013", 0.018·X} D <sub>AL</sub> ≤ 0.027"	In 99% of the tests: D <sub>AC</sub> ≤ max{0.0007", 0.01·X} D <sub>AL</sub> ≤ 0.016"	In all the tests: D <sub>Ref</sub> ≤ 1.5%	In all the tests: D <sub>Ref</sub> ≤ 2.0%	In all the tests: D <sub>Ref</sub> ≤ 2.5%
Input/output linearity	No requirements	D <sub>Lin</sub> ≤ 7.65	No requirements		
Spatial frequency response	MTF <sub>min</sub> (f) ≤ MTF(f) ≤ 1.12 see [1] for PIV MTF <sub>min</sub> (f)	MTF <sub>min</sub> (f) ≤ MTF(f) ≤ 1.05 see [1] MTF <sub>min</sub> (f) values	For each region: TSF ≥ 0.20	For each region: TSF ≥ 0.15	For each region: TSF ≥ 0.12
Gray level uniformity	In 99% of the cases: D <sub>RC</sub> <sup>dark</sup> ≤ 1.5; D <sub>RC</sub> <sup>light</sup> ≤ 3 For 99% of the pixels: D <sub>PP</sub> <sup>dark</sup> ≤ 8; D <sub>PP</sub> <sup>light</sup> ≤ 22 For every two small areas: D <sub>St</sub> <sup>dark</sup> ≤ 3; D <sub>St</sub> <sup>light</sup> ≤ 12	In 99% of the cases: D <sub>RC</sub> <sup>dark</sup> ≤ 1; D <sub>RC</sub> <sup>light</sup> ≤ 2 For 99.9% of the pixels: D <sub>PP</sub> <sup>dark</sup> ≤ 8; D <sub>PP</sub> <sup>light</sup> ≤ 22 For every two small areas: D <sub>St</sub> <sup>dark</sup> ≤ 3; D <sub>St</sub> <sup>light</sup> ≤ 12	No requirements		
Signal-to-noise <sup>1</sup>	SNR ≥ 70.6	SNR ≥ 125	SNR ≥ 70.6	SNR ≥ 49.4	SNR ≥ 30.9
Fingerprint gray range	For 80% of the images: DR ≥ 150	DR ≥ 200 for 80% images; DR ≥ 128 for 99% images	For 10% of the images: DR ≥ 150	For 10% of the images: DR ≥ 140	For 10% of the images: DR ≥ 130

Figure 21. Required quality for fingerprint capture based on different standards<sup>99</sup>

Image credit: A. Alessandrini et al/CiteSeerX

For as long as people have discussed fingerprint-based biometrics, they have also asked, “Is it possible to trick a fingerprint sensor?”

The answer is simple: yes. It is possible to find dozens of approaches showing how to defeat fingerprint sensors and how to improve the security of such sensors in academic papers. Some of those papers even include images of fake fingers created to trick sensors.<sup>100</sup>



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

Image credit: Aditya Singh Rathore et al/Network and Distributed Systems Security (NDSS) Symposium

The papers we reviewed regularly included success rate statistics of finger-spoofing attacks on different classes of devices. For the partial fingerprint sensors often used in smartphones and laptops, the success rate can reach nearly 90%.<sup>102</sup> For more specialized devices that use full fingerprints, the success rate is lower but still high enough to consider spoofing attack as a serious problem.

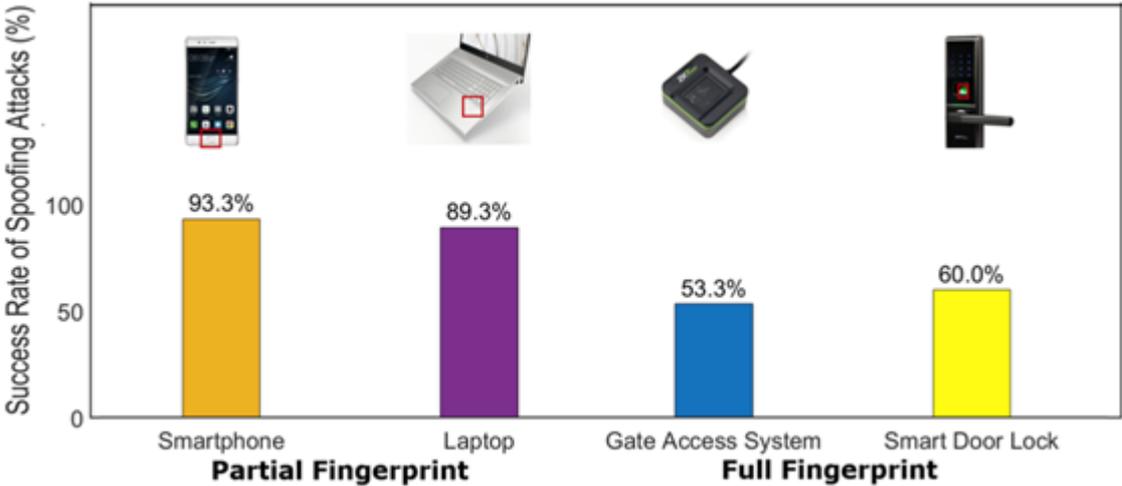


Figure 23. Success rate of spoofing attack with high-precision fake fingers

It is important to note that the sensor is just one piece of the puzzle during fingerprint-based authentication. Fingerprint data stored on the device can also be attacked. In some cases, malicious processes can gain access to the fingerprint sensor and fingerprints can be collected from a victim. These attacks have already been illustrated at security conferences<sup>103</sup> and confirm how biometric-based identification and authentication sensors can be tricked. In bigger deployments and distributed systems, the attack surface is even wider.

In this paper, we focus on the risks of exposed biometric features in social media. In this context, it is important to know if photographs can be used to recreate, enroll, or authenticate a person. Again, the answer is yes, and we have found several confirmations of such scenarios. The first confirmation occurred in 2019 when a researcher called “darkshark9” was able to unlock a Samsung Galaxy S10 by printing a 3D model of his finger. He used a photograph of his fingerprint on a wine glass and created an alpha mask from the fingerprint using Adobe Photoshop. After that, he used Autodesk 3ds Max software to make a highly detailed 3D model. This 3D model was printed on an AnyCubic Photon LCD resin printer with a quality capable of keeping all the ridges of the fingerprint properly rendered. In the end, the researcher was able to use his printed finger model to successfully unlock the phone.<sup>104</sup>

In 2020, researchers from Cisco Talos achieved an average 80% success rate defeating fingerprint scanners across a dozen devices. They also used a 3D printer to generate imposter fingers and had a budget under US\$2,000 to implement the attack. The researchers tested three different scenarios for capturing fingerprints, including direct collection where they took a mold of the target’s relevant fingerprint.

The second scenario used sensor data gathered from scanners like those at border crossings, while the third involved lifting prints from objects like a bottle that the target had held. Notably, Apple's MacBook Pro 2018 Touch ID was one of the devices that was successfully tricked by the researchers.<sup>105</sup>

These two examples confirm that possession of fingerprint photos is often enough to bypass fingerprint sensors. In the context of this paper, the only question left is whether it is possible to trick fingerprint-based identification and authentication with the restrictions we have in our scope here. A more precise way to ask this would be, "Can publicly exposed images of fingerprints be used to identify a person or bypass fingerprint-based security mechanisms?" The answer to both versions of the question is yes.

In two cases, we found police officers using exposed media content to track criminals. In the first one, a drug dealer in Liverpool was identified after they shared a photo of Stilton cheese on an online chat, which led to the exposure of their fingerprints and palm pattern.<sup>106</sup> In the second case, a digital image of a fingerprint helped resolve a fraud case in Finland.<sup>107, 108</sup>

At the 2014 Chaos Communication Congress, biometry hacker and programmer Jan Krissler presented some interesting research related to the recreation of fingerprint patterns from photos exposed on social media. Krissler used several high-resolution photos, including a photo from a press release of the German Defense Minister at that time, Ursula von der Leyen, to reverse-engineer her fingerprints.<sup>109</sup> It is worth noting that the quality of online photos has risen substantially since 2014 due to the increase in sophistication of today's modern mobile devices.

In sum, these cases mean the following:

- A variety of fingerprint sensors, including those embedded in smartphones and laptops, can be tricked successfully in attacks.
- Photos and videos can be used to recreate fingerprint patterns necessary for authentication.
- The quality of public media content is enough to obtain and use fingerprint patterns exposed on posted media for possible malicious activity.

## Facial Recognition

Facial recognition is based on several approaches, the simplest option of which is to recognize frames from ordinary cameras like web cameras, cameras embedded in a variety of IoT devices, and smartphones. More advanced options rely on the use of near-infrared range because of the high level of robustness to illumination that changes in the acquired images.<sup>110</sup>

Additional security enhancements include the projection of thousands of invisible dots to collect extra information about face features or liveness detection where, according to recent research, machines are outperforming humans.<sup>111</sup>

Several standards and minimal requirements for the image quality needed to conduct face recognition exist, such as ISO/IEC 19794-5 – Biometric data interchange formats. We can also consider that exposed facial images, which are matching requirements for the National Institute of Standards and Technology (NIST) Ongoing Face Recognition Vendor Test (FRVT),<sup>112</sup> fall within the scope of this paper. The following is an example of an image from the NIST paper that states that the portrait orientation of a 640-by-480-pixel image is enough for facial recognition. That also means that this resolution quality has existed for many years in many popularly used cameras and devices.

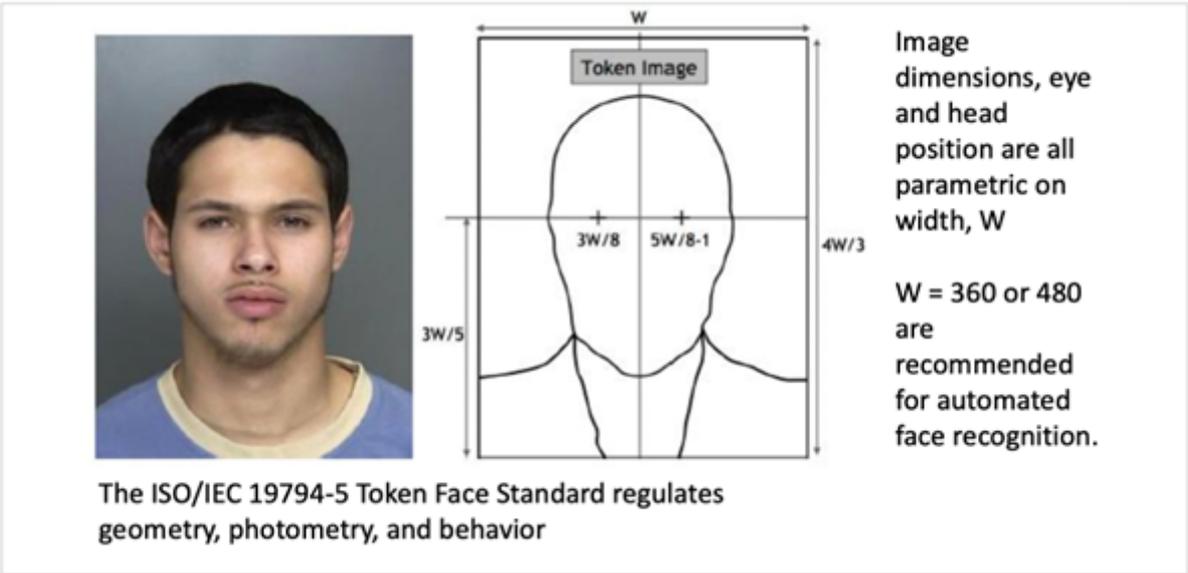


Figure 24. Parameters of images for face recognition<sup>113</sup>

*Image credit: Patrick Grother et al/National Institute of Standards and Technology (NIST)*

Several attacks on face recognition devices have been successfully demonstrated by Trend Micro researchers in another recent project that investigated the security of edge devices. The scenarios included the demonstration of several attack vectors like the bypass of facial recognition using static photos displayed on mobile devices.<sup>114</sup>

More advanced sensors can claim liveness detection as a key feature that helps prevent impersonation attacks. The attacks scenarios that successfully bypass liveness detection have also been demonstrated at security conferences.<sup>115</sup> The authors used the following prototype to bypass the attention detection mechanism of Face ID.

