**Requirements Misuse and Abuse Cases**

**Student**: Patrick Walsh

**Date**: 4/5/2021

**School**: University of Maryland Global Campus

**Course**: SDEV 360 7380

**Professor**: Dr. Alla Webb

**ATM abuse/misuse**

One common attack on Automatic Teller Machines (ATM) is when criminals capture card information when a customer inserts their card into the ATM (Positive Technologies, 2018). The type of information captured includes the debit card number, expiration date, and the cardholder’s name. This type of attack takes place at the Session level as described in the Use Cases for Example ATM System (Bjork, n.d.). At the Session level, a user inserts their ATM or debit card into the card reader slot of the ATM and enters a PIN to gain access to their account (Bjork, n.d.). Once the user accesses their account, they can then make various transactions such as making a deposit, withdrawal, checking account balance, or transferring funds (Bjork, n.d.). This is where attackers can intercept card information to gain access to the user’s accounts. This can be done either by gaining physical access to the ATM and installing a malicious card reading device (often called a ‘skimmer’) or by gaining access to the network to which the ATM is connected (Positive Technologies, 2018). The sensitive card information is encoded onto the magnetic strip on the back of most debit cards, and this magnetic strip is what the ATM card reader scans in order to retrieve the user’s account information such as their name and card number. This same information can be stolen from malicious card readers to create duplicate cards or to sell the card information on the dark web (Positive Technologies, 2018). In fact, it is estimated that stolen card information accounts for around 25% of all items sold on the dark web (Positive Technologies, 2018). In some cases, a camera is used to record when the user enters their PIN (Siciliano, 2020).

In the second scenario where an attacker gains network access to steal card information, the attacker uses a network traffic sniffer to watch all transactions between the card reader and ATM operating system or between the ATM and the remote processing center (Positive Technologies, 2018). The difficult part for an attacker in this scenario is gaining access to the network. Once they have gained access to the network, it is relatively easy to watch the network traffic because it is almost always unencrypted (Positive Technologies, 2018). With a network sniffer such as Wireshark, the attacker can easily see all the transactions in plain, unencrypted cleartext.

**Mitigations**

To guard against these types of attacks, the network traffic between the ATM card reader and processing center should be encrypted to prevent attackers from reading the transaction information in plain cleartext (Positive Technologies, 2018). To prevent cameras from recording a user entering their PIN, the user should cover the keypad with their hand when entering their PIN (Siciliano, 2020). Additionally, users should take care to watch for signs of tampering with ATMs in case the card readers have been compromised and ‘skimmers’ have been installed (Siciliano, 2020).

**PII research**

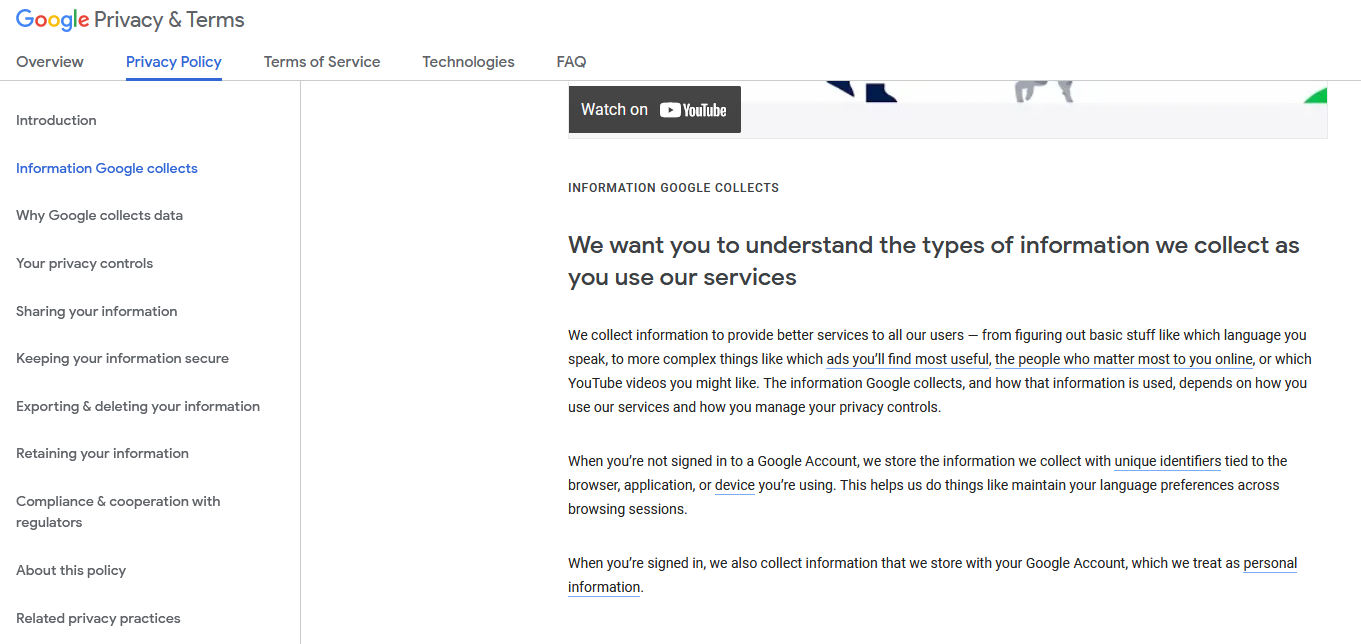
Organizations gather Personally Identifiable Information (PII) on an ongoing basis for a variety of reasons. Whether in the context of businesses gathering PII on their customers for marketing purposes, law enforcement agencies or intelligence agencies gathering PII on persons of interest, the collection and protection of PII is an important topic to understand, both for the collectors of PII and those being collected on. The National Institute of Standards and Technology (NIST) describes (2010) PII as “any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information” (p. 7). While this is a broadly defined definition of PII encompassing multiple kinds of data, it is important to note that some information in isolation may not be considered PII until aggregated to form a more comprehensive image of an individual. For example, zip code alone may not be considered PII since that piece of information by itself is not enough to identify an individual, but zip code plus street address possibly would be enough. NIST also names (2010) passport number, driver’s license number, bank account or credit card numbers, email addresses, and photographic images as other forms of PII.

