WEDF Student Initiative Submission

Data Privacy: A Case Study of Mexican Telephony Legislation

Balerdi, Kenzo* & Coppellotti, Nicolás**
**BSc in Computer Science, Slippery Rock University*[1]
***Masters in Economics and Public Policy, Universidad Adolfo Ibáñez*[2]

1. Introduction

Privacy has concerned human beings all along their history. We consider this right as being essential to protect our personal autonomy and deny interference from third parties which might be harmful towards how we choose to live our life. Data privacy has gained relevance in the last few decades amidst scandals such as Cambridge Analytica's involvement in the 2016 US election and the 2016 UK referendum, through the purchase, processing, and commercialization of personal data of voters obtained through Facebook.

In the following paper we will elucidate the current situation regarding data privacy. This will be done through a general outlook on the matter followed by the analysis of a new legislation that has been passed in the lower chamber of mexican congress regarding biometric data collection through cell phones to try to lower criminal activity.

2. Data Privacy: General Outlook

Although general privacy laws date back to the end of the 19th century with the publication of the article "The Right to Privacy" by attorneys Samuel Warren and Louis Brandeis, the origins of data privacy as we know it today can be traced back to 1970s Europe. Beginning with Germany, then Sweden and other european countries, a series of national laws regarding data privacy were developed due to several computing advancements.1 These laws have been held under scrutiny and improved through the years as new technologies come into play, with

[1] Pennsylvania, United States
[2] Santiago, Chile

the General Data Protection Regulation (GDPR) being the most recent one. The primary aim of the GDPR is to give control of personal data to their users and simplify current laws by unifying regulations within EU countries.

The EU has been the trendsetter regarding data protection laws, with other countries following suit in different ways. The United States for example has lagged because there is no unifying legislation across all states, this is due to the federal structure of the country and each state having its own data protection laws to worry about. One case that is worth mentioning is the situation in New Zealand. Recently, political actors have put data protection in the agenda with a series of laws passed to protect users in this regard. A different story is the one of developing countries, these nations have yet to reach the standards of the EU or New Zealand, mainly because they have other concerns, but they will have to start discussing these issues if they do not wish to have considerable problems in the future.2

The first question we must ask ourselves is ¿Why is data privacy relevant and why should we destine resources towards its development and implementation? In the era we live in, data is being collected, stored, and processed at a faster rate than ever before from a series of digital and technological sources.3 The fact that this data can be then used for purposes users are unaware of, makes it imperative for public organisms to make sure that this does not happen, and no harm is done to each individual. We should also take into consideration that there are certain age groups that are more vulnerable, particularly the case of children. They are unaware of all the risks that exist regarding the potential misuse of their personal information, therefore, we should take certain measures that protect children and other vulnerable groups.

When discussing data privacy, there seems to be a consensus on the principles data protection legislation should include. First and foremost, there must be transparency regarding data collection and usage, users need to know what, how and for what purposes information is being collected. Another important aspect of data privacy is control, users should be able to access said data and delete both the information collected and the source that is collecting it (website, software, etc) if they deem necessary. A third element of data privacy that is often overlooked is what some experts call notification, meaning that we should be informed about any issues regarding our information, be it loss, misuse, or any other violations that could compromise our privacy.4It is worth noting that data privacy should be present in all stages of data’s life cycle, starting from its collection and/or generation, going through the phase where it is processed, stored, and analysed, and finally up to the point when it is deleted or discarded (if this is the case).

Well known economist Richard Thaler developed a theory known as the Nudge with lawyer Cass Sunstein which could help us tackle the problem regarding data privacy.5 This theory states that you can influence people's decisions with a slight change in the way the decision is presented (choice architecture). A common example is the design of a cafeteria and the distribution of the food. If you wish for people to eat healthier, you should put salads closer to the customers and the other choices should be farther away. If we now apply this theory to the field of data privacy, what could be done is the following: whenever users are accessing for the first time a platform that will retrieve their data, the registration to said platform could be structured in such a way that each person knows exactly what they are getting into so they can make a fully informed decision whether they think it's best for them to enter that platform.