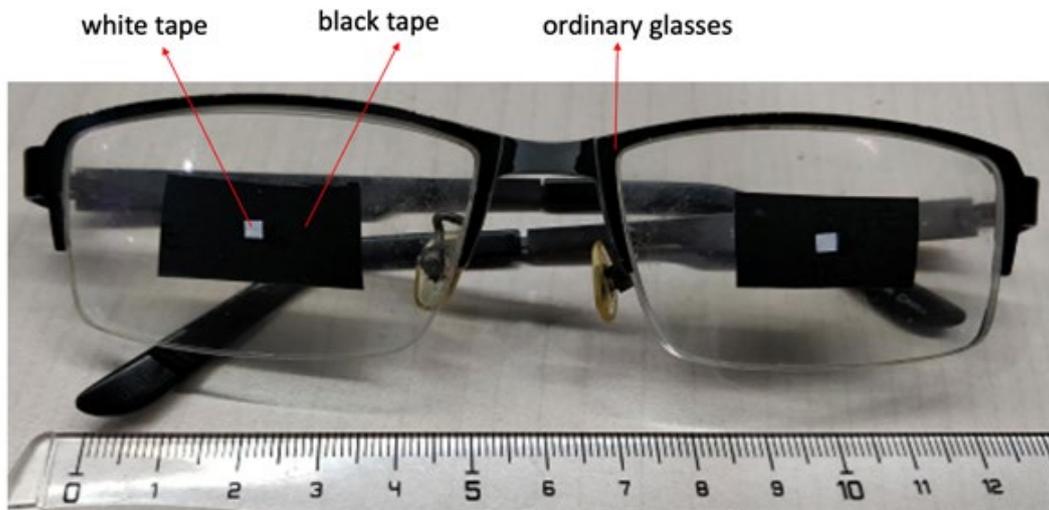


Figure 25. Prototype of glasses used to bypass the attention detection mechanism of Face ID, presented at BlackHat USA 2019<sup>116</sup>

*Image credit: Yu Chen, Bin Ma, HC Ma/BlackHat*

Clearly, human faces are one of the most publicly exposed biometric features that an attacker can misuse. Since this has already been confirmed by dozens of research papers, we decided to dive deeper into the less investigated biometric features in the context of public media exposure, namely iris recognition.

## Iris Recognition

Iris recognition is often used in more sensitive areas like automated border control, access to server rooms in data centers, and access to government buildings. The leak of iris patterns in media content is not as obvious as the leak of voice patterns in audio records or facial patterns in portrait photos or videos. Since we already have confirmation of successful attacks on face recognition systems in our previous research, we decided to conduct a deeper analysis and investigation of the possible misuses of an iris pattern.

We raised the following questions in our research:

- Is the quality of exposed social media content enough to enroll or recognize eye patterns?
- Can exposed eye patterns or photographs of different objects be detected as eyes by a hardware iris sensor?
- Is it possible to enroll a pattern from an image and also authenticate it using an image?
- Can the pattern of one person under certain conditions be recognized as belonging to another person?
- Is it possible to enroll a pattern from a social media image, and then authenticate it using the real eye?
- Is it possible to enroll a real eye and then authenticate it using an image from social media?

To answer these questions, we made an initial analysis confirming that the resolution of leaked images could suffice for use. We then purchased a hardware iris sensor (IriShield-USB MK 2120U) and conducted a series of experiments. In this section, we share our insights on the conducted experiments.

## What is the Baseline for Detection and Recognition?

To understand how the sensor processes the iris and what the baseline is, we enrolled an iris several times from the same researcher. We then conducted recognition of the same enrolled iris before doing the same for an unenrolled iris.

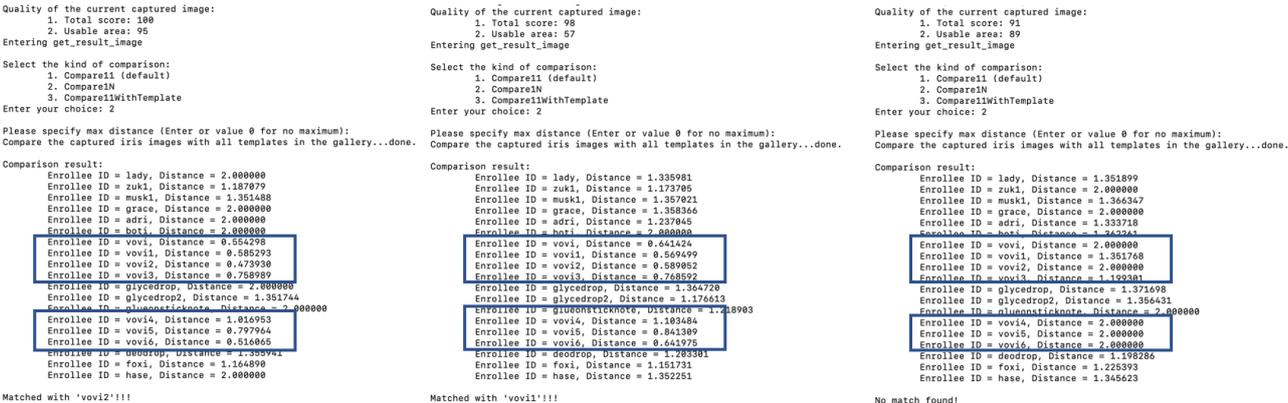


Figure 26. The baseline for pattern recognition: an enrolled iris in perfect conditions (left), an enrolled iris in slightly degraded conditions with the eye partially closed (middle), and an unenrolled eye with perfect conditions (right)

In the screenshot, we see that in the near ideal conditions (usable area 95, total score 100), the distance is around 0.5 to 0.8 for the known patterns, which should match, and around 1.2 to 2 for other enrolled patterns. For degraded conditions (usable area 57, total score 98), the distance is around 0.6 to 0.9 for the known pattern, which should match, and around 1.2 to 2.0 for other patterns. The same ratio, around 1.2 to 2.0, was maintained for the attempt to recognize an unenrolled pattern.

Based on this observation, we can say that having a maximal distance between 0.8 and 1.2 would be accepted in our experiments as successful, while having the stricter distance below 0.8 can significantly increase the success of attacks in the wild.

## Is the Quality of Exposed Media Content Enough to Enroll or Recognize Eye Patterns?

Many portrait photos from official government and corporate websites, journals, and news outlets with several megapixel resolution are potentially suitable for iris processing.

According to the ISO/IEC 19794-6:2011 – Information technology – Biometric data interchange formats – Part 6: Iris image data,<sup>117</sup> a VGA resolution of 640 by 480 pixels is suitable for an eye and JPEG 2000 and

PNG formats are suitable for compression. An alternative standard from the NIST<sup>118</sup> suggests that the resolution of about 160 pixels for an iris, or a pixel scale between 15.7 and 12.3 pixels per millimeter, is enough for iris recognition. This scale is widely seen on many commercial and professional portraits that are publicly available.

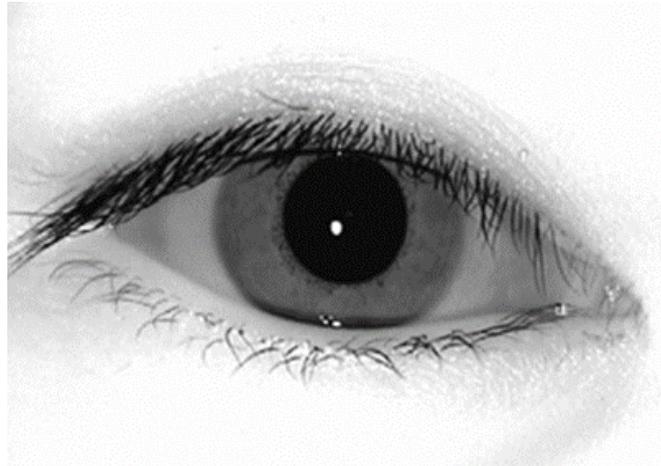


Figure 27. Example of eye image provided in ISO/IEC 19794-6:2011 suitable for iris recognition

During this research, we conducted a series of black box analysis with a hardware iris sensor. Black box analysis means that we haven't opened the case of the device to analyze its electronics and have used standard firmware and tools provided by the vendor to conduct our experiments.

We found that several preliminary stages are required before an iris pattern can be enrolled or recognized. After initiation, the device captures and analyzes a series of frames in the near-infrared range. The objective of initial analysis is to recognize the fact that an eye was presented to device. The next stage is to spot the iris and analyze the quality of the provided pattern. The quality had two criteria on the device we tested: the usable area and a total score. Both seemed to be measured between the range 0 and 100 based on the results we obtained in our experiments.

As long as both these criteria are above predefined threshold values, the next stage of the algorithm will be triggered. At this stage, a pattern with appropriate quality can be either enrolled into the system or compared one-to-one or one-is-to-many with previously stored patterns. Reaching and passing this stage by using exposed media content was a crucial part of the research stage.

