3.
PROFESSOR: That sounds like a good choice. Anyone else? Hassan?
HASSAN: My defining moment was a little different. It was when I made the swim team earlier this year.

4.
PROFESSOR: Great that you attained your goal. That is a good example of how our achievements can lead to a new identity. All right. Was anyone influenced by other students? Yes, Sonya?
SONYA: Well, I definitely was influenced by my friends in my study group …

Listening 2 Beyond the ID card

Beyond the ID card

Good morning everybody. Today I'm going to be talking about methods used for identifying people. Every day there are situations in which we have to identify who we are. Not that long ago, a photo ID was sufficient for most purposes. But nowadays, we live in a world full of technology where there are issues with identity theft and the need to confirm our identity in other ways.

Thus, there is now a need to move beyond the basic information on our photo IDs. For example, we have user IDs and passwords to use with our computers. It's also becoming more common for us to be identified using biometric information. Biometrics is the process where a unique physical feature of a person – for example, someone's face or voice – is recorded electronically and used to confirm the person's identity.

All right. So first, I plan to briefly look at photo IDs and passwords. Then, I'll talk in more detail about why using biometrics is a more reliable way to identify someone.

So, now let's focus on photo IDs; for instance, a passport or a driver's license. These may vary a bit from country to country as to what personal information they include, but in general, these IDs typically include a person's photo, name, nationality, gender (male or female), and an identification number. It may also include the hair color, eye color, and height of the person. An advantage of a photo ID is someone can look at the photo and quickly check who you are. A disadvantage is it can be lost or stolen and photos can be altered.

OK, so what about passwords, user IDs and PINs – personal identification numbers? Well, while these are excellent ways to protect our bank accounts, computers and social media profiles, this information could be stolen and used by somebody else. There's no way to guarantee that the person entering the password or PIN is the real owner of the account, and as such, these are not reliable ways to establish identity.

Now, let's turn our attention to biometrics. I want to look at how biometric information is used to identify someone. The oldest way is by taking a person's fingerprint. You are all probably familiar with this. Do you know why each fingerprint is unique? It's because the skin on each of our fingers has a unique pattern. Although the skin on our fingers is flexible, a fingerprint is one reliable way to identify someone. This is especially true nowadays when 3D scanners are used.

The second biometric form of identification I want to mention uses voice. Each person's voice has a unique combination of features, such as pitch and rhythm. This makes it possible for a recording of a person's voice to be used to confirm identity. To make a voice ID, the user records themselves saying a short sentence. Later, when they want to access the account or, whatever's protected by the voice ID, they repeat the sentence. If the pitch and rhythm of the two sentences match, the person's identity can usually be established. This is useful in situations where the person cannot be seen; for example, on the telephone. Voice recognition is generally considered a reliable way to identify someone. Of course, voice recognition software isn't 100% accurate, so it cannot always be relied on for all situations.

Next, let's consider how DNA testing is used to identify people. All people share over 99% of the same DNA information. However, there is a very small amount of DNA information that varies from one person to another. The small amount is used in DNA testing. Let me explain. Let's say, the police submit two samples of hair to a DNA crime lab. The lab extracts the DNA from one sample of hair and compares it to the DNA they extract from another sample to see how closely the two samples match. The lab looks for the probability the two samples are from the same person. However, they can't say with absolute certainty that two DNA samples are from the same person, and for this reason, DNA testing is not 100% reliable as a type of identification.

Let's move on to the last type of biometrics I want to cover: it's iris recognition. The iris is the colored part of your eye. To create an iris ID, a person's iris is scanned. The scan creates an image of the pattern in the iris. Because the iris pattern in each eye is unique, the patterns can be used to confirm our identity.

Compared to other types of biometrics, iris recognition is especially good for identification. There are a couple of reasons for this. First, because the iris is inside the eye and well-protected from damage, it doesn't change over time. Second, because the iris is mostly flat, it is easy to create a very accurate video image of it. As a result, iris recognition is one of the most reliable biometric forms of ID we have. For this reason, iris recognition is often used in automated border crossing between some countries and in buildings where security is important.

As technology develops, there will continue to be new biometric ways to identify people. Given that biometrics is based on our unique physical features, this makes it the most reliable way to identify people.

Words and expressions

identity theft 身份窃取
biometrics *n.* 生物测量学，生物识别技术
pitch *n.* 音高
rhythm *n.* 节奏
submit *v.* 提交
extract *v.* 提取，提炼