3. Mexico's Biometric Data Collection Problem

Concerned over alarmingly high kidnapping and extortion cases in their country, mexican lawmakers have devised a bill that intends to gather biometric data from all cellphone users in a bid to prevent criminals from getting access to anonymous mobile communication devices. According to a special report published by the University of San Diego's 'Justice in Mexico' program, the National Public Security System recorded an average of 73 kidnappings per month, with over 88% of them being kidnappings for ransom6. The bill is still being discussed in the senate.

Even though the initiative might seem like a step in the right direction in order to reduce kidnapping and extortion cases, the collection of biometric data at this scale raises many privacy concerns. This hearkens back to a similar program that was put in place in Mexico in 2009, which was terminated in 2012 due to the collected data being mishandled and later sold in the black market7.

3.1 Questionable Solution to a Real Problem

Before addressing any of the negative externalities that might come from keeping a registry of biometric data, it is important to assess whether this method will be effective in tackling the problem at hand. The main idea behind the bill is to prevent kidnappings and ransom situations by linking every cell phone number to a person, making it difficult for criminals to extort victims without giving away their identity.

However, there are many ways for criminals to go around these restrictions, making it unclear whether the program will help reduce this type of crime.

3.1.1 Phone ‘spoofing’

According to the American FCC, ‘Spoofing’ is when a caller deliberately falsifies the information transmitted to a caller ID display to disguise their identity8.

Due to the myriad of VoIP software solutions on the market, it is easy for a person to anonymously get a number, generate a number that matches the victim’s area codes (neighbor spoofing), or even hijack existing legitimate phone numbers.

A report that gathered data in the United States for over three years concluded that over 62% of high-risk calls were executed using VoIP software9, which in most cases make use of spoofing techniques.

3.1.2 Phone theft and criminal impersonation

People in Mexico have also expressed their concern about how these measures might increase occurrences of phone theft, which were already at an average of 60 a day in 2018 in Mexico City alone10. With phone theft being that common, it is not far fetched to imagine organized criminals

stealing phones for the sole purpose of calling extortion victims, and in the process incriminating the original owner of the phone.

3.1.3 Alternative modes of communication

Another clear oversight by the proposed bill is the fact that mobile telephony is already being replaced by other means of communication11, be it by VoIP technologies or increasingly by messaging apps that only require a wireless connection, with no identification necessary for usage. These applications, paired with VPN technologies would make it nearly impossible to reliably track a criminal engaging in extortion practices.

3.2 Privacy Concerns

Even if the registry could theoretically help reduce crime, the potential dangers associated with collecting such data should not be ignored. Unauthorized access to an individual’s information endangers their privacy, freedom and safety, be it by criminals, bad actors or even authoritarian regimes.

3.2.1 Pitfalls of collecting biometric data

Currently only 8% of countries with analogous registries also require biometric data to be collected12, among them are China, Saudi Arabia and Pakistan, all of them with questionable records of human rights violations.

In China for instance there have been cases of embezzlement and identity theft related to facial recognition data being used in tandem with face-swapping AI systems13. The government itself has also used facial recognition CCTV systems to keep track of its citizens and their activities. By western standards, this behavior could be seen as infringing on an individual’s right to privacy.

3.2.2 Data security and leaks

As mentioned before, the Mexican government used to have a similar registry put in place in 2009 (RENAUT) which was terminated in 2012 due to the data being sold in the black market2. This is far from an isolated occurrence, with China having a very similar issue with its biometric databases, where people could buy a package of 1000 citizen identification pictures for about 30 cents (US$)13.

Even though the world of Cybersecurity has evolved rapidly, there is no such thing as a perfectly secure system. Even if the Mexican government were to implement a state-of-the-art system with the safest standards in the industry, the fact remains that Cybersecurity is a never ending arms race between security measures and vulnerability exploitation. There will always be a window of opportunity, for a security breach to occur and for sensitive information to be stolen and sold without consent.

3.2.3 Potential misuse by authority

With many minority populations being persecuted and targeted by different states throughout the world, the collection of biometric data could aid efforts of repression or even genocide.