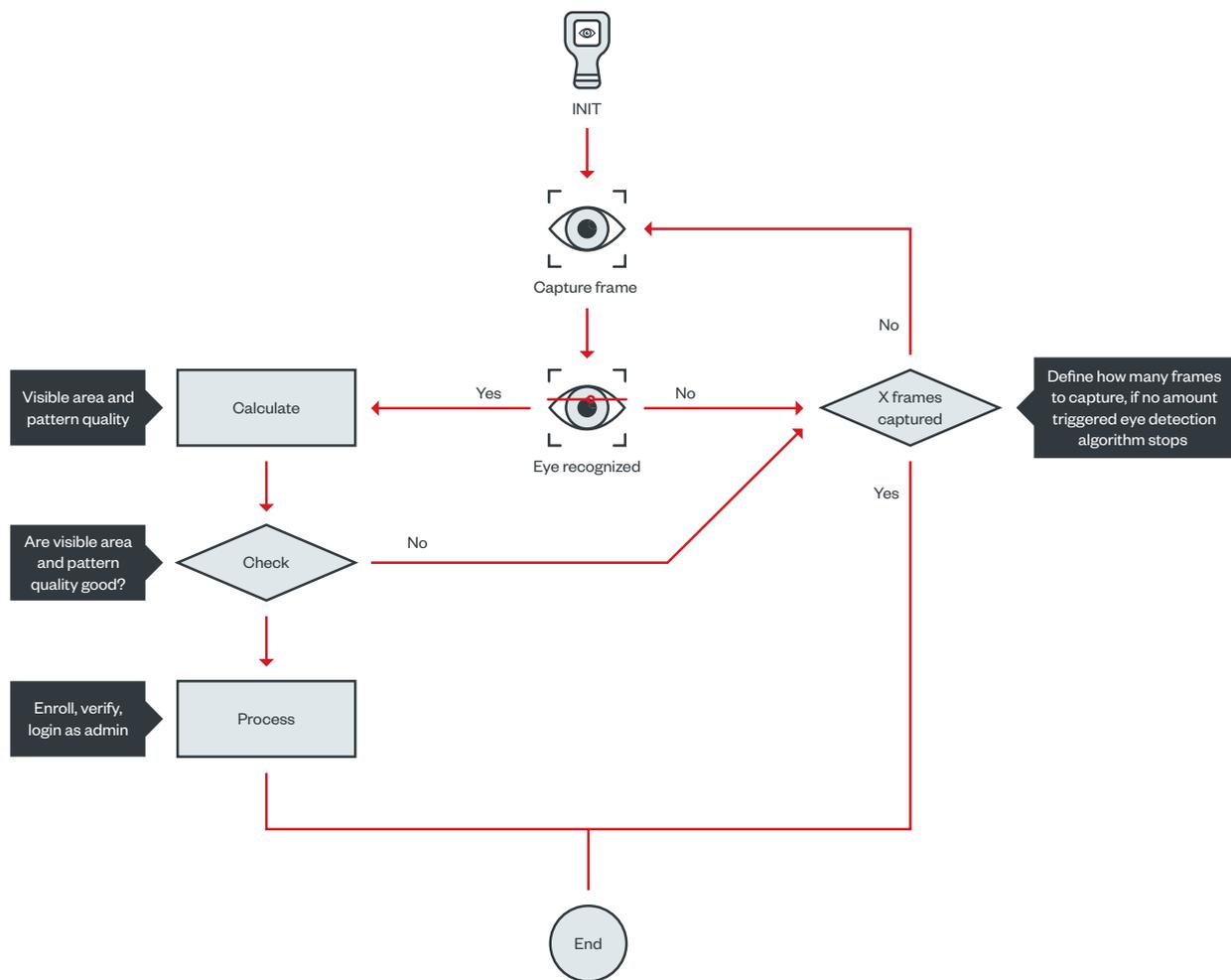


Figure 28. Diagram of the image-processing logic

The path to reach this stage was far from straightforward since we intentionally chose a hardware iris sensor instead of using ordinary cameras to capture and process iris patterns. The sensor has a variety of security measures to minimize the attack surface.

The focus distance at which an eye can be captured is limited, and because of this, the size of the pattern presented to the device is also limited in physical size. The device also has additional security features that limit the use of external lenses to manipulate the size of the provided pattern.

We conducted experiments with several smartphone external lenses connected to the iris sensor. As a result, the quality of captured images degrades so significantly that it was barely possible to trigger eye recognition. We think that these security measures significantly limited the attack surface compared to a situation where cameras are embedded in smartphones and used for iris capture and processing.

For example, it was not possible to present the image of an eye that is significantly bigger than a normal eye at a greater distance to the sensor, something that is potentially possible for normal lenses. Also, the iris scanners' use of near-infrared filters and the embedded light source significantly limits the sources from which the images can be collected to attempt to present a pattern to the sensor.

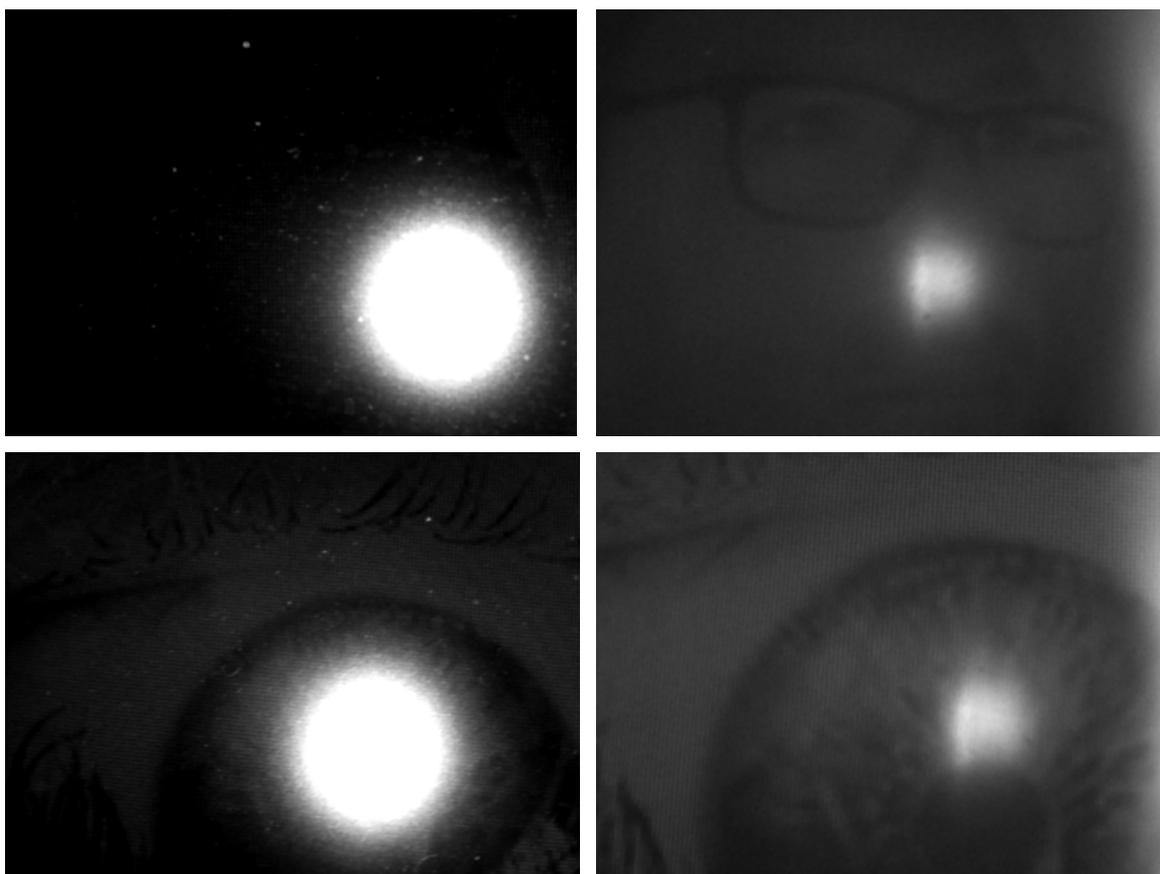


Figure 29. Examples of the image captures from an Apple MacBook Pro display: standard capture (left) versus light source covered (right); an eye displayed on the Samsung monitor with standard capture versus light source covered (bottom)

It was clear that due to security measures of the hardware iris sensor, the quality of the first images we captured was far from the expectations and requirements of the standards. We continued our investigation, gradually improving results every time. After our first experiments, it was clear that sensors will carry out zero actions of iris recognition before first detecting that an eye was successfully presented to the sensor.

More importantly, understanding how the camera recognizes a human eye and not a random object was a key step to moving forward with our research.

### **Can Exposed Eye Patterns or Photographs of Different Objects Be Detected as Eyes by a Hardware Iris Sensor?**

After several rounds of experimentation, we manipulated several images, shapes, and objects that triggered the eye detection routine.

The iris sensor we tested indicates when an eye is detected by blinking with a blue light. At this stage, parameters like usable area and total score are captured. Successfully bypassing this stage was key to continuing with our experiments on iris pattern recognition. We first started experiments with real eyes,

which were detected almost immediately according to the device. We then moved to testing exposed eye images from social media, eyes displayed on various screen types, and eyes printed on different types of paper.

With exposed media, we initially had limited success. Over several days there were several successful eye recognitions, but these happened after long attempts of moving the camera around images to view them from different angles, distances, and positions. Although we had limited success, it was a significant step forward. We also found that bypassing eye detection is very important to move our research further.

To understand how the eye detection algorithm works, we conducted a series of experiments under different lighting conditions both by using the embedded source of light in the camera and by covering it. During experiments on real eyes, the detection of an eye was much better when we used the embedded light. This led us to our hypothesis about the importance of the role of light reflection in eye detection algorithms.

We compared images that were captured by the camera when eyes were successfully detected and found that a bright white dot located in the middle of the pupil was one of the key features for these images. Knowing this, we modified our patterns by adding a white circle with different radii in the middle of the pupil and found that this significantly improved eye detection rate.



Figure 30. Example of patterns created from exposed media content

For the experiments, we also scaled exposed social media images to different sizes to find the best size suitable for fooling the iris sensor. With this modification, the eye detection ratio increased dramatically, but we still decided to conduct several extra experiments to challenge the limits of the eye detection algorithm.

The next experiment was to create a fully artificial image of an eye using embedded shapes in Microsoft Word and then see if it is possible to trick the eye recognition algorithm. Unexpectedly, the attempt was successful in many (but not all) cases. The success depended on the textures around the “artificial iris” and the size of the image.

We tested the eye bypassing algorithm using images of an eye drawn in different scales. It should be noted that this is to recognize the image as being an eye, not to match this eye image successfully against a previously stored pattern.

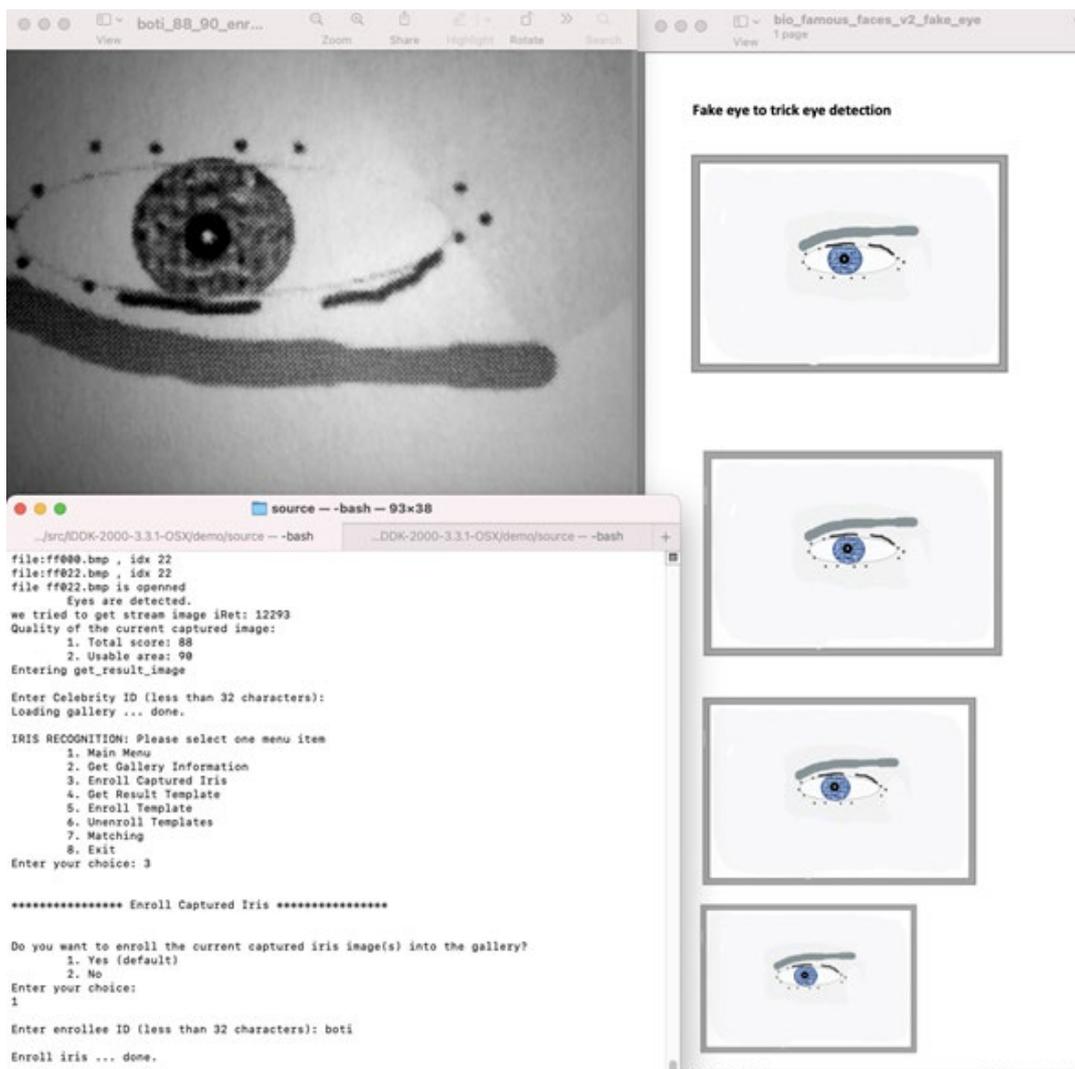


Figure 31. An “advanced version” of an artificial iris created using embedded shapes in Microsoft Word that was successfully recognized with a quality acceptable for enrollment

Based on these results, we went through an extra round of experiments to see what the simplest version of an “eye” triggers the eye detection routine. The answer was that most of the time, an image with three simple embedded circles, one of which just had texture plus one line, was enough to trigger the routing. The results of this experiment are provided in Figure 32.

