President: Regina Jarillo Romo

Moderators: Carolina González Suástegui & Alejandra Domínguez Morales

Conference Officer: Jesus Peng

TOPIC B. The controversy arising from the collection of biometrics

I. Introduction

While historically the use of biometrics was only reserved for military and law enforcement purposes, nowadays, the implementation of biometrics has become so widespread that almost every government or other legal entity uses it in a manner or other to identify their people of interest. One of the main reasons behind the recent boost in popularity of biometric identification is thanks to the inherent accuracy these have over traditional means of proving one's identity. It's estimated that the probability of finding a duplicate fingerprint is one in 64 billion. On top of that, unlike passwords or documents, biometric data has the advantage of not being stolen, forged, forgotten and lost.[1]

Aside from applications in public security and citizen registration, the use of biometrics has potential benefits across a wide variety of sectors. First of all, border control and migration have started using passports (biometric passports) with the hopes of increasing security and maintaining efficiency as can be seen with the United States' IDENT biometric system or the European Union's EURODAC.

Additionally, biometrics have also found their way inside physical access control systems that ranges from a personal device using fingerprint sensors to facilities that hold sensitive information and material. Finally, biometrics also potential commercial applications as evidenced by the increase in the use of Know Your Customer processes (KYC) in business establishments. Here,

[1] US government hack stole fingerprints of 5.6 million federal employees. The Guardian. United States, 14/07/2014. In: https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints (05/02/2020).

retailers build up a facial recognition database that can identify premium customers and customers that have committed shoplifted before in an attempt to combat financial crime.

Nonetheless, the widespread use of biometrics has also had its fair share of opposition. Amongst the biggest elements of concern are function creep and personal privacy. Being biometric data as sensitive as they are due to their inherent characteristics, having that information mishandled can incur many severe consequences such as identity theft.

Additionally, as most biometric data is stored in a server, it is vulnerable to hacking as seen with the 2015 case where a server containing 5.6 million US government employees' fingerprints was compromised in a digital attack.[2] On the other hand, given that the information gathered by biometrics cannot be changed and can be used to identify a person for that person's lifetime, its risks of violating personal privacy when implemented without a strong legal and ethical framework can effectively violate that person's human rights.

II. Concept definition

- *Biometric:* the biological measurements that allow for a person to be identified using unique characteristics such as fingerprint maps, retina scans, facial recognition, and gene sequencing.
- *Morphological measures:* forms of biometrics that consists of fingerprints, vein pattern, iris, and retina scans and face structure.
- *Biological measures:* forms of biometrics that consist of DNA sequencing
- *Behavioral measurements:* forms of biometrics that consist of voice recognition, signature dynamics, gait, gestures, footsteps, etc.

[2] US government hack stole fingerprints of 5.6 million federal employees. The Guardian. United Sates, 14/07/2014. In: https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints (05/02/2020).

- *Function creep:* When technology or system is used for purposes beyond its original purpose.

III. Current problematic

"We are currently witnessing a rapid rise in biometric security. Borders are apparently becoming 'smart'; passports are becoming e-passports, and when you set out on your travels your data double is already at your destination. Access to airports and even continents will increasingly be determined not by your national citizenship but by the security of your identity".[3] In an era where almost everything is digitized, as regular users of the internet, we become more vulnerable as every single detail is uploaded and hug upon a visible curtain that can be rolled over by anyone with a computer and access to Wi-Fi. An airport is just an example.

"In a world of identity politics and risk management, surveillance is turning decisively to the body as a document for identification, and as a source of prediction". [4] Biometrics can encompass physical and physiological characteristics among fingerprints, facial recognition, iris recognition, hand geometry, retina recognition, and vascular recognition. Meanwhile, the behavior and personality characteristics include signature, handwriting, speech, and keyboard write recognition, as well as recognition in the way of walking. Assigning each individual its own unique print to be recognized with, and more lately, to be hacked and threatened by.

Nowadays the current problem on data-based storage of this important and intrinsically personal information is that it can easily be stolen and damage not only a single person but complete companies. A work from the Institute of Electrical and Electronics Engineers, called Biometrics-based cryptographic key generator establishes a possible resolution to the problems presented by the

[3] The birth of biometric security. Anthropology Today. 02/04/2020. In: http://mural.maynoothuniversity.ie/3014/1/The_Birth_of_Biometric_Security.pdf (05/02/2020).