A recent example would be the persecution of Uighurs in China, where people are being sent to ‘internment camps’ against their will to undergo re-education programs. It has been alleged that these camps are nothing but forced labor camps, and that subjects are beaten, raped and tortured14. The use of biometric data for massive surveillance makes it easier for individuals to be captured and monitored after release.

With Mexico currently dealing with forced disappearances, extra-judicial killings and torture cases against the armed forces, the police and the justice system15, it would be a terrible candidate to be given a system akin to the Chinese.

4. Discussion

By current data protection standards, the Mexican biometric data collection program falls apart under heavy scrutiny. Even though there is transparency regarding the specific data being collected, the purpose and further use of the data is not clear. Users have no control over the data once collected, and there are no systems in place to notify them about the loss, misuse, or violations of their data.

Paired with the fact that the program promises to be ineffective towards solving the extortion/kidnapping problem, the privacy issues raised make it a ridiculous way to spend taxpayer money at best, and a glaring endangerment of citizens' privacy at worst.

The thing mexican authorities should ask themselves when discussing this new legislation is the following: ¿Is this solution really tackling the problem at hand or will it create new problems down the line?

5. References

[1] Solove, George. A Brief History of Information Privacy Law. George Washington University Press. 2006.

[2] Zwitter, Andrej. Big Data Ethics. Journal of Big Data & Society, pp. 1-6. 2014

[3] Jain, Priyank et. al. Big data privacy: a technological perspective and review. Journal of Big Data, pp. 3-25.

[4] Isaak, Jim & Hanna, Mina. User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. Computer Journal. Vol 51, No. 8. 2018.

[5] Thaler, Richard & Sunstein, Cass. Nudge: Improving Decisions About Health, Wealth and Happiness. Penguin Group. New York. 2008.

[6] McGinnis, Teagan, et al. 2020, Organized Crime and Violence in Mexico 2020 Special Report, justiceinmexico.org/wp-content/uploads/2020/07/OCVM-2020.pdf.

[7] Monroy, Jorge. "Concluyó Destrucción De Datos Del Renaut." El Economista, 19 Oct. 2017, www.eleconomista.com.mx/politica/Concluyo-destruccion-de-datos-del-Renaut-20130512-0087. html.

[8] Caller ID Spoofing. Federal Communications Commission, 23 Sept. 2020, www.fcc.gov/consumers/guides/spoofing-and-caller-id.

[9] Transaction Network Services, 2019 Robocall Investigation Report, March 2019 ecfsapi.fcc.gov/file/10515248878426/Transaction%20Network%20Services%20-2019%20Roboc all%20Investigation%20Report.pdf.

[10] Se Roban 60 Celulares Al Día En La CDMX. El Financiero, 2 July 2019, www.elfinanciero.com.mx/nacional/se-roban-60-celulares-al-dia-en-la-cdmx.

[11] Samadder, Rhik. “End of the Line: Our Guide to the Death of the Telephone.” The Guardian, Guardian News and Media, 24 June 2018, www.theguardian.com/global/2018/jun/24/landline-mobile-guide-death-telephone.

[12] Garrison, Cassandra. “Kidnap Capital Mexico Eyes Biometric Phone Registry, Sparking Privacy Fears.” Reuters, Thomson Reuters, 16 Feb. 2021, www.reuters.com/article/us-mexico-telecoms-focus/kidnap-capital-mexico-eyes-biometric-phone -registry-sparking-privacy-fears-idUSKBN2AG1AK.

[13] Chen, Wu. “Biometric Risk: Why China Should Say No To ‘Face Swiping.’” Worldcrunch, 20 Nov. 2020, worldcrunch.com/opinion-analysis/biometric-risk-why-china-should-say-no-to-face-swiping.

[14] “Who Are the Uighurs and Why Is the US Accusing China of Genocide?” BBC News, BBC, 9 Feb. 2021, www.bbc.com/news/world-asia-china-22278037.

[15] Roth, Kenneth. “World Report 2020: Rights Trends in Mexico.” Human Rights Watch, 14 Jan. 2020, www.hrw.org/world-report/2020/country-chapters/mexico.