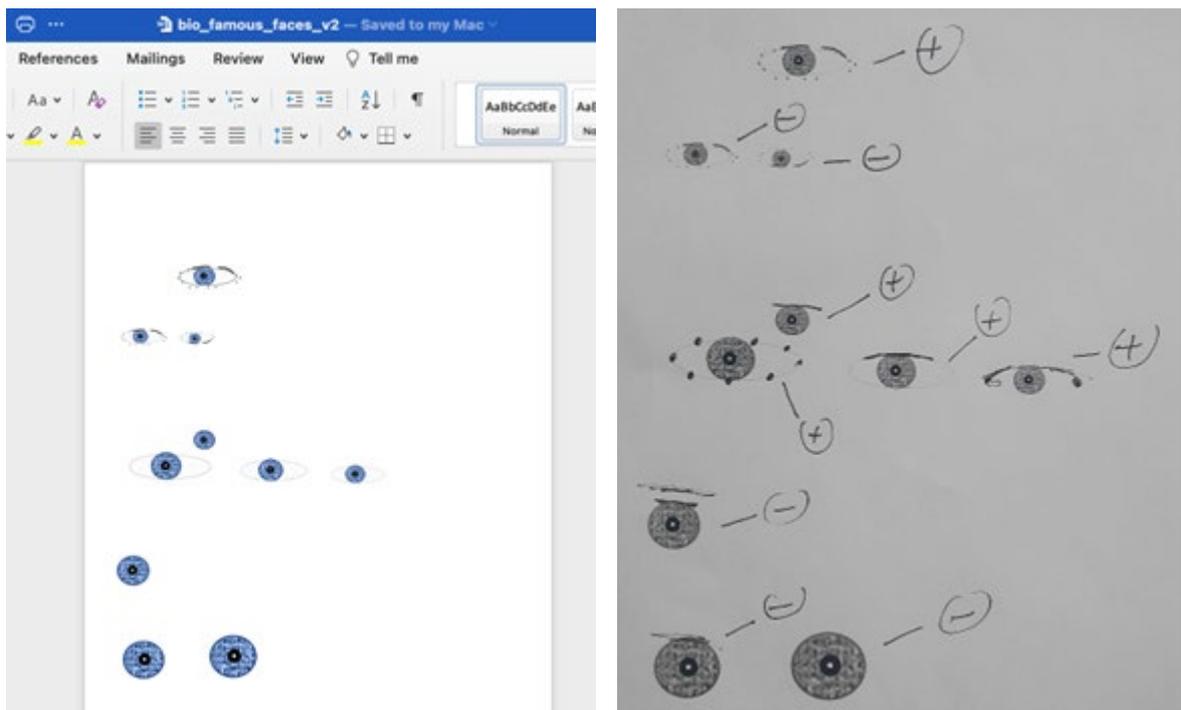


Figure 32. A simplified version of an artificial iris created using embedded shapes in Microsoft Word showing successful and non-successful eye detections; the “+” symbol means the camera recognized the image as an eye

The next experiments were conducted to understand if non-eye related images and objects can trigger eye detection by the iris sensor. We found several classes of objects that triggered the eye detection routine. We experimented with different types of liquids, plush toys, and transparent glue drops on photos. We succeeded at least once with every class of object.

On the left and the middle sections of the Figure 33, we show that an eye of a plush toy together with a liquid drop on a Trend Micro-branded mousepad triggers eye detection. The image captured by the iris sensor when the eye detection was triggered is on the right side of the figure.

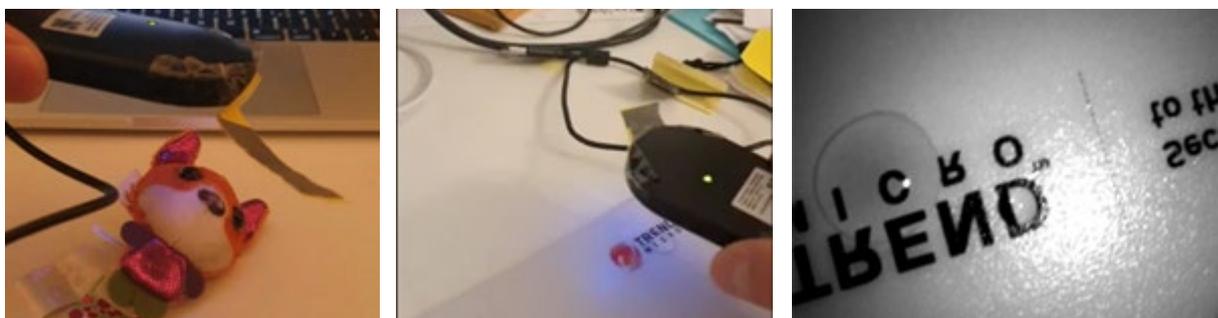


Figure 33. The eye of a plush toy and the drop of the liquid on the Trend Micro mousepad trigger the eye detection routine.

After those experiments, our understanding of how to trigger the eye detection phase of the camera advanced significantly. We then moved on to targeting pattern recognition. More importantly, for this stage of the research, we found it was not necessary to wait for the processing of several hundred frames. After image enhancements, we could trigger the eye detection routine almost immediately if patterns were of the appropriate quality.

### Is It Possible to Enroll an Eye Pattern From an Image and Authenticate From Another Image?

The answer is yes. We were even able to successfully enroll and recognize irises captured from portraits exposed on the internet.

While the iris sensor we tested works in near-infrared light, it significantly degrades the quality of images captured from the screens of devices with active displays. At the same time, it is still possible to use passive displays like a Kindle E-reader to display an image of an iris that would be visible in near-infrared light. In Figure 34, we see a comparison of an iris presented on different media and captured by an iPad camera and an AD 100 iris sensor. This is from the arXiv archive.<sup>119</sup>

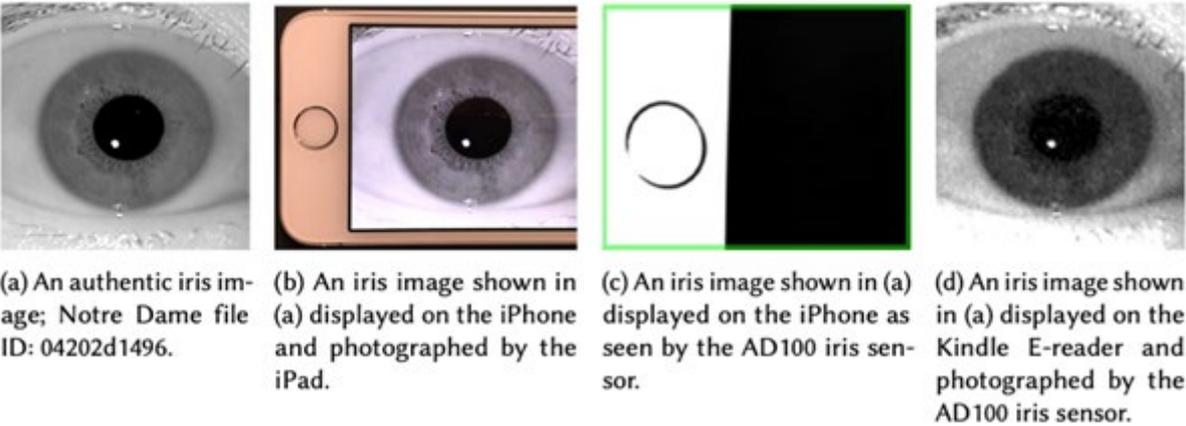


Figure 34. Comparison of an iris presented on different media and captured by different devices

In our experiments, we printed images of irises that we collected from the internet. We made some minor modifications on the images to improve eye detection ratio. For the experiments, we chose several portrait pictures from journals or official company websites.

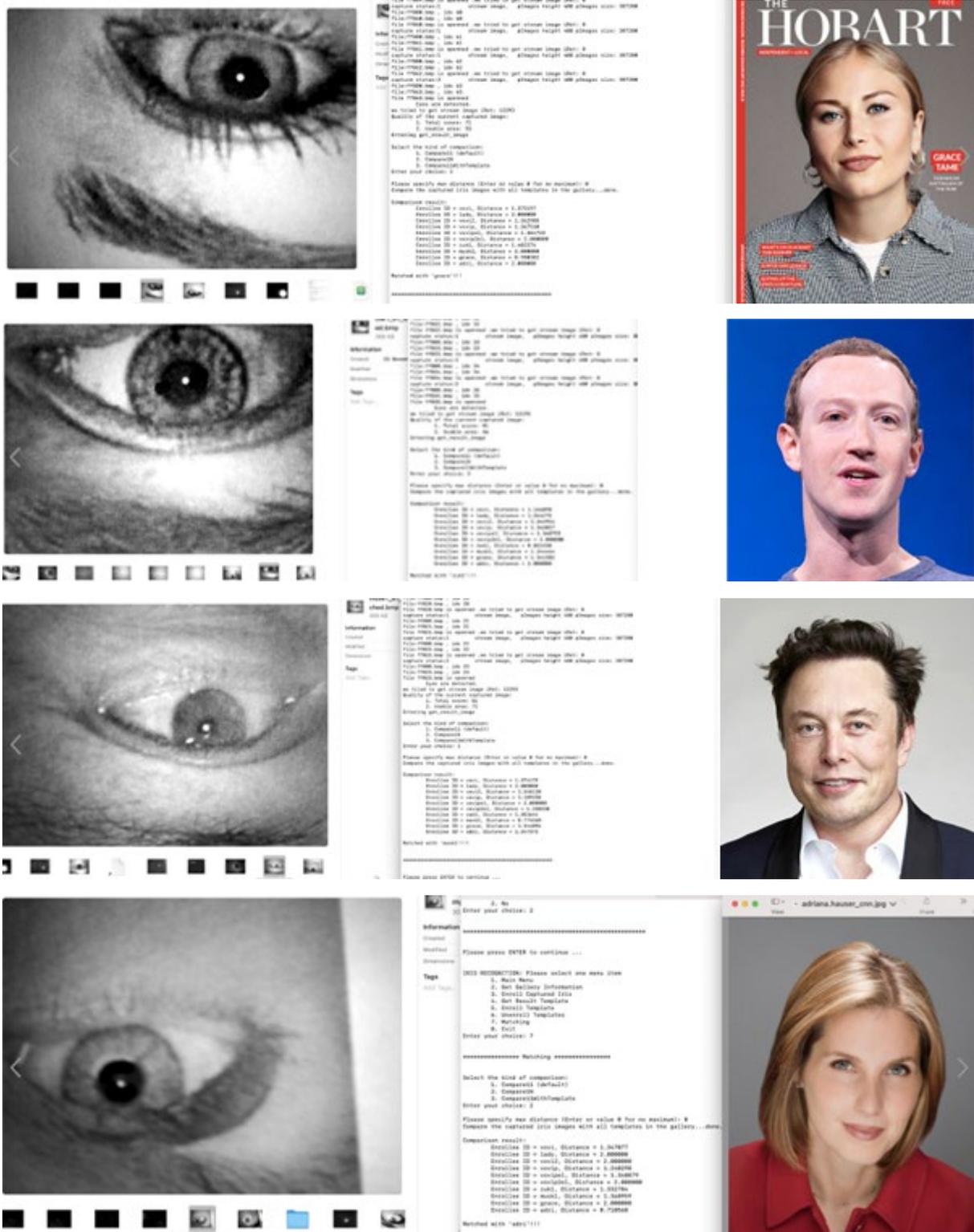


Figure 35. Examples of successful enrollment and matching of irises captured from portraits exposed on the internet (the second and third portraits are just representations of images from Wired<sup>120</sup> and Bloomberg<sup>121</sup>)

