

Original Article

# Ethics, Privacy, and Security: Analyzing Data Breaches and their Impact

Manan Buddhadev

Department of Computer Science, Rochester Institute of Technology, New York, USA.

Received Date: 18 January 2025

Revised Date: 25 February 2025

Accepted Date: 21 April 2025

**Abstract:** Privacy has been a fundamental concern for humanity since early civilization, and the rapid increase in information sharing has only intensified this issue. Social media has become a primary medium for communication and connection worldwide. Notably, a January 2018 report from Facebook stated that the platform had over 2.2 billion active monthly users [1], illustrating the vast number of people who share personal information online.

*This paper examines data privacy breaches and the ethical policies designed to protect data privacy. Additionally, it presents a cause-and-effect model analyzing significant data privacy breaches from the past.*

**Keywords:** Ethics, AI, Privacy, Data Governance, Data Science, Data Engineering, Data Breaches.

## I. INTRODUCTION

While ethics may not be legally binding, they should always be upheld in any work. Ethics are in every walk of life, and when something is unethical, most of the time, it is immoral as well. Furthermore, ethics are the building blocks of any research project or item, and the researcher should not cross a moral line for his/her project's success. In this paper, we will be looking at ethics from the point of view of data science and data privacy. However, to know whether something is ethical or not, we needed to know the definition of ethics in data privacy, and hence, we looked at multiple papers that discuss the topic of ethics.

The Association for Computing Machinery (ACM) has outlined a set of ethical standards for all computing professionals, as detailed in [2]. This document highlights the ethical principles that computing professionals should uphold, the responsibilities expected of them, the actions that computing leaders should take, and guidelines on how to adhere to the code of ethics.

The ethical principles outlined in [2] state that computing professionals should strive to improve lives by creating applications and software that simplify daily tasks. Additionally, these principles emphasize that computing professionals must respect individuals from all walks of life and refrain from any form of discrimination [2].

One principle highlights that regardless of their actions, the computing profession also should avoid causing harm to individuals, groups, or communities. If harm is possible or has already occurred, it should be mitigated or eliminated [2]. This principle also underscores the importance of careful data collection and aggregation, emphasizing that professionals should be mindful of how data is stored and used [2]. Another principle stresses the need for honesty in professional practices, stating that individuals and companies should be transparent about their actions and intentions while avoiding misrepresentation [2]. The fourth principle reiterates the importance of non-discrimination, asserting that computing professionals and companies should not discriminate based on caste, creed, sex, age, nationality, religion, color, or similar factors [2].

Furthermore, there is a principle that acknowledges the efforts researchers put into developing new ideas and technologies. Therefore, professionals should give due credit to researchers and follow ethical methods to prevent plagiarism [2]. The sixth principle is crucial for data privacy, stating that, given the ease of data collection, it is the responsibility of computing professionals to use data appropriately [2]. It emphasizes that private data should only be utilized when necessary and encrypted to protect users' privacy [2].

Finally, the last ethical principle ties together the first, second, and sixth principles, asserting that customer confidentiality must be preserved before conducting any data analytics [2]. It also specifies that data should not be disclosed unless it pertains to national security, illegal activity, or violations of the Code [2]. [2] also provides guidelines for the responsibilities of a computing professional, where the first guideline states that the computing professional should always give his/her 100% and provide the best quality of work and the process of performing the work. The following guide line is a follow-up to the first one, and it



mentions that computing professionals should maintain a high standard of knowledge, capability, and ethics that they follow [2]. The next guideline is to know the rules of work and to comply with them [2] and also, another guideline states that the professionals should be open to feedback as well as provide feedback to people they work with [2]. The following guideline states that the people working on a particular system or part of the software should evaluate the systems correctly and ensure they analyze the potential threats and security risks[2]. The guideline states that professionals assigned to a particular area should be well acquainted with that area of computing[2]. The following guideline states that the computing professional should familiarize customers with various technologies and create public awareness about important matters about computing[2]. The penultimate guideline states that the computing professional should only access the information they are authorized to [2]. The last and final guideline states that the software should be made in a way that can be used across multiple systems, and they should make sure that the applications are secure[2].

The paper [3] states that usually, there is a fine line between ethics and law, wherein if it is not clearly understood, it can harm people's privacy a lot. The paper gives an example of ethical hacking wherein a hacker breaks into a system to reveal loopholes in the security and, thus, compromise the privacy of the people for the greater good. One of the examples in [4] is where an ethical hacker named Elliot Alderson broke into the Aadhar's system to prove that it is flawed and then tweeted that he is in favor of Aadhar but believes that the security of such a crucial system with such highly sensitive data should be stringent. The paper calls such ethical hackers "Robin Hood" [3]. Lastly, the paper mentions that such loopholes in the definition of law and ethics should exist to expose important details or leave some breathing room to make privacy a more manageable thing [3].