[4] Neil Gerlach, Sheryl N. Hamilton, Rebecca Sullivan, Priscilla L. Walton. Becoming Bio subjects. University of Toronto Press, Canada, Toronto, 2011.

taking of biometrics worldwide, with the aim of optimizing this process in the most effective and efficient way; "Instead of using PINs and passwords as cryptographic keys that are either easy to forget or vulnerable to dictionary attacks, easy-to-carry and difficult-to-transfer keys can be generated based on user-specific biometric information. A framework is proposed to generate stable cryptographic keys from biometric data that is unstable in nature".[5]

The IPC (Information and Privacy Commissioner) of Ontario, Canada; believes that if left unregulated, this technology could be used in ways that could compromise informational privacy. But it also finds itself in a neutral position, as they assure that if properly designed and regulated, this technology could actually be a means to enhance privacy. In this way, the take of biometrics doesn't seem aggressively accusatory and day to day users don't appear to be vulnerable at all. But what happens when the usage and management of this personal information aren't "properly designed and regulated"?

"Damage due to theft or misuse is potentially irreversible since the biometric data of an individual cannot be changed and once compromised, it would not be safe to use it again".[6] When talking about the *irreversible* effects incurred by misuse of biometric data, discrimination and public spread of your personal information are relatively lighter.

The problems could be spread to other fields that aren't financially straight forward-focused, as to the medical area, where patients' information has to be delicately treated and well-kept for the patient's health insurance at all times. Besides the fact that hospitals and clinics have not only to offer privacy but to make sure their clients, in this case, patients are protected to share their medical history to their doctor and the whole institute or center. "Contrary to classical recording methods of patient's medical data, which are,

[5] Biometrics-based cryptographic key generation. IEEE. 22/02/2005. In: https://ieeexplore.ieee.org/abstract/document/1394707?section=abstract (06/02/2020).
[6] The working party on the protection of individuals with regard to the processing of personal data. European Commission. Belgium, 27/04/2012. In: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (05/02/2020).

based on paper documents, nowadays all this sensitive data can be managed and forwarded through digital systems. These make it possible for both patients and healthcare workers to access medical data or receive remote medical treatment using wireless interfaces whenever and wherever. However, simplifying access to these sensitive and private data can directly put a patient's health and life in danger", points out the Institute of Electrical and Electronics Engineers.[7]

"Biometric technology is rapidly becoming a part of our everyday lives. With the advancement in Information technology, there has been an increase in threats to the system and its assets and therefore there has been a need to improve the security measures. The need for more and more reliable user authentication techniques has increased concerns about security and rapid advancements in networking, communication, and mobility these days. Biometrics is one such authentication method that helps verify the users of the system. Biometric technologies are becoming the foundation of highly secure identification and personal verification solutions. To ensure the integrity and confidentiality of its system it is necessary for every organization to have a good Security Policy. Security policy is an important factor to help secure the system, but by itself, it will not help secure an information system".[8]

IV. International initiatives

The United Nations Organization (UN), in 1948, it adopts the document known as the Universal Declaration of Human Rights, in which article 12 states that people have the right to the protection of the law of their personal data. With the wide acceptance of biometrics to verify identity, especially in an open network environment, the challenges posed by the privacy, reliability, and security of biometric data are increasingly complicated and demanding.

[7] Electronic health records: Is it a risk worth taking in healthcare delivery? GMS Health Technology Assessment. 10/12/2015. In: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4677576/ (06/02/2020).

[8] Biometrics and information security. Research Gate. 2008. In: https://www.researchgate.net/publication/240319488_Biometrics_and_information_security (06/02/2020).

At the present time, the International Organization for Standardization (ISO), the International Electro-technical Commission (IEC), and the ITU Telecommunication Standardization Sector (ITU – T) are the ones in charge of creating and developing the policies and norms for biometric security all around the globe. Industrial consortiums also create standards that support the objectives of their members, while specialized agencies of the United Nations, such as the International Civil Aviation Organization (ICAO) and the International Labor Organization (ILO) write and draw up more specific rules to be followed.[9]

Since the establishment of its Subcommittee 37 on Biometrics, in June 2002, the Joint Technical Committee (JTC 1) of the ISO / IEC has developed more than 30 international standards on biometrics. JTC 1's work related to biometrics standards is also carried out by its Subcommittee 27 on IT Security Techniques (covering template protection, algorithm security, and security assessment), and its Subcommittee 17 on Cards and Personal Identification.[10]

Within ITU – T, work on biometrics began in 2001 under the responsibility of ITU-T Study Group 17, which coordinates these activities throughout all its Working Groups. In particular, the said Commission is responsible for the study of identity management; that is, the appropriate technical methods to identify individuals and protect their identities. Work is being intensified to address the new challenge of achieving a safer infrastructure, services, and network applications. Obviously, telecommunications applications that use mobile terminals and Internet services require authentication methods that not only provide a high degree of security but are convenient for users. To date, more than 70 ITU – T Safety Recommendations have been published.[11]

[9] A practical guide to biometric security technology. IT Professional. 01/01/2001. In: https://cedar.buffalo.edu/~govind/CSE717/papers/PracticalGuide.pdf (06/02/2020).

[10] Biometría y normas. Actualidades de la UIT. 2010. In: https://www.itu.int/net/itunews/issues/2010/01/05-es.aspx (06/02/2020).