*Image credit: Wikimedia Commons*

We were able to successfully enroll and recognize majority of the patterns that have enough resolution and quality. Examples of enrollment and recognition together with original photos are provided in Figure 35. For two patterns, the distance is even below the stricter 0.8 threshold (0.71, 0.77), while for one it is close (0.82), and for another, it is below the maximal 1.0 distance (0.98).

This experiment confirms the possibility of attacks on biometric systems with remote iris authentication, where creation of accounts can also be done remotely.

## Can the Eye Pattern of One Person Be Recognized as Belonging to Another Person Under Certain Conditions?

The answer is it is sometimes possible. According to our experiments on tuning the presented eye image, and through knowledge of how the vendor implements security thresholds, this is possible under some less likely conditions.

In the screenshot in Figure 36, we can see the result of matching an iris pattern that hasn't been enrolled into the system with one of the patterns enrolled into the system. It is important to note that the conditions when the iris was captured were intentionally degraded — the eye was not fully opened and the lighting conditions were deliberately not perfect. The distance 0.96 is also below the threshold we determined in our baseline experiments. This is visible in the screenshot, where the total score is relatively low, and the usable area also indicates that the iris was not fully visible.

```
file:ff030.bmp , idx 30
file ff030.bmp is opened
  Eyes are detected.
we tried to get stream image iRet: 12293
Quality of the current captured image:
  1. Total score: 32
  2. Usable area: 43
Entering get_result_image

Select the kind of comparison:
  1. Compare11 (default)
  2. Compare1N
  3. Compare11WithTemplate
Enter your choice: 2

Please specify max distance (Enter or value 0 for no maximum)
Compare the captured iris images with all templates in the g

Comparison result:
  Enrollee ID = lady, Distance = 1.341388
  Enrollee ID = zuk1, Distance = 1.239555
  Enrollee ID = musk1, Distance = 1.230378
  Enrollee ID = grace, Distance = 1.348928
  Enrollee ID = adri, Distance = 1.210109
  Enrollee ID = boti, Distance = 1.181434
  Enrollee ID = vovi, Distance = 1.342836
  Enrollee ID = vovi1, Distance = 1.175032
  Enrollee ID = vovi2, Distance = 1.203831
  Enrollee ID = vovi3, Distance = 0.966689
  Enrollee ID = glycedrop, Distance = 1.347872
  Enrollee ID = glycedrop2, Distance = 1.149981
  Enrollee ID = glueonsticknote, Distance = 1.253842
  Enrollee ID = vovi4, Distance = 1.216360
  Enrollee ID = vovi5, Distance = 1.200771
  Enrollee ID = vovi6, Distance = 1.216494
  Enrollee ID = deodrop, Distance = 1.278133
  Enrollee ID = foxi, Distance = 1.223609
  Enrollee ID = hase, Distance = 1.340965

Matched with 'vovi3'!!!
```

Figure 36. Result of the recognition of a pattern that wasn't enrolled into the system in a one-is-to-many test

However, the scenario we investigated in this section has real-life use cases with remote biometric authentication, specifically in situations where the authenticating party does not have full control over the biometric sensor and environmental conditions. One example is when a user uses biometrics to authenticate an account on an online banking portal.

## Is It Possible to Enroll a Pattern From an Image and Authenticate It With the Corresponding Real Eye?

The answer is yes. We succeeded in enrolling a pattern from the researcher by using a printed image of an eye and managed to match it to the real eye pattern.

We conducted this experiment using images of the researcher's eyes printed on paper. The experiment itself took several rounds and required finding appropriate lighting conditions for capturing.

```
Comparison result:
  Enrollee ID = lady, Distance = 1.352432
  Enrollee ID = vovip, Distance = 1.345469
  Enrollee ID = vovipel, Distance = 2.000000
  Enrollee ID = vovip2el, Distance = 1.200633
  Enrollee ID = zuk1, Distance = 1.335125
  Enrollee ID = musk1, Distance = 1.381506
  Enrollee ID = grace, Distance = 2.000000
  Enrollee ID = adri, Distance = 2.000000
  Enrollee ID = vovidl1, Distance = 1.231451
  Enrollee ID = vovipdl1, Distance = 0.811143

Matched with 'vovipdl1'!!!
```

Figure 37. Matching of a real eye to the pattern enrolled from an image printed on paper

The distance between the enrolled pattern and the pattern from a real eye captured (0.81) was comparable to the distance of a real eye that was enrolled and matched. Successful implementation of this attack can help attackers implement different scenarios, including creating accounts for people who never provided their biometrics for enrollment.

The ability to enroll a person from leaked media and authenticate their real eye can lead, for example, to extortion and reputational damage. An attacker might expose that a high-profile individual (a politician, a celebrity, or a top government or corporate employer) is allegedly partaking in controversial activities such as gambling or pornography. This type of accusation, coupled with faked biometric evidence, can be very hard for that person to fight against.

This would be made even harder with an intentionally leaked (and faked) database showing logs related to dates and times of logins plus successful authentication using a verifiable biometric pattern.

## Is It Possible to Enroll a Real Eye and Authenticate It Against a Pattern From an Image?

The answer is probably yes. We conducted experiments with patterns printed on monochrome laser printers with results coming close to successful.

The resolution of the printer was limited compared to other photo printers that were not tested. The closest distance was for patterns enrolled from the same person under different conditions; however, the distance 1.18 was still more than 1.0, and so it is above the thresholds we determined as a baseline for our experiments to accept the results as a successful one-is-to-many identification.

```
Enrollee ID = lady, Distance = 2.000000
Enrollee ID = zuk1, Distance = 1.229158
Enrollee ID = musk1, Distance = 2.000000
Enrollee ID = grace, Distance = 1.231238
Enrollee ID = adri, Distance = 1.262931
Enrollee ID = boti, Distance = 2.000000
Enrollee ID = vovi, Distance = 1.351827
Enrollee ID = vovi1, Distance = 1.337057
Enrollee ID = vovi2, Distance = 1.207523
Enrollee ID = vovi3, Distance = 1.209559
Enrollee ID = glycedrop, Distance = 2.000000
Enrollee ID = glycedrop2, Distance = 1.333445
Enrollee ID = glueonsticknote, Distance = 2.000000
Enrollee ID = vovi4, Distance = 1.180270
Enrollee ID = vovi5, Distance = 1.207059
Enrollee ID = vovi6, Distance = 1.199296
```

Figure 38. Attempt to match a printed pattern to the pattern enrolled from a real eye

Since the major focus of this research is related to the risks of exposed biometric data, we decided to leave opportunities for future research here and stop our experiments with hardware iris sensors at this point. We already have enough findings to prove that exposed biometric data can be used in attacks and presented to different biometric sensors.

Also, considering that in many cases, normal (not near-infrared) cameras are used, the reuse of exposed biometric patterns would be even easier.

# References

- 1 Artem Kukhareenko. (n.d.). *NtechLab*. “Real Time Planetary Scale Face Recognition System.” Accessed on Sept. 23, 2022, at [https://www.nist.gov/system/files/documents/2020/09/03/10\\_ntechlab\\_nist\\_2016.pdf](https://www.nist.gov/system/files/documents/2020/09/03/10_ntechlab_nist_2016.pdf).
- 2 NBC New York. (Aug. 22, 2016). *NBC New York*. “Some Burglars Using Social Media to Find Targets, I-Team Survey Shows.” Accessed on Sept. 23, 2022, at <https://www.nbcnewyork.com/news/local/investigations-i-team-social-media-use-survey-new-york-new-jersey/1329983>.
- 3 Sketchfab. (n.d.). *Sketchfab*. “tag:facescan.” Accessed on Sept. 23, 2022, at [https://sketchfab.com/search?q=tag%3Afacescan&sort\\_by=-likeCount&type=models](https://sketchfab.com/search?q=tag%3Afacescan&sort_by=-likeCount&type=models).
- 4 Thomas Brewster. (n.d.) *Forbes*. “We Broke Into A Bunch Of Android Phones With A 3D-Printed Head.” Accessed on Sept. 23, 2022, at <https://www.forbes.com/sites/thomasbrewster/2018/12/13/we-broke-into-a-bunch-of-android-phones-with-a-3d-printed-head/?sh=450b8efa1330>.
- 5 Vivek Wadhwa. (July 5, 2021). *Foreign Policy*. “Killer Flying Robots Are Here. What Do We Do Now?” Accessed on Sept. 23, 2022, at <https://foreignpolicy.com/2021/07/05/killer-flying-robots-drones-autonomous-ai-artificial-intelligence-facial-recognition-targets-turkey-libya>.
- 6 Makeup | cosmetics. (n.d.). *Telegram*. Accessed on Sept. 23, 2022, at <https://t.me/ideyaka/2226%20>.
- 7 Magic of beauty | make up | cosmetics. (n.d.) *Telegram*. Accessed on Sept. 23, 2022, at <https://t.me/makiyazh3/8677>.
- 8 Danny Donchev. (Sept. 9, 2022). *FortuneLords*. “40 Mind Blowing YouTube Facts, Figures and Statistics – 2022.” Accessed on Sept. 23, 2022, at <https://fortunelords.com/youtube-statistics>.
- 9 SerScience. (June 16, 2022, at 2:34 p.m.) *Twitter*. “Just writing...” Accessed on Sept. 23, 2022, at [https://twitter.com/science\\_ser/status/1537322831813431296](https://twitter.com/science_ser/status/1537322831813431296).
- 10 European Commission. (n.d.). *European Commission*. “Search results (54132)”. Accessed on Sept. 23, 2022, at <https://audiovisual.ec.europa.eu/en/search?mediatype=PHOTO&categories=Portrait>.
- 11 European Commission. (n.d.). *European Commission*. “Search results (54132)”. Accessed on Sept. 23, 2022, at <https://audiovisual.ec.europa.eu/en/search?mediatype=PHOTO&categories=Portrait>.
- 12 European Commission. (n.d.). *European Commission*. “Helena Dalli, European Commissioner for Equality.” Accessed on Sept. 23, 2022, at <https://audiovisual.ec.europa.eu/en/photo-details/P-041101~2F00-01>.
- 13 European Commission. (n.d.). *European Commission*. “Participation of Ursula von der Leyen, President of the European Commission, in the plenary session of the European Parliament.” Accessed on Sept. 23, 2022, at <https://audiovisual.ec.europa.eu/en/photo-details/P-057062~2F00-49>.
- 14 Loukia Gyftopoulou. (June 28, 2022). *Bloomberg*. “Jupiter CEO Quits \$68 Billion Firm to Sit at the Beach and ‘Do Nothing.’” Accessed on Sept. 23, 2022, at <https://www.bloomberg.com/news/articles/2022-06-28/formica-plans-to-step-down-as-jupiter-ceo-beesley-to-take-over>.
- 15 Larisa Brown. (March 20, 2021). *The Sunday Times*. “Army creates Ranger regiment to free up Special Forces.” Accessed on Sept. 23, 2022, at <https://www.thetimes.co.uk/article/british-army-creates-ranger-regiment-k0kfckkw3>.
- 16 Larisa Brown. (March 20, 2021). *The Sunday Times*. “Army creates Ranger regiment to free up Special Forces.” Accessed on Sept. 23, 2022, at <https://www.thetimes.co.uk/article/british-army-creates-ranger-regiment-k0kfckkw3>.
- 17 Larisa Brown. (March 20, 2021). *The Sunday Times*. “Army creates Ranger regiment to free up Special Forces.” Accessed on Sept. 23, 2022, at <https://www.thetimes.co.uk/article/british-army-creates-ranger-regiment-k0kfckkw3>.
- 18 Konrad Lischka. (Nov. 5, 2011). *Spiegel*. “Grinsemaske ohne Botschaft.” Accessed on Sept. 23, 2022, at <https://www.spiegel.de/netzwelt/netzpolitik/anonymus-und-guy-fawkes-grinsemaske-ohne-botschaft-a-795927.html>.
- 19 Numaan Huq et al. (Aug. 8, 2022). *Trend Micro*. “The Trouble with the Metaverse.” Accessed on Sept. 23, 2022, at <https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/metaworse-the-trouble-with-the-metaverse>.
- 20 Numaan Huq et al. (Feb. 16, 2021). *Trend Micro*. “Cybersecurity for Connected Cars: Exploring Risks in 5G, Cloud, and Other Connected Technologies.” Accessed on Sept. 23, 2022, at [https://documents.trendmicro.com/assets/white\\_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf](https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-for-connected-cars-exploring-risks-in-5g-cloud-and-other-connected-technologies.pdf).