Lastly, [5] defines the term data privacy where it states that data privacy is where the user's data is collected or stored while keeping in mind what the legal rights of the users are [5]. The paper further states that data privacy also covers how to manage data breaches and the cost it entails [5]. The article also discusses how data privacy protection is critical and how it can be compromised [5]. The article reviews three different data protection policies:

#### **A. International Data Privacy Principals[5]**

IDPP has 13 principles [5] wherein three principles are related to compliance with legal policies, security policies, and access policies for employees to protect data from unauthorized access. There are six principles which are regarding how to handle customer data. One principle states that there should be a system in place that covers all data access with authorization control, another principle states that data breaches should be made known to users if they are related to sensitive data, and the last two principles are related to contracts between the customer and the companies, in cases contracts exist, or they do not what is to be done [5]

#### **B. Hong Kong Data Protection Principles of Personal Data [5]**

The Hong Kong Data Protection Principles of Personal Data has six principles. Where the first principle is related to data collection, the second principle is about how long the data is to be stored, the third principle defines how the data should be used; the fourth principle states security policy compliance, the fifth principle states that companies should disclose the data they are collecting or using along with the reason whereas the last principle says that the subjects should be allowed to view and modify their data at will [5]

#### **C. Hexa-decimal Code of Conduct [5]**

The hexadecimal code of conduct provides a flow of operations into three stages. The first stage identifies the type of data to collect, and the second stage gathers the necessary resources for smooth execution. It also mentions providing incentives to employees who have complied with the ethical policies, and the third stage is defining success metrics [5].

This paper looks at the new privacy protection law by the European government, the General Data Protection Regulation (GDPR), in section 2. We will review some of the most impactful data privacy and security breaches in section 3. Next, in section 4, we look at why most data or privacy breaches happen and map them to the articles for further reading. Lastly, in section 5, we will shed some light on prevention measures for the future and conclude the paper 6.

## **II. GENERAL DATA PROTECTION REGULATION (GDPR)**

### **A. What is GDPR and How to Comply with It?**

The European Union updated the General Data Protection Regulation (GDPR) to replace the previous European Data Protection Directive established in 1995 [6]. Thus, it has been roughly 13 years since someone addressed sensitive issues like data management and privacy. The GDPR applies to all the organizations affiliated with the EU from the 25th of March 2018 [7]. The penalty for non-compliance is pretty hefty, which is EUR 20 million or 4% of worldwide turnover, the highest of either [7][8].

The GDPR is built upon several key principles aimed at enhancing user privacy and standardizing data protection laws across industries. The core aspects include:

- a) Standardization of Data Protection Regulations [7].
- b) Consumer Rights [7]
  - Right to Access (Article 15) – Users can request access to their personal data [7].
  - Right to Erasure (Article 17) – Users can request that their data be deleted permanently [7].
  - Data Portability (Article 20) – Users can transfer their data across different service providers [7] [9].
  - User Consent (Article 7) – Organizations must obtain clear and explicit consent before processing user data [7] [9].
  - Parental Advisory & Child Data Protection (Article 8) – Additional protections for children’s data [7][9].
- c) Legal & Ethical Justifications for Data Processing [7].
- d) Enforcement of Compliance Measures [7].
- e) Incident Response & Breach Notification Procedures [7].

Rather than discussing these points individually, this paper will analyze GDPR’s overall impact and its role in ensuring data privacy. Notably, high-profile breaches, such as the Cambridge Analytica incident, have demonstrated the urgent need for strict data protection laws like GDPR. The regulation mandates that any company serving even a single EU citizen must comply with GDPR [7]. If a data breach affects an EU citizen, the responsible company faces significant fines and legal consequences [7].

GDPR also enforces privacy by design, ensuring that data security measures are embedded into systems from the outset (Article 25) [7]. Organizations must appoint a Data Protection Officer (DPO) to oversee compliance and ensure best practices in data protection [7]. Moreover, GDPR limits user profiling and targeted content placement, requiring companies to conduct risk assessments and, in high-risk cases, obtain approval from Data Protection Authorities (DPA) [7].

The regulation also streamlines incident response protocols in the event of a data breach. Under Article 33, organizations must notify the Supervisory Authority within 72 hours of discovering a breach. If the leaked data was unencrypted and poses a risk to users, the affected individuals must also be informed [7].

## **B. GDPR Implications and Effects**

- **Impact on Research:** GDPR has significantly affected research and data-driven projects. For instance, in a study analyzing unstructured data from social media (Facebook, Twitter, Reddit, etc.) to predict stock market trends, the Cambridge Analytica incident and GDPR compliance issues made it impossible to test the model. This case highlights how privacy laws can restrict data accessibility, potentially hindering academic and commercial research efforts.
- **Limitations on Data Monetization:** GDPR prevents companies from selling user data to third parties without explicit consent [10]. While this enhances privacy, it has also led to concerns about the emergence of black markets for user data, where illicit sellers weigh the risks of selling personal data against potential profits. If left unchecked, such underground activities could further endanger user privacy.
- **Challenges in Cloud Forensics:** As outlined in [7], GDPR does not fully address cloud forensic challenges, where hackers can infiltrate cloud services, delete traces of their intrusion, and compromise data security. In such cases, companies may struggle to detect breaches or determine what data was accessed, posing significant compliance and security risks. Some organizations may even circumvent compliance measures, leading to future vulnerabilities in cloud-based infrastructures.