The question of when companies go too far in collecting PII is difficult to answer because people draw the line of what they consider to be reasonable at different places. Social media giants like Facebook and Twitter, for example, have often come under scrutiny from both government and the public at large for their massive data mining of users’ personal data. Facebook in particular was recently fined an historic $5 billion by the U.S. Federal Trade Commission (FTC) for failing to protect users’ PII (Baig & Snider, 2019). This fine came as a conclusion of the investigation into the 2018 Cambridge Analytica scandal where Facebook was accused of selling the personal information of 50 million of its users which was used to create targeted ads during the 2016 U.S. presidential election (Baig & Snider, 2019). As part of the settlement, Facebook was forced to pay a separate $100 million fine in response to data misuse charges by the U.S. Securities and Exchange Commission (SEC). While this Facebook settlement was unprecedented in its scale, it is not an unusual occurrence. Just two years prior to the Facebook settlement, Upromise was forced to pay $500 thousand in fines for data privacy violations, and Google was forced to pay $22.5 million in fines in 2012 (Baig & Snider, 2019). Additionally, credit-reporting company Equifax was fined $575-700 million after a massive data breach was discovered and Equifax was accused of failing to properly safeguard its customers’ PII (Baig & Snider, 2019).

When a user signs up to use Google services like Gmail or YouTube, that user must sign Google’s Privacy Policy which explains what PII Google collects, how it is collected, what the PII will be used for, and how long Google will retain the PII (Google, 2021).

**Figure 1**

*Screenshot of Google’s Privacy Policy*



*Note.* Google’s Privacy Policy is open for anyone to read online. Link is available on the References page.

According to Google’s Privacy Policy, the company collects which language the user speaks, people the user contacts most frequently, metadata about the device and applications the user is on (Google, 2021). Additionally, Google tracks which videos the user watches, the user’s voice recording, search terms, browser history, purchasing activities, datetime stamps of messages, sender and recipient’s phone number or email address, IP addresses, and duration of calls, just to name a few (Google, 2021). Unfortunately, there is very little a user can do to mitigate this collection of PII as long as they choose to use Google products. The best steps a person can make if they are concerned about protecting their online privacy is to use services who are less intrusive than Google and Facebook. As the vendor, a company like Google could alleviate their need to conduct such massive data mining of PII if they were to radically change their business model. For example, Google could offer a paid version of Gmail that does not collect the user’s PII and instead relied on a monthly or annual subscription fee to fund services rather than offering “free” services in exchange for the monetization of the user’s data. Such is the case with data privacy-centric email services like ProtonMail and Malifence (Taylor, 2021).

Ultimately, each individual will have to decide how much PII they are comfortable handing over to technology companies and if the trade-off of less privacy for convenience is worth it. In the end I believe that we, as a society will continue to move the goal post as to what is considered reasonable privacy, since we are continually living in a less private world.

**References**

Baig, E. C., & Snider, M. (2019, July 24). *Facebook fined $5 billion by FTC, must update and adopt new privacy, security measures*. USA TODAY. https://eu.usatoday.com/story/tech/news/2019/07/24/facebook-pay-record-5-billion-fine-u-s-privacy-violations/1812499001/

Bjork, R. C. (n.d.). *Use Cases for Example ATM System*. Gordon College. http://www.math-cs.gordon.edu/courses/cs211/ATMExample/UseCases.html

Google. (2021, February 4). *Google Privacy Policy*. Google Privacy & Terms. https://policies.google.com/privacy?hl=en-US#infocollect

Positive Technologies. (2018, November 14). *ATM logic attacks: scenarios, 2018*. Positive Technologies Security. https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/

Siciliano, R. (2020, August 9). *Here’s What You Need to Know to Protect Yourself From ATM Skimming*. The Balance. https://www.thebalance.com/what-is-atm-skimming-1947475

Taylor, S. (2021, January 11). *12 Best Private & Secure Email Services*. Restore Privacy. https://restoreprivacy.com/email/secure/