- 21 SciShow Kids. (May 16, 2018). *YouTube*. "See Your Own Fingerprints!" Accessed on Sept. 23, 2022, at [https://www.youtube.com/watch?v=cZKGpg\\_ftw&ab\\_channel=SciShowKids](https://www.youtube.com/watch?v=cZKGpg_ftw&ab_channel=SciShowKids).
- 22 Alyssa A. Reinhart. (2004). *California State Science Fair*. "Comparing the Differences of Clarity of Fingerprints on the Surface of Glass in Different Temperature Environments." Accessed on Sept. 23, 2022, at <https://csef.usc.edu/History/2004/Projects/J0514.pdf>.
- 23 Joanna MacLeod. (Sept. 2, 2017). *Murdoch University*. "Affordable Counterfeit Fingerprints: Investigating the Potential Forensic Applications of 3D Printing." Accessed on Sept. 23, 2022, at <https://researchrepository.murdoch.edu.au/id/eprint/39806/1/MacLeod2017.pdf>.
- 24 German Castignani et al. (2015). *IEEE Xplore*. "Driver Behavior Profiling Using Smartphones: A Low-Cost Platform for Driver Monitoring." Accessed on Sept. 23, 2022, at <https://ieeexplore.ieee.org/abstract/document/7014406>.
- 25 Abayomi Moradeyo Otebolaku and Maria Teresa Andrade. (May 2016). *Journal of Network and Computer Applications*. "User context recognition using smartphone sensors and classification models." Accessed on Sept. 23, 2022, at <https://www.sciencedirect.com/science/article/abs/pii/S1084804516300261>.
- 26 Payments Journal. (June 4, 2020). *Payments Journal*. "By 2024, How Many Smartphone Owners Will Use Biometrics?" Accessed on Sept. 23, 2022, at <https://www.paymentsjournal.com/by-2024-how-many-smartphone-owners-will-use-biometrics/>.
- 27 Allan Jay. (n.d.). *FinancesOnline*. "Number of Smartphone and Mobile Phone Users Worldwide in 2022/2023: Demographics, Statistics, Predictions." Accessed on Sept. 23, 2022, at <https://financesonline.com/number-of-smartphone-users-worldwide/>.
- 28 Vincenzo Ciancaglini et al. (Sept. 8, 2020). *Trend Micro*. "Identified and Authorized: Sneaking Past Edge-Based Access Control Devices." Accessed on Sept. 23, 2022, at [https://documents.trendmicro.com/assets/white\\_papers/wp-identified-and-authorized-sneaking-past-edge-based-access-control-devices.pdf](https://documents.trendmicro.com/assets/white_papers/wp-identified-and-authorized-sneaking-past-edge-based-access-control-devices.pdf).
- 29 Defend Digital Me. (n.d.) *Defend Digital Me*. "The State of Biometrics 2022: A Review of Policy and Practice in UK Education". Last accessed on Oct. 7, 2022 at <https://defenddigitalme.org/research/state-biometrics-2022/>.
- 30 NAN. (July 5, 2021). *The Guardian*. "FG embarks on biometric enumeration of pupils on school feeding programme." Accessed on Sept. 23, 2022, at <https://guardian.ng/news/fg-embarks-on-biometric-enumeration-of-pupils-on-school-feeding-programme>.
- 31 Christiawan. (October 2018). *IEEE Xplore*. "Fingershield ATM – ATM Security System using Fingerprint Authentication." Accessed on Sept. 23, 2022, at <https://ieeexplore.ieee.org/document/8605473/authors#authors>.
- 32 Alex Schmidt. (Aug. 6, 2013). *Marketplace*. "Brazilian banks lead way on biometrics." Accessed on Sept. 23, 2022, at <https://www.marketplace.org/2013/08/06/brazilian-banks-lead-way-biometrics>.
- 33 Will Sturgeon. (Aug. 12, 2004). *ZDNET*. "Biometrics used to keep German Olympians safe." Accessed on Sept. 23, 2022, at <https://www.zdnet.com/article/programming-languages-its-time-to-stop-using-c-and-c-for-new-projects-says-microsoft-azure-cto>.
- 34 Sports Business Journal. (July 11, 2022). *Sports Business Journal*. "Partly cloudy: While Clear's tech is well-respected, the company is still figuring out where it fits in the sports world." Accessed on Sept. 23, 2022, at <https://www.sportsbusinessjournal.com/Journal/Issues/2022/07/11/Portfolio/Facilities-and-Ticketing.aspx>.
- 35 Lufthansa Group. (April 28, 2022). *Lufthansa Group*. "Contactless travel with facial recognition: Star Alliance Biometrics now also at Hamburg Airport." Accessed on Sept. 23, 2022, at <https://www.lufthansagroup.com/en/newsroom/releases/contactless-travel-with-facial-recognition-star-alliance-biometrics-now-also-at-hamburg-airport.html>.
- 36 Chris Burt. (Jan. 5, 2022). *Biometric Update*. "Easier queues with biometrics, touchless check-ins set to reach more airports." Accessed on Sept. 23, 2022, at <https://www.biometricupdate.com/202201/easier-queues-with-biometrics-touchless-check-ins-set-to-reach-more-airports>.
- 37 FBI. (n.d.). *FBI*. "Next Generation Identification (NGI)." Accessed on Sept. 23, 2022, at <https://www.biometricupdate.com/202201/easier-queues-with-biometrics-touchless-check-ins-set-to-reach-more-airports>.
- 38 Unique Identification Authority of India (UIDAI). (n.d.). *Unique Identification Authority of India (UIDAI)*. "About UIDAI." Accessed on Sept. 23, 2022, at <https://uidai.gov.in/en/about-uidai.html>.
- 39 Federal Authority for Identity, Citizenship, Customs & Port Security (ICP). (Nov. 8, 2022). *Federal Authority for Identity, Citizenship, Customs & Port Security (ICP)*. "UAE Pass." Accessed on Sept. 23, 2022, at <https://icp.gov.ae/en/uae-pass>.

- 40 Identity Week. (May 19, 2021). *Identity Week*. "Evolution not revolution: Why mobile fingerprint sensors are here to stay." Accessed on Sept. 23, 2022, at <https://identityweek.net/evolution-not-revolution-why-mobile-fingerprint-sensors-are-here-to-stay>.
- 41 Patrick Farley. (June 22, 2022). *Microsoft*. "Quickstart: Use the Face service." Accessed on Sept. 23, 2022, at <https://learn.microsoft.com/en-us/azure/cognitive-services/computer-vision/quickstarts-sdk/identity-client-library?tabs=visual-studio&pivots=programming-language-csharp>.
- 42 Amazon Web Services. (n.d.). *Amazon Web Services*. "Detecting and analyzing faces." Accessed on Sept. 23, 2022, at <https://docs.aws.amazon.com/rekognition/latest/dg/faces.html>.
- 43 YouTube Help. (n.d.). *Google*. "Updated Terms of Service FAQs." Accessed on Sept. 23, 2022, at <https://support.google.com/youtube/answer/10090902?hl=en#zippy=%2Cwhy-did-you-change-the-terms-of-service%2Cwhat-are-the-main-changes%2Cchow-will-this-affect-my-ypp-monetization%2Cdoes-this-have-to-do-with-the-european-union-copyright-directive-or-gdpr%2Cwhat-does-this-mean-for-my-privacy-or-data>.
- 44 Mayra Rosario Fuentes et al. (Dec. 2, 2021). *Trend Micro*. "Security for the Next-Generation Retail Supply Chain." Accessed on Sept. 23, 2022, at <https://www.trendmicro.com/vinfo/fi/security/news/internet-of-things/security-for-the-next-generation-retail-supply-chain>.
- 45 Mayra Rosario Fuentes et al. (Dec. 2, 2021). *Trend Micro*. "Security for the Next-Generation Retail Supply Chain." Accessed on Sept. 23, 2022, at <https://www.trendmicro.com/vinfo/fi/security/news/internet-of-things/security-for-the-next-generation-retail-supply-chain>.
- 46 Sergio Mannino. (May 8, 2020). *Forbes*. "How Facial Recognition Will Change Retail." Accessed on Sept. 23, 2022, at <https://www.forbes.com/sites/forbesbusinesscouncil/2020/05/08/how-facial-recognition-will-change-retail/?sh=3db4b94f3daa>.
- 47 Tech Xplore. (Oct. 15, 2021). *Tech Xplore*. "Moscow metro launches face recognition payments." Accessed on Sept. 23, 2022, at <https://techxplore.com/news/2021-10-moscow-metro-recognition-payments.html>.
- 48 Tech Xplore. (Oct. 25, 2020). *Tech Xplore*. "Dubai introduces facial recognition on public transport." Accessed on Sept. 23, 2022, at <https://techxplore.com/news/2020-10-dubai-facial-recognition.html>.
- 49 Arij Dekker. (Aug. 2001). *Symposium on Global Review of 2000 Round of Population and Housing Censuses: Mid-Decade Assessment and Future Prospects*. "Adapting new technologies to census operations." Accessed on Sept. 23, 2022, at [https://unstats.un.org/unsd/demographic/docs/symposium\\_06.htm](https://unstats.un.org/unsd/demographic/docs/symposium_06.htm).
- 50 PTI. (June 7, 2022). *The Wire*. "Election Commission Says It Is Time to Explore Remote Voting." Accessed on Sept. 23, 2022, at <https://thewire.in/government/election-commission-says-it-is-time-to-exlore-remote-voting>.
- 51 Ayang Macdonald. (April 14, 2022). *Biometric Update*. "Nigeria's biometric voter system detects over 1M invalid entries." Accessed on Sept. 23, 2022, at <https://www.biometricupdate.com/202204/nigerias-biometric-voter-system-detects-over-1m-invalid-entries>.
- 52 Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin. (June 13, 2017). *Trend Micro*. "Fake News and Cyber Propaganda: The Use and Abuse of Social Media." Accessed on Sept. 23, 2022, at [https://documents.trendmicro.com/assets/white\\_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf](https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf).
- 53 China Copyright and Media. (June 14, 2014). *China Copyright and Media*. "Planning Outline for the Construction of a Social Credit System (2014-2020)." Accessed on Sept. 23, 2022, at <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020>.
- 54 Lisa Green. (March 27, 2019). *MarketWatch*. "Should you let your car insurer monitor you?" Accessed on Sept. 23, 2022, at <https://www.marketwatch.com/story/should-you-let-your-car-insurer-monitor-you-2019-03-27>.
- 55 Vikram Dodd. (Jan. 24, 2020). *The Guardian*. "Met police to begin using live facial recognition cameras in London." Accessed on Sept. 23, 2022, at <https://www.theguardian.com/technology/2020/jan/24/met-police-begin-using-live-facial-recognition-cameras>.
- 56 BBC News. (Nov. 27, 2018). *BBC News*. "Chinese AI caught out by face in bus ad." Accessed on Sept. 23, 2022, at <https://www.bbc.com/news/technology-46357004>.
- 57 Thomas Brewster. (Jan. 29, 2020). *Forbes*. "Remember FindFace? The Russian Facial Recognition Company Just Turned On A Massive, Multimillion-Dollar Moscow Surveillance System." Accessed on Sept. 23, 2022, at <https://www.forbes.com/sites/thomasbrewster/2020/01/29/findface-rolls-out-huge-facial-recognition-surveillance-in-moscow-russia/?sh=5c154311463b>.