Firstly, let us take a look at the effect of GDPR on research, wherein the primary example is of my thesis in which I was planning to go through unstructured data from sources like Facebook, Twitter, Reddit, etcetera to predict if the stock market would go up or down the next day. However, after researching for three months, I came up with a model, but due to the Cambridge Analytica incident and the GDPR compliance, I could not test the model. Thus, proving that GDPR and privacy safety measures can have severe impacts on research. Secondly, due to the regulation, the organizations that collect the data cannot sell it to third-party users for profits [10]. Thus, due to the regulations, there is a possibility that there arises a black market for data where the sellers analyze the risks of sharing a particular piece of data concerning the fines. This also means that if not kept in check the user’s data is now at further risk and has become more valuable in terms of money and information.

Lastly, as addressed in [7] problems like Cloud Forensic Problem, where the attacker can enter the cloud, access the data and delete all the traces of the intrusion, there is very little a company can do. First of all the company cannot even detect if the intrusion happened or not since the hacker deletes her/his traces from the cloud and at the same time these organizations cannot change the permissions the hackers get once they are in the cloud [7]. Such issues may lead to some companies cutting corners around the compliance and could lead to more significant problems in the future.

### III. DATA PRIVACY BREACHES

#### A. Cambridge Analytica

##### a) Case Overview

One of the most significant cases of ethics in privacy breaches is the Facebook–Cambridge Analytica data incident. This incident differed from most data breach cases, which typically involve a hacker compromising a database and leaking the data. Instead, it was far more devastating because users voluntarily provided their data to Aleksandr Kogan, a researcher at the University of Cambridge [11]. Kogan created an app called This Is Your Digital Life [12], which was downloaded by 270,000 people [12]. However, this did not mean that only the data of 270,000 users was compromised. Facebook’s GraphAPI allowed developers to access information about users and their friends, ultimately affecting approximately 87 million people [11] [12]. Kogan subsequently passed the data to Cambridge Analytica, a data mining firm, which constituted a breach of privacy. Users had consented only to share their information with Kogan’s app, not with third parties [12]. Once in possession of the data, Cambridge Analytica mined it and created geo-location-based user profiles to assist political campaigns in targeting potential voters and influencing them based on their personal information [11] [12]. This process violated laws, Facebook’s policies regarding the sharing of application data, and the users’ trust. The incident had significant repercussions, including a campaign called #DeleteFacebook and a notable decline in Facebook’s stock price [12].

##### b) Consequences and Implications

The incident influenced political events [11], notably affecting many people’s lives. Additionally, Cambridge Analytica’s involvement in the EU referendum came under scrutiny, and the firm was also reported to have contributed to Ted Cruz’s 2015 presidential campaign [13].

The most significant impact, however, was the breach of users’ trust and the violation of their privacy. When Mark Zuckerberg was asked, “Would you tell us which hotel you are staying at?” During his testimony at the Capitol, he declined to disclose the name of the hotel. If Zuckerberg was uncomfortable revealing such a trivial piece of information, how severely was the privacy of individuals violated? The information gathered included users’ likes, dislikes, friends, and other highly personal data, which was then profiled and used to influence users, potentially causing them to make decisions they may or may not have wanted to make.

##### c) Response and Remediation

Facebook has already implemented several solutions in response to the incident. One notable change is that developers can no longer access data about users without explicit consent. This policy change eliminates the chain of data polling that previously allowed access to users’ friends’ information. According to [13], Facebook was aware of the potential for such data mining and the sale of user data but failed to take action at the time. Facebook should have implemented the necessary changes to GraphAPI or, at the very least, monitored where the data was being transmitted. During his testimony, Mark Zuckerberg stated, “We told Cambridge Analytica to delete the data, and they confirmed that they did. We believed them, but it turns out they did not delete it.” Facebook should have been more proactive in ensuring the data was properly deleted and verified that no backups existed. Finally, the introduction of the General Data Protection Regulation (GDPR) has ensured that companies now inform users about why their data is being collected and the potential implications of its use.

#### B. Target Data Breach

##### a) Case Overview

People typically do not consider the implications of using a credit card at a super market. However, with the ever-expanding credit history that links your credit limit, previous addresses, and creditworthiness, it becomes easier to profile an individual. In 2012, Target took advantage of this by conducting predictive analysis to increase sales to pregnant women and foster long-term customer loyalty [14]. By analyzing customer data, Target sought to identify individuals who were likely to be pregnant in order to send them targeted pregnancy-related coupons [14] [15] [16]. To build this predictive model, Target enlisted Andrew Pole, a professional with a master’s degree in economics and statistics [14].

One of the most striking statements made by Charles Duhigg in [14] is when he recounts two of Andrew Pole's colleagues asking if he could determine whether a customer was pregnant without her consent. This raises significant privacy concerns, as it demonstrates how a company can seek to uncover sensitive information without explicit permission from the individual. According to Martin Moylan in [17], this type of analysis, which targeted sales growth, involved approximately 50 employees.

Duhigg explains the pregnancy prediction process in [14], where the procedure began by creating a customer database. This was achieved by generating a "Guest ID" through the collection of personal information, such as credit card or coupon use, survey responses, customer care interactions, and email opens [14]. Once a basic profile was established, Target sought to associate various features with the customer in order to enhance the predictive model [14]. These features included age, marital status, address, driving distance to the store, the types of credit cards used, browsing history, and more [14]. Additionally, companies often purchase external data, such as ethnicity, employment history, education background, financial data, social media interests, and even personal preferences like preferred coffee brands or toilet paper choices [14].