[11] *Ibid.*

Privacy-Enhancing Technologies (PET) are the technical answer to social and legal privacy requirements. PET becomes constituents for tools to manage users' personal data. Users can thereby control their individual digital identity, i.e. their individual partial identities in an online world. Existing commercially available identity management systems (IMS) do not yet provide privacy-enhancing functionality.[12]

The Organization for Economic Co-operation and Development's 2004 report on biometrics focused on security and privacy issues, covering three areas of privacy: functional change, monitoring risk, consent and transparency. The most in-depth discussion of biometric privacy issues was the 2006 National Science and Technology Council report Privacy and Biometrics.

Since 2007, several international conferences on ethics, law or policy related to the application of biometric technology have been held with the launch of the RISE (Rising pan-European and International Awareness on Biometrics and Security Ethics) project (2009-2012) funded by the European Commission's Seventh Framework Programme. RISE is a 36-month EU funded project which aims at setting up an international initiative to monitor ethical and policy issues raised by biometrics and security technologies. RISE aims to deepen, extend to Asian actors and ensure the continuity of European and international dialogue already initiated by the two linked projects BITE and HIDE, and by the two previous conferences on ethics and biometrics organized by the EC Research Directorate General and the US Directorate of Homeland Security Privacy Office respectively in 2005 and 2006.[13]

The European Biometrics Technology Forum was established in Dublin, Ireland. The academic papers of authoritative journals were published continuously, and the discussion of ethical issues was more in-depth, including some important ethical issues.

[12] Privacy-enhancing identity management. Science Direct. No uodate date. In: https://www.sciencedirect.com/science/article/pii/S1363412704000147 (06/02/2020).
[13] Ethical Issues in Biometrics. United States. 2011. In: http://www.capurro.de/biometrics.html (06/02/2020).

V. Guidance questions

1. What types of biometric identification are most widely used and which ones have the potential of representing the greatest threat to citizens?
2. Under which circumstances should the use of biometrics, along with the data gathered by such means, be ethically accepted or rejected?
3. How does the current international legislation fare against the misuse of data collected from biometrics?
4. How can the framework revolving the gathering of personal information by biometrics be strengthened protect the parties involved in a safely manner?

VI. Bibliography

1. A practical guide to biometric security technology. IT Professional. 01/01/2001. In: https://cedar.buffalo.edu/~govind/CSE717/papers/PracticalGuide.pdf (06/02/2020).
2. Biometrics-based cryptographic key generation. IEEE. 22/02/2005. In: https://ieeexplore.ieee.org/abstract/document/1394707?section=abstract (06/02/2020).
3. Biometrics. Information and Privacy Commissioner of Ontario. No update date. In: https://www.ipc.on.ca/privacy-organizations/data-and-technology-management/biometrics/ (06/02/2020).
4. Benefits of Biometric Authentication in Information Security. USA, New York. No update date. In: http://www.m2sys.com/blog/information-security/benefits-biometric-authentication-information-security/ (06/02/2020).

5. Biometría y normas. Actualidades de la UIT. 2010. In: https://www.itu.int/net/itunews/issues/2010/01/05-es.aspx (06/02/2020).
6. Ethical Issues in Biometrics. United States. 2011. In: http://www.capurro.de/biometrics.html (06/02/2020).
7. Electronic health records: Is it a risk worth taking in healthcare delivery? GMS Health Technology Assessment. 10/12/2015. In: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4677576/ (06/02/2020).
8. Neil Gerlach, Sheryl N. Hamilton, Rebecca Sullivan, Priscilla L. Walton. Becoming Bio subjects. University of Toronto Press, Canada, Toronto, 2011.
9. Privacy-enhancing identity management. Science Direct. No update date. In: https://www.sciencedirect.com/science/article/pii/S1363412704000147 (06/02/2020).
10. ¿Qué y cuáles son los datos biométricos? The Economist. Mexico, 29/05/2018. In: https://www.eleconomista.com.mx/tecnologia/Que-y-cuales-son-los-datos-biometricos-20180529-0068.html (06/02/2020).
11. Secure and lightweight biometric-based remote patient authentication scheme for home healthcare systems. Research Gate. 2018. In: https://www.researchgate.net/publication/324943618_Secure_and_lightweight_biometric-based_remote_patient_authentication_scheme_for_home_healthcare_systems (06/02/2020).
12. The birth of biometric security. Anthropology Today. 27/03/2019. In: https://rai.onlinelibrary.wiley.com/doi/pdf/10.1111/j.1467-8322.2009.00654.x (06/02/2020).

13. The working party on the protection of individuals with regard to the processing of personal data. European Commission. Belgium, 27/04/2012. In: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf (05/02/2020).
14. US government hack stole fingerprints of 5.6 million federal employees. The Guardian. United States, 14/07/2014. In: https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints (05/02/2020).