- 58 Forum of Incident Response and Security Teams (FIRST). (n.d.). *Forum of Incident Response and Security Teams (FIRST)*. "Conference Program." Accessed on Sept. 23, 2022, at <https://www.first.org/conference/2022/program#pYour-Phone-is-Not-Your-Phone-A-Dive-Into-SMS-PVA-Fraud>.
- 59 Numaan Huq et al. (Feb. 16, 2021). *Trend Micro*. "In Transit, Interconnected, at Risk: Cybersecurity Risks of Connected Cars." Accessed on Sept. 23, 2022, at <https://www.trendmicro.com/vinfo/ae/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars>.
- 60 Patrick Howell O'Neill. (Aug. 14, 2019). *MIT Technology Review*. "Data leak exposes unchangeable biometric data of over 1 million people." Accessed on Sept. 23, 2022, at .
- 61 SafetyDetectives. (March 11, 2020). *SafetyDetectives*. "Brazil: Millions of Records Leaked, Including Biometric Data." Accessed on Sept. 23, 2022, at <https://www.safetydetectives.com/blog/antheus-leak-report>.
- 62 Antonio Bianchi et al. (2018). *Network and Distributed Systems Security (NDSS) Symposium*. "Broken Fingers: On the Usage of the Fingerprint API in Android." Accessed on Sept. 23, 2022, at [https://reyammer.io/publications/2018\\_ndss\\_fingerprint.pdf](https://reyammer.io/publications/2018_ndss_fingerprint.pdf).
- 63 The MITRE Corporation. (n.d.). *The Mitre Corporation*. "CVE-2020-7958." Accessed on Sept. 23, 2022, at <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-7958>.
- 64 Christian Zeitz et al. (n.d.). *CiteSeerX*. "Security issues of Internet-based biometric authentication systems: risks of Man-in-the-Middle and BioPhishing on the example of BioWebAuth." Accessed on Sept. 23, 2022, at <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1022.5453&rep=rep1&type=pdf>.
- 65 Robert McArdle. (Sept. 1, 2020). *Trend Micro*. "The Life Cycle of a Compromised (Cloud) Server." Accessed on Sept. 23, 2022, at [https://www.trendmicro.com/de\\_de/research/20/i/the-life-cycle-of-a-compromised-cloud-server.html](https://www.trendmicro.com/de_de/research/20/i/the-life-cycle-of-a-compromised-cloud-server.html).
- 66 Eduardo Baptista. (April 8, 2022). *Reuters*. "China uses AI software to improve its surveillance capabilities." Accessed on Sept. 23, 2022, at <https://www.reuters.com/world/china/china-uses-ai-software-improve-its-surveillance-capabilities-2022-04-08>.
- 67 The Moscow Times. (May 24, 2018). *The Moscow Times*. "Moscow Arrests 42 Suspects Using New Facial Recognition Technology in Metro Station." Accessed on Sept. 23, 2022, at <https://www.themoscowtimes.com/2018/05/24/russias-gazprom-satisfied-after-settling-eu-antitrust-case-without-fines-a61566>.
- 68 Trend Micro. (May 8, 2018). *Trend Micro*. "Exposed Video Streams: How Hackers Abuse Surveillance Cameras." Accessed on Sept. 23, 2022, at <https://www.trendmicro.com/vinfo/fr/security/news/internet-of-things/exposed-video-streams-how-hackers-abuse-surveillance-cameras>.
- 69 Ars Electronica. (n.d.). *Ars Electronica*. "Obama Deep Fake Jordan Peele." Accessed on Sept. 23, 2022, at <https://ars.electronica.art/center/en/obama-deep-fake>.
- 70 BBC News. (Nov. 12, 2019). *BBC News*. "The fake video where Johnson and Corbyn endorse each other." Accessed on Sept. 23, 2022, at <https://www.bbc.com/news/av/technology-50381728>.
- 71 Business Standard. (July 19, 2019). *Business Standard*. "'Deepfake CEOs' are stealing millions from companies." Accessed on Sept. 23, 2022, at [https://www.business-standard.com/article/news-ani/deepfake-ceos-are-stealing-millions-from-companies-119071901535\\_1.html](https://www.business-standard.com/article/news-ani/deepfake-ceos-are-stealing-millions-from-companies-119071901535_1.html).
- 72 Trend Micro, United Nations Interregional Crime and Justice Research Institute (UNICRI), and Europol. (Nov. 19, 2020). *Trend Micro, United Nations Interregional Crime and Justice Research Institute (UNICRI), and Europol*. "Exploiting AI: How Cybercriminals Misuse and Abuse AI and ML." Accessed on Sept. 23, 2022, at <https://www.trendmicro.com/vinfo/ie/security/news/cybercrime-and-digital-threats/exploiting-ai-how-cybercriminals-misuse-abuse-ai-and-ml>.
- 73 Payment Village. (n.d.). *Payment Village*. "How I used deepfakes to bypass security verifications in a bank." Accessed on Sept. 23, 2022, at <https://www.paymentvillage.org/blog/how-i-used-deepfakes-to-bypass-security-verifications-in-a-bank>.
- 74 Payment Village. (n.d.). *Payment Village*. "How I used deepfakes to bypass security verifications in a bank." Accessed on Sept. 23, 2022, at <https://www.paymentvillage.org/blog/how-i-used-deepfakes-to-bypass-security-verifications-in-a-bank>.
- 75 Stephen Hilt. (Sept. 27, 2017). *Trend Micro*. "The Sound of a Targeted Attack." Accessed on Sept. 23, 2022, at <https://documents.trendmicro.com/assets/pdf/the-sound-of-a-targeted-attack.pdf>.
- 76 Stephen Mayhew. (May 23, 2012). *Biometric Update*. "Bank call centers using voice verification." Accessed on Sept. 23, 2022, at <https://www.biometricupdate.com/201205/bank-call-centers-using-voice-verification>.

- 77 Zhengyu Dong et al. (Feb 15, 2022). *Trend Micro*. "SMS PVA: An Underground Service Enabling Threat Actors to Register Bulk Fake Accounts." Accessed on Sept. 23, 2022, at [https://documents.trendmicro.com/assets/white\\_papers/wp-sms-pva-underground-service-enabling-threat-actors-to-register-bulk-fake-accounts.pdf](https://documents.trendmicro.com/assets/white_papers/wp-sms-pva-underground-service-enabling-threat-actors-to-register-bulk-fake-accounts.pdf).
- 78 Barbara Ortutay. (June 24, 2022). *ABC News*. "Instagram tests using AI, other tools for age verification." Accessed on Sept. 23, 2022, at <https://abcnews.go.com/Technology/wireStory/instagram-tests-ai-tools-age-verification-85592466>.
- 79 Shilpi Sharma and JS Sodhi. (2014). *International Journal of Security and Its Applications*. "Implementation of Biometric Techniques in Social Networking Sites." Accessed on Sept. 23, 2022, at [http://article.nadiapub.com/IJSIA/vol8\\_no6/5.pdf](http://article.nadiapub.com/IJSIA/vol8_no6/5.pdf).
- 80 Zhengyu Dong et al. (Feb 15, 2022). *Trend Micro*. "SMS PVA: An Underground Service Enabling Threat Actors to Register Bulk Fake Accounts." Accessed on Sept. 23, 2022, at [https://documents.trendmicro.com/assets/white\\_papers/wp-sms-pva-underground-service-enabling-threat-actors-to-register-bulk-fake-accounts.pdf](https://documents.trendmicro.com/assets/white_papers/wp-sms-pva-underground-service-enabling-threat-actors-to-register-bulk-fake-accounts.pdf).
- 81 Alex Gailey. (April 26, 2021). *NextAdvisor*. "Your Auto Insurer Wants to Ride Shotgun With You. Are the Savings Worth It?" Accessed on Sept. 23, 2022, at <https://time.com/nextadvisor/insurance/car/telematics-monitor-driving-insurance-discount>.
- 82 Fei-Yuang Wang et al. (Aug. 19, 2010). *IEEE Xplore*. "A Study of the Human Flesh Search Engine: Crowd-Powered Expansion of Online Knowledge." Accessed on Sept. 23, 2022, at <https://ieeexplore.ieee.org/document/5551046>.
- 83 Mayra Rosario Fuentes et al. (Dec. 2, 2021). *Trend Micro*. "Security for the Next-Generation Retail Supply Chain." Accessed on Sept. 23, 2022, at <https://www.trendmicro.com/vinfo/fi/security/news/internet-of-things/security-for-the-next-generation-retail-supply-chain>.
- 84 Erica Tempesta. (May 19, 2022). *The Daily Mail*. "Real Housewives of Dallas star Tiffany Moon proudly shows off her \$3 MILLION closet, which has a special FINGERPRINT lock and is home to millions of dollars worth of Hermès bags - including 'the world's tiniest Birkin.'" Accessed on Sept. 23, 2022, at <https://www.dailymail.co.uk/femail/article-10831465/Real-Housewives-Dallas-star-Tiffany-Moon-proudly-shows-3-MILLION-closet.html>.
- 85 Mayra Rosario Fuentes et al. (Dec. 2, 2021). *Trend Micro*. "Security for the Next-Generation Retail Supply Chain." Accessed on Sept. 23, 2022, at <https://www.trendmicro.com/vinfo/fi/security/news/internet-of-things/security-for-the-next-generation-retail-supply-chain>.
- 86 How to Infosec. (June 11, 2021). *How to Infosec*. "What is Salami Attack?" Accessed on Sept. 23, 2022, at <https://howtoinfosec.com/2021/06/11/what-is-salami-attack>.
- 87 Luana Pascu. (Aug. 5, 2020). *Biometric Update*. "Hackers may have manipulated Apple biometric security glitch to access iCloud accounts." Accessed on Sept. 23, 2022, on <https://www.biometricupdate.com/202008/hackers-may-have-manipulated-apple-biometric-security-glitch-to-access-icloud-accounts>.
- 88 Mahesh Joshi, Bodhisatwa Mazumdar, and Somnath Dey. (May 18, 2018). *arXiv*. "Security Vulnerabilities Against Fingerprint Biometric System." Accessed on Sept. 23, 2022, at <https://arxiv.org/pdf/1805.07116.pdf>.
- 89 Arman Bhalla. (May 25, 2021). *ACM Digital Library*. "MoveAR: Continuous Biometric Authentication for Augmented Reality Headsets." Accessed on Sept. 23, 2022, on <https://dl.acm.org/doi/abs/10.1145/3457339.3457983>.
- 90 Ioanna Toufexi. (June 22, 2022). *CambridgeshireLive*. "Six ways driving your car will change by 2030." Accessed on Sept. 23, 2022, at <https://www.cambridge-news.co.uk/news/motors/six-ways-driving-your-car-24291332>.
- 91 Intersoft Consulting. (n.d.). *Intersoft Consulting*. "General Data Protection Regulation GDPR." Accessed on Sept. 23, 2022, at <https://gdpr-info.eu>.
- 92 The European Data Protection Board. (Jan. 29, 2020). *The European Data Protection Board*. "Guidelines 3/2019 on processing of personal data through video devices Version 2.0." Accessed on Sept. 23, 2022, at [https://edpb.europa.eu/sites/default/files/files/file1/edpb\\_guidelines\\_201903\\_video\\_devices\\_en\\_0.pdf](https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf).
- 93 Amanda Morris and Lulu Garcia-Navarro. (Jan. 20, 2019). *NPR*. "Could The 10-Year Challenge Be Putting Your Data At Risk?" Accessed on Sept. 23, 2022, at <https://www.npr.org/2019/01/20/686897486/could-the-10-year-challenge-be-putting-your-data-at-risk?t=1657982303769>.
- 94 Google. (n.d.). *Google*. "Google Images." Accessed on Sept. 23, 2022, at <https://images.google.com>.
- 95 Yandex. (n.d.). *Yandex*. "Yandex Images." Accessed on Sept. 23, 2022, at <https://yandex.com/images>.
- 96 Jazmin Castro. (April 25, 2021). *YouTube*. "Best Mascara Combo to Make Your Lashes Pop." Accessed on Sept. 23, 2022, at [https://www.youtube.com/watch?v=7CjGM2grg\\_0&ab\\_channel=JazminCastro](https://www.youtube.com/watch?v=7CjGM2grg_0&ab_channel=JazminCastro).