With a comprehensive customer profile in place, Target was able to make predictions. According to Pole in [16], during the first trimester of pregnancy, women typically purchase magnesium, zinc, and calcium supplements, followed by unscented lotion in the second trimester. As they approached their delivery date, they often bought hand sanitizers, washcloths, and scent-free soaps [16]. By inputting these variables into the predictive model, Target could calculate a confidence level, and based on that, send targeted coupons to expectant mothers, fostering long-term customer loyalty [14] [16].

However, a year into the successful deployment of this predictive model, the first privacy breach came to light. A father went to a Target store to complain about a pregnancy-related coupon his daughter had received. He was upset that Target was allegedly influencing his daughter to get pregnant by sending such offers [14]. After the store manager apologized, the father revealed that he had not been aware of his daughter's pregnancy, and the expected delivery date was just a few months away.

#### *b) Consequences and Implications*

This case illustrates how companies can possess deeply personal and sensitive information about customers—information that they may not be willing to share. The data collected by companies is so detailed that it can include everything from an individual's recent whereabouts to the products they use in daily life. Moreover, the methods these companies use to gather such data are highly unethical. For example, in the case of Target, the company allegedly processed a customer's credit card and coupon redemption history without obtaining explicit consent from the customer. Storing and mining this data was not necessary for the business's core operations but was done in an effort to increase sales by targeting specific demographics.

This scenario is not unique. Many companies today engage in similar data collection and mining practices under the guise of providing a "better" user experience or personalized products. These companies often get away with unethical data mining because their terms of service are long, convoluted, and filled with legal jargon that users cannot fully understand. As a result, users unknowingly consent to the mining of their personal data.

#### *c) Response and Remediation*

The solution to this issue is not as straightforward as simply informing users about how their data is being used. There is a competitive race to gather data and build more accurate customer profiles to enhance sales through analytics. The General Data Protection Regulation (GDPR) in the European Union [8] is one of the first steps toward creating a universal framework to protect individuals' privacy. However, GDPR applies only within the EU. Companies should proactively implement similar privacy protection measures for all the countries they serve, regardless of whether they are legally required to do so.

Secondly, companies should provide a clear and concise summary of their terms of service when collecting user data. This summary should explain the purpose of data collection and the scope of its use. The reach of data collection should be limited to the application or service the user is interacting with, and should not extend to collecting personal information unrelated to the service. Lastly, users should have the right to consent to any data mining activities performed on their personal data. If a company has collected information that the user did not explicitly provide, the user should have the right to know how the company obtained it. Additionally, users should have the option to sue companies that violate their privacy rights.

### **C. OfficeMax**

#### *a) Case Overview*

The family was understandably shocked and distressed by the receipt of such a letter, which resurfaced painful memories of the tragedy [18-27]. After recovering from the initial shock, Mike Seay questioned how a stationery company like OfficeMax

could possess such deeply personal information that was not publicly available. He was puzzled about how they obtained access to this data [18–27].

Upon reaching out to officials from OfficeMax, they did not disclose any specific names or sources for the data, instead claiming that they had been using a third-party mailing list. They offered an apology for sending such insensitive mail [18–27].

*b) Consequences and Implications*

This case clearly demonstrates that companies often do not limit the data they store to just the products or services they offer. Rather, they extend their data collection to various external sources to acquire highly personal, sensitive information. In the case of Ashley’s family, receiving such a letter brought back painful memories of their loss. Such scenarios make it evident that certain types of data—especially those concerning personal tragedies—should not be accessible to companies for marketing purposes.

Furthermore, Mike Seay raised an important question: why would an office supply company possess such private information? This case raises a critical ethical concern: where does the boundary for unethical data mining stop? When do companies cross the line by storing information that is unrelated to their core business?

*c) Response and Remediation*

The situation highlighted above shows that, regardless of how private certain information may be, there are ways for companies to gain access to it. To address this issue, laws should prohibit companies from storing any personal data beyond the customer’s name and mailing address unless explicitly provided by the individual. If companies claim to use third-party mailing lists, those lists should be made transparent, and users should have the ability to opt out or remove their information from these lists.

Another potential solution would be to eliminate the use of third-party mailing lists altogether. Companies that wish to obtain a customer’s mailing address should be required to ask the customer directly. They should offer an enrollment form for promotional emails, with an option for users to easily unenroll via a helpline number or email. Furthermore, companies should face significant penalties for non-compliance with these policies, which would act as a deterrent.

Lastly, there should be a dedicated complaint channel—such as a mailbox, helpline, or email address—where users can report incidents like the one described above. This would allow regulatory officials to address complaints promptly and impose fines on companies that violate privacy regulations, thus making the process smoother for both consumers and authorities.

**D. Uber**

*a) Case Overview*

How often do you take an Uber, whether for a quick ride to visit a friend, heading to the airport, or running errands like grocery shopping? Have you ever stopped to consider the amount of sensitive data Uber has access to during your rides?

In addition to knowing your name, Uber collects detailed data, including your credit card information, pick-up location, in-transit location, drop-off point, driver ratings and feedback, and even details about your fellow riders when using UberPOOL. One would expect that this information is stored securely, encrypted, and only accessible to authorized individuals. However, as highlighted in several reports [28–36], this is not the case. Some Uber employees were granted full access to this data through a tool known as “God View.”

One notable example of misuse involved Uber employees tracking public figures, such as Beyoncé [29]. These employees also had the ability to access the trip information of their ex-partners and friends [28, 29]. This data, far from being encrypted, was not even kept confidential. This breach came to light, and as a result, Uber was fined \$20,000 [32], a relatively small amount considering the severity of the privacy invasion.

In addition to “God View,” Uber ran another controversial operation known as “Greyball,” which aimed to evade law enforcement and government regulators trying to shut down Uber’s operations in various cities worldwide. As reported [37–46], this operation was carried out in cities such as Boston and Las Vegas in the United States, as well as other countries like Australia, the United Kingdom, and China [38, 40, 41].

The way Uber implemented “Greyball” was by identifying government officials trying to shut them down. When these officials attempted to book a ride, Uber would display a fake app interface showing “ghost” cars or no cars at all [37–42]. Uber used several tactics to identify these officials, including analyzing credit scores to determine whether a user was connected to law

enforcement or government agencies [38, 40– 42]. They also used geolocation data to identify when the app was frequently opened near government offices, thus flagging potential "targets" for Greyball [38, 40–42]. Furthermore, Uber tracked social media profiles to gauge if users were involved with law enforcement or government agencies, along with monitoring if the app was accessed suspiciously often [38, 40–42, 44].

*b) Consequences and Implications*

These incidents reveal how companies like Uber collect a vast amount of sensitive and personal data beyond what is necessary for providing their services. The use of "God View" and "Greyball" raises significant privacy concerns, demonstrating that not only can personal data be accessed by unauthorized employees, but it can also be used to track individuals in ways that may be unethical or even illegal. This disregard for privacy highlights the lack of control users have over their data, even when it involves highly sensitive information, such as their location and interactions.

Moreover, Uber's actions—particularly the abuse of "God View" to track celebrities and ex-partners, as well as the manipulation of data to avoid regulatory scrutiny—underscore the broader ethical issues surrounding the collection and use of user data. It raises a crucial question: to what extent should companies be allowed to track their users' behaviors and leverage this data for internal purposes without informed consent?

*c) Response and Remediation*

To mitigate the privacy concerns outlined above, companies like Uber should implement strict access controls and ensure that only authorized personnel can access sensitive user data. This data should be encrypted and handled with the utmost care to prevent unauthorized access.

Additionally, the operation of tools like "Greyball" should be prohibited. Companies should be held accountable for unethical practices like evading law enforcement and manipulating app interfaces to deceive users and regulators. Transparency in data usage is essential, and users should be informed about the data collected, how it is being used, and the entities accessing it.

Furthermore, companies must adopt ethical guidelines and regulatory frameworks that align with privacy standards such as the GDPR. By offering users greater control over their data and implementing clear, user-friendly opt-in and opt-out options, Uber and other companies can build trust and ensure that user privacy is respected.

#### **IV. Equifax Data Breach**

*a) Case Overview*

Equifax is one of the leading credit reporting agencies, along with TransUnion and Experian [47]. The role of a credit reporting agency is to assess the creditworthiness of a customer based on their ability to repay borrowed credit. This information can determine whether a customer is eligible for a credit card, how much credit should be extended, and whether a person qualifies for home loans, car loans, or any other type of loan. As a result, these agencies store highly sensitive information such as Social Security Numbers (SSNs), credit card numbers, and addresses.

In July 2017, one of the largest data breaches occurred when Equifax was compromised [48–51]. According to reports, the breach was due to a security flaw in Equifax's web application systems, caused by a vulnerability in the underlying technology they were using—Apache Struts [47, 52–54]. Apache named the vulnerability "CVE-2017-5638" [53, 54] and alerted users to the issue in March 2017 [53]. The vulnerability created a backdoor into the servers, allowing attackers to execute malicious code remotely [53, 54]. The biggest fault of Equifax was their failure to act upon the notification and patch provided by Apache, leading to the breach.

Initially, Equifax reported that 143.3 million people were affected, but later corrected the number to 145 million [47–50, 52]. Of these, 209,000 individuals had their credit card numbers compromised [53, 55, 56]. Additionally, other personal information stolen included driver's license numbers, dates of birth, SSNs, and names [47–50, 52].

This breach was not the first instance of Equifax mishandling sensitive customer data. On a previous occasion, the company sent a woman 300 credit reports from other customers, which included SSNs, loan numbers, and credit card details due to an error [48, 57].

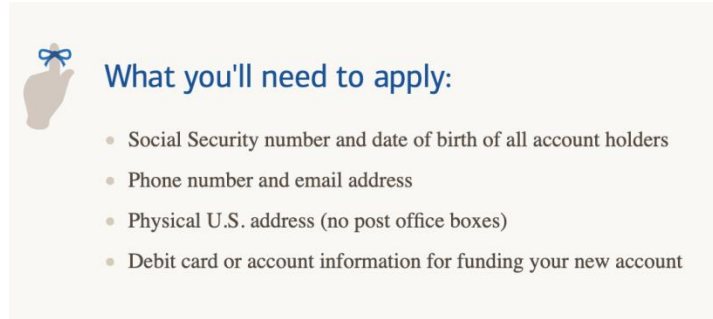
Furthermore, Equifax's actions after the breach were also criticized. The company did not notify affected customers until two months after the breach occurred—despite it happening in July 2017, the official statement was not made until September.