- 97 NtechLab. (n.d.). *NtechLab*. "Public Safety With Findface." Accessed on Sept. 23, 2022, at [https://ntechlab.com/en\\_au/solution/public-safety](https://ntechlab.com/en_au/solution/public-safety).
- 98 Patrick Grother, Wayne Salamon, and Randaswami Chandramouli. (July 2013). *National Institute of Standards and Technology (NIST)*. "Biometric Specifications for Personal Identity Verification." Accessed on Sept. 23, 2022, at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-76-2.pdf>.
- 99 A. Alessandrini et al. (n.d.). *CiteSeerX*. "Definition of Fingerprint Scanner Image Quality Specifications by Operational Quality." Accessed on Sept. 23, 2022, at <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.566.4224&rep=rep1&type=pdf>.
- 100 Aditya Singh Rathore et al. (2022). *Network and Distributed Systems Security (NDSS) Symposium*. "FakeGuard: Exploring Haptic Response to Mitigate the Vulnerability in Commercial Fingerprint Anti-Spoofing." Accessed on Sept. 23, 2022, at <https://www.ndss-symposium.org/wp-content/uploads/2022-82-paper.pdf>.
- 101 Aditya Singh Rathore et al. (2022). *Network and Distributed Systems Security (NDSS) Symposium*. "FakeGuard: Exploring Haptic Response to Mitigate the Vulnerability in Commercial Fingerprint Anti-Spoofing." Accessed on Sept. 23, 2022, at <https://www.ndss-symposium.org/wp-content/uploads/2022-82-paper.pdf>.
- 102 Aditya Singh Rathore et al. (2022). *Network and Distributed Systems Security (NDSS) Symposium*. "FakeGuard: Exploring Haptic Response to Mitigate the Vulnerability in Commercial Fingerprint Anti-Spoofing." Accessed on Sept. 23, 2022, at <https://www.ndss-symposium.org/wp-content/uploads/2022-82-paper.pdf>.
- 103 Yulong Zhang et al. (n.d.). *BlackHat*. "Fingerprints On Mobile Devices: Abusing and Leaking." Accessed on Sept. 23, 2022, at <https://www.blackhat.com/docs/us-15/materials/us-15-Zhang-Fingerprints-On-Mobile-Devices-Abusing-And-Leaking-wp.pdf>.
- 104 Davey Winder. (April 6, 2019). *Forbes*. "Samsung Galaxy S10 Fingerprint Scanner Hacked — Here's What You Need to Know." Accessed on Sept. 23, 2022, at <https://www.forbes.com/sites/daveywinder/2019/04/06/samsung-galaxy-s10-fingerprint-scanner-hacked-heres-what-you-need-to-know/?sh=1fe040755d42>.
- 105 Davey Winder. (April 6, 2019). *Forbes*. "Samsung Galaxy S10 Fingerprint Scanner Hacked — Here's What You Need to Know." Accessed on Sept. 23, 2022, at <https://www.forbes.com/sites/daveywinder/2019/04/06/samsung-galaxy-s10-fingerprint-scanner-hacked-heres-what-you-need-to-know/?sh=1fe040755d42>.
- 106 BBC News. (May 24, 2021). *BBC News*. "Cheese photo leads to Liverpool drug dealer's downfall." Accessed on Sept. 23, 2022, at <https://www.bbc.com/news/uk-england-merseyside-57226165.amp>.
- 107 Mikko Hypponen. (June 10, 2022, 6:36 p.m.) *Twitter*. "Local police caught a scammer..." Accessed on Sept. 23, 2022, at <https://twitter.com/mikko/status/1535209158995329024>.
- 108 Poliisi. (June 9, 2022). *Poliisi*. "Petosrikos selvisi tekniikan avulla." Accessed on Sept. 23, 2022, at <https://poliisi.fi/-/petosrikos-selvisi-tekniikan-avulla>.
- 109 Alex Hern. (Dec. 30, 2014). *The Guardian*. "Hacker fakes German minister's fingerprints using photos of her hands." Accessed on Sept. 23, 2022, at <https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hands>.
- 110 Sajhad Farokhi, Jan Flusser, and Usman Ullah Sheikh. (August 2016). *Computer Science Review*. "Near infrared face recognition: A literature survey." Accessed on Sept. 23, 2022, at <https://www.sciencedirect.com/science/article/abs/pii/S1574013716300673?via%3Dihub>.
- 111 ID R&D. (2022). *ID R&D*. "Human or Machine: AI Proves Best at Spotting Biometric Attacks." Accessed on Sept. 23, 2022, at <https://www.idrnd.ai/wp-content/uploads/2022/01/ResearchBrief-HumanVsMachine-JAN2422.pdf>.
- 112 Patrick Grother et al. (July 13, 2022). *National Institute of Standards and Technology (NIST)*. Accessed on Sept. 23, 2022, at [https://pages.nist.gov/frvt/reports/quality/frvt\\_quality\\_report.pdf](https://pages.nist.gov/frvt/reports/quality/frvt_quality_report.pdf).
- 113 Patrick Grother et al. (July 13, 2022). *National Institute of Standards and Technology (NIST)*. Accessed on Sept. 23, 2022, at [https://pages.nist.gov/frvt/reports/quality/frvt\\_quality\\_report.pdf](https://pages.nist.gov/frvt/reports/quality/frvt_quality_report.pdf).
- 114 Vincenzo Ciancaglini et al. (Sept. 8, 2020). *Trend Micro*. "Identified and Authorized: Sneaking Past Edge-Based Access Control Devices." Accessed on Sept. 23, 2022, at [https://documents.trendmicro.com/assets/white\\_papers/wp-identified-and-authorized-sneaking-past-edge-based-access-control-devices.pdf](https://documents.trendmicro.com/assets/white_papers/wp-identified-and-authorized-sneaking-past-edge-based-access-control-devices.pdf).
- 115 Yu Chen, Bin Ma, and HC Ma. (2019). *BlackHat*. "Biometric Authentication Under Threat: Liveness Detection Hacking." Accessed on Sept. 23, 2022, at <https://i.blackhat.com/USA-19/Wednesday/us-19-Chen-Biometric-Authentication-Under-Threat-Liveness-Detection-Hacking.pdf>.

- 116 Yu Chen, Bin Ma, and HC Ma. (2019). *BlackHat*. “Biometric Authentication Under Threat: Liveness Detection Hacking.” Accessed on Sept. 23, 2022, at <https://i.blackhat.com/USA-19/Wednesday/us-19-Chen-Biometric-Authentication-Under-Threat-Liveness-Detection-Hacking.pdf>.
- 117 International Organization for Standardization (ISO). (2017). *International Organization for Standardization (ISO)*. “ISO/IEC 19794-6:2011 Information technology — Biometric data interchange formats — Part 6: Iris image data.” Accessed on Sept. 23, 2022, at <https://www.iso.org/standard/50868.html>.
- 118 Dan Potter, Patrick Grother, and Elham Tabassi. (May 8, 2013). *National Institute of Standards and Technology (NIST)*. Accessed on Sept. 23, 2022, at [https://www.nist.gov/system/files/documents/2021/06/07/idqt\\_testplan\\_draft\\_v7\\_6.pdf](https://www.nist.gov/system/files/documents/2021/06/07/idqt_testplan_draft_v7_6.pdf).
- 119 Adam Czajka and Kevin W. Bowyer. (June 13, 2018). *arXiv*. “Presentation Attack Detection for Iris Recognition: An Assessment of the State of the Art.” Accessed on Sept. 23, 2022, at <https://arxiv.org/pdf/1804.00194.pdf>.
- 120 Craig Trudell. (Feb. 7, 2022). *Bloomberg*. “Tesla Subpoenaed by SEC About Complying With Musk Settlement”. Accessed on Oct. 13, 2022 at <https://www.bloomberg.com/news/articles/2022-02-07/tesla-subpoenaed-by-sec-about-take-private-settlement-compliance#xj4y7vzkg>.
- 121 Fred Vogelstein. (Feb. 9, 2019). *Wired*. “How WIRED Covered Facebook These Past 15 Years.” Accessed on Oct. 13, 2022 at [https://media.wired.com/photos/5c54e3eca9851f2c3080460f/master/pass/FB-Oct2007-wi200710\\_101\\_pdf.jpg](https://media.wired.com/photos/5c54e3eca9851f2c3080460f/master/pass/FB-Oct2007-wi200710_101_pdf.jpg).



## TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

[www.trendmicro.com](http://www.trendmicro.com)