During this period, the company continued to sell stock, potentially to mitigate losses, while claiming that the board was unaware of the breach [48].

*b) Consequences and Implications*

The data breach mentioned above is one of the most impactful privacy breaches among all recent incidents. The significance of this breach lies in the fact that highly sensitive information, such as names, addresses, Social Security Numbers (SSNs), driver's license numbers, and birth dates, was compromised. Let us explore how these pieces of information can lead to a massive invasion of privacy for anyone affected.

For example, assume a person wishes to open a bank account. To do so, they would typically need to provide their SSN, date of birth, and physical address. To confirm these requirements, I referred to [58] and retrieved the image 3.5.



**Figure 1 : Requirements - Bank of America [58]**

The same risks apply when trying to get a credit card, as the credit score and personal details required for approval are very similar.

Moreover, if you apply for a job, your credit score is often checked, and if your SSN, full name, and birthdate are exposed, a third party could potentially use this information to apply for the job in your name. The consequences of someone else having access to your SSN and other sensitive data are severe. Beyond opening credit cards, bank accounts, or securing jobs, an individual with this information could take out loans, purchase a house or a car, or acquire other products in the victim's name.

For another example, consider booking a flight with an airline. A hacker could call customer service to make changes to the reservation. In order to verify the identity of the caller, the airline representative might ask for the hacker's full name and date of birth, both of which the hacker now has. This would allow the hacker to cancel your flight or make other alterations. The risks are not limited to airlines; the hacker could exploit similar verification processes across various services using the data from the breach.

Lastly, the long-term impact of this breach will affect an entire generation. Individuals will need to remain vigilant for any suspicious activity related to their credit information, and there's also the possibility that their personal data could be used for criminal activities. The breach not only exposed sensitive financial data but also provided hackers with the physical addresses of the victims, heightening the threat further.

*c) Response and Remediation*

This case differs from the others mentioned above because the data compromised is far more sensitive. The critical issue with this breach is that a person cannot change their date of birth or SSN, making it much harder to recover from.

As highlighted in the article [59], it is important for individuals to regularly check their credit reports for any anomalies and take advantage of credit monitoring services offered by credit card companies. Additionally, the article recommends that individuals freeze their accounts and report any fraud to prevent hackers from opening new accounts in their name. If someone discovers that their identity has been used fraudulently, they can visit [identitytheft.gov/data-breach](https://www.identitytheft.gov/data-breach) to report the issue. There are also third-party monitoring services, such as LifeLock [60], which help track potential identity theft. However, these services are not foolproof. In fact, Life Lock previously failed to provide the promised protection and was fined \$12 million as a result [61].

Therefore, it is crucial for individuals to remain vigilant about their own identity security and promptly report any suspicious activity to credit agencies and government officials to protect themselves.

#### IV. CAUSES AND EFFECT MODEL

This section will cover cases beyond those mentioned in Sections 3.1, 3.2, 3.3, 3.4, and 3.5. We have created a cause-and-effect diagram based on all the cases, which outlines the reasons behind privacy breaches, as shown in Figure 4. This figure maps the cases according to specific causes, with the mapping details provided further in this section. The key to the mapping corresponds to the case names and the numbers shown in Figure 4, and the complete documentation of each case can be found in the references section.

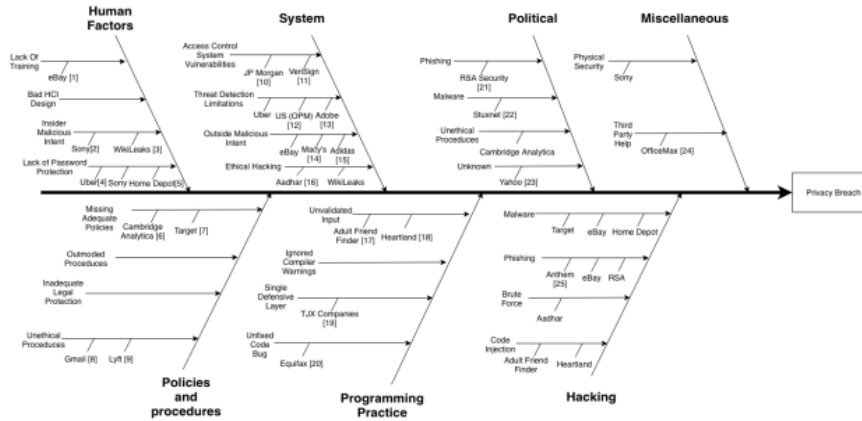


Figure 2 : Ishikawa Model

Figure 4 illustrates a cause-and-effect model, where the final effect is located on the rightmost side of the diagram, and the eight arrows on the left side represent the reasons behind the occurrence of the final effect. Each cause is further broken down into sub-causes, many of which are associated with specific case studies, denoted by the smallest line with a number next to it. According to [62], the Ishikawa model, also known as the "fishbone" diagram, can be used to evaluate a process by analyzing each of its components. Furthermore, in [63], the authors suggest that the Ishikawa model helps identify the major causes of a problem and brings them together for a more thorough evaluation of the effect and its causes.

The following is the mapping for the Ishikawa model:

- eBay Data Breach [64]: [65] [66]
- Sony Data Breach [64]: [67]
- WikiLeaks: [68]
- Uber Data Breach [64]: [69]
- Home Depot Data Breach [64]: [70]
- Cambridge Analytica: [11]
- Target Data Breach [64]: [71]
- Gmail Reading User’s Emails: [72]
- Lyft God View: [73]
- JP Morgan Data Breach [64]: [74]
- VeriSign Data Breach [64]: [75]
- United States Office of Personnel Management (US OPM) [64]: [76]
- Adobe Data Breach [64]: [77] [78]
- Macy’s Data Breach [79]: [80] [81]
- Adidas Data Breach [79]: [82] [83]
- Aadhar Data Breach [79]: [4] [84]
- Adult Friend Finder Data Breach [64]: [85]
- Heartland Payment Systems Data Breach [64]: [86]
- TJX Companies Data Breach [64]: [87]
- Equifax Data Breach [64]: [54]
- RSA Security [64]: [88]
- Stuxnet [64]: [89]
- Yahoo Data Breaches [64]: [90]

- OfficeMax Privacy Breach: [24]
- Anthem Data Breach [64]: [91]

The figure below highlights the most likely reasons that can lead to privacy breaches, incorporating relevant case studies for each cause. It can be inferred that, while hackers occasionally outsmart systems and security protocols, the majority of privacy breaches occur due to human error.

#### V. FUTURE WORK

This paper has explored a wide range of data and privacy breaches, along with their underlying causes. However, significant gaps still exist in the current legal framework, which allows companies to exploit these loopholes. While the General Data Protection Regulation (GDPR) has set a precedent in prioritizing data privacy protection, more comprehensive laws should be enacted globally to ensure better protection for individuals' privacy.

One potential improvement would be for governments worldwide to collaborate on creating stricter data privacy laws. Additionally, governments can offer enhanced protection and incentives for whistleblowers, encouraging insiders to report violations without fear of retaliation.

Finally, public awareness campaigns should be intensified to ensure that the general population understands the risks associated with fraudulent use of their data. These campaigns should focus on issues such as phishing, password security, recognizing malicious emails, and identifying sensitive information that should remain private. Moreover, companies should prioritize employee training to ensure rigorous code reviews, promptly addressing any vulnerabilities detected to prevent potential breaches.

#### VI. CONCLUSION

- **User Awareness and Control:** Users should be better informed about what data they are sharing with companies. It is essential that companies provide clear and transparent information regarding data collection practices. Additionally, users should have the option to opt-out of marketing campaigns or other services if they do not wish to receive them. This empowers users to maintain control over their personal information and preferences.
- **Improved System Security:** Companies must prioritize system security and conduct rigorous vulnerability checks. Any identified weaknesses should be addressed immediately, without delay, to prevent potential breaches. Ensuring strong cybersecurity measures can help avoid exposure of sensitive user data.
- **Transparency and Accountability:** Companies must be transparent when data breaches occur and should not withhold information from affected customers. Early notification is essential so that customers can take preventative actions, such as freezing their accounts or monitoring for identity theft, to mitigate potential harm.
- **Stronger Regulations:** More regulations, similar to the GDPR, should be implemented globally to enhance data privacy protection. These regulations should focus on safeguarding user information while also allowing businesses to operate ethically and responsibly. Regulatory frameworks that prioritize user well-being can help strike a balance between consumer rights and corporate interests.
- **Clear and Accessible Terms of Service:** Companies should make their terms of service more user-friendly, ensuring they are easily understandable and accessible to the general public. Avoiding complex legal jargon will help users make informed decisions before agreeing to terms, preventing deceptive practices and fostering trust between businesses and consumers.

#### V. REFERENCES

- [1] Facebook, "Company Info – Facebook Newsroom." [Online]. Available: <https://newsroom.fb.com/company-info/>. Accessed: Mar. 25, 2025.
- [2] Association for Computing Machinery, "ACM Code of Ethics and Professional Conduct," ACM, 2018.
- [3] G. G. Fuster and S. Gutwirth, "Ethics, law and privacy: Disentangling law from ethics in privacy discourse," in Proc. IEEE Int. Symp. Ethics in Eng., Sci., and Technol., 2014, p. 12.
- [4] R. Sengupta, "'Vigilante hacker' flags security concerns in Aadhaar, govt websites again," The Times of India, 2018.
- [5] W. W. Lee, W. Zhang, and H. Chang, "An ethical approach to data privacy protection," ISACA, 2016.
- [6] P. Shrivastava, "All you need to know about GDPR - Explained," Hacker Noon. [Online]. Available: <https://hackernoon.com/all-you-need-to-know-about-gdpr-explained-8e336a1987ea>. Accessed: Mar. 25, 2025.
- [7] B. Duncan, "Can EU General Data Protection Regulation compliance be achieved when using cloud computing?" CLOUD COMPUTING 2018, p. 11, 2018.
- [8] European Union, "General Data Protection Regulation." [Online]. Available: <https://gdpr-info.eu/>. Accessed: Mar. 16, 2025.

- [9] M. Cornock, "General Data Protection Regulation (GDPR) and implications for research," Elsevier, 2018.
- [10] D. Allen, A. Berg, C. Berg, and J. Potts, "Some economic consequences of the GDPR," 2018.
- [11] A. Chang, "The Facebook and Cambridge Analytica scandal, explained with a simple diagram," Vox, 2018. [Online]. Available: <https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram>. Accessed: Mar. 25, 2025.
- [12] The Verge, "Facebook's Cambridge Analytica data scandal, explained - YouTube," YouTube, 2018. [Online]. Available: <https://www.youtube.com/watch?v=VDR8qGmyEQg>. Accessed: Mar. 25, 2025.
- [13] S. B. Psaila, "Cambridge Analytica explained: The facts, implications, and open questions," GIP Digital Watch, 2018. [Online]. Available: <https://dig.watch/trends/cambridge-analytica>. Accessed: Mar. 25, 2025.
- [14] C. Duhigg, "How companies learn your secrets," The New York Times, Feb. 16, 2012.
- [15] F. Z. Maksood and G. Achuthan, "Analysis of data mining techniques and its applications," Analysis, vol. 140, no. 3, 2016.
- [16] K. Hill, "How Target figured out a teen girl was pregnant before her father did," Forbes, 2012.
- [17] M. Moylan, "Target's deep customer data mining raises eyebrows," MPR News, 2012. [Online]. Available: <https://www.mprnews.org/story/2012/03/07/target-data-mining-privacy>. Accessed: Mar. 25, 2025.
- [18] A. Weldon, "Attentional commons and the common good: Technology and higher education," Intersections, vol. 2015, no. 42, p. 8, 2015.
- [19] C. Doctorow, "OfficeMax sends junkmail addressed to 'Daughter Killed In Car Crash'," Boing Boing, 2014. [Online]. Available: <https://boingboing.net/2014/01/20/officemax-sends-junkmail-adre.html>. Accessed: Mar. 22, 2025.
- [20] HuffPost, "Mike Seay gets OfficeMax junk mail referencing daughter killed in car crash," HuffPost, 2014. [Online]. Available: <https://www.huffingtonpost.com/2014/01/20/mike-seay-officemax-letten-4632822.html>. Accessed: Mar. 22, 2025.
- [21] M. Pearce, "OfficeMax executive apologizes over 'daughter killed' mailer," Los Angeles Times, 2014. [Online]. Available: <http://www.latimes.com/nation/la-na-officemax-mess-20140121-story.html>. Accessed: Mar. 22, 2025.
- [22] A. Merrick, "A death in the database," The New Yorker, 2014. [Online]. Available: <https://www.newyorker.com/business/currency/a-death-in-the-database>. Accessed: Mar. 22, 2025.
- [23] R. Orlove, "How does OfficeMax know this man's daughter was killed in a car crash?" Jalopnik, 2014. [Online]. Available: <https://jalopnik.com/how-does-officemax-know-this-mans-daughter-was-killed-i-1505042599>. Accessed: Mar. 22, 2025.
- [24] N. Kwan, "OfficeMax sends letter to 'Daughter Killed in Car Crash'," NBC Chicago, 2014. [Online]. Available: <https://www.nbcchicago.com/news/local/OfficeMax-Sends-Letter-to-Daughter-Killed-in-Car-Crash-240941291.html>. Accessed: Mar. 22, 2025.
- [25] N. Kwan, "OfficeMax apologizes for 'Daughter Killed in Car Crash' letter," NBC Chicago, 2014. [Online]. Available: <https://www.nbcchicago.com/news/local/OfficeMax-Apologizes-Illinois-Family-Letter-241147581.html>. Accessed: Mar. 22, 2025.
- [26] J. Howerton, "OfficeMax letter includes shocking note about recipient's dead daughter," Business Insider, 2014. [Online]. Available: <http://www.businessinsider.com/officemax-letter-includes-shocking-note-about-recipients-dead-daughter-2014-1>. Accessed: Mar. 22, 2025.
- [27] Fox News Insider, "OfficeMax junk mail letter mentions death of couple's daughter," 2014. [Online]. Available: <http://insider.foxnews.com/2014/01/20/officemax-junk-mail-letter-mentions-death-couples-daughter>. Accessed: Mar. 22, 2025.
- [28] R. Morgan, "Uber settles federal probe over 'God View' spy software," New York Post, 2017. [Online]. Available: <https://nypost.com/2017/08/15/uber-settles-federal-probe-over-god-view-spy-software/>. Accessed: Mar. 15, 2025.
- [29] C. Smith, "Uber allegedly spied on celebrities like Beyoncé for years," New York Post, 2016. [Online]. Available: <https://nypost.com/2016/12/13/uber-allegedly-spied-on-celebrities-like-beyonce-for-years/>. Accessed: Mar. 15, 2025.
- [30] S. Frizell, "What is Uber really doing with your data?" Time, 2014. [Online]. Available: <http://time.com/3595025/uber-data/>. Accessed: Mar. 15, 2025.
- [31] E. Bacharach, "Uber has a 'God View' tool and was allegedly using it to spy on celebs," Cosmopolitan, 2016. [Online]. Available: <https://www.cosmopolitan.com/lifestyle/a8495499/uber-using-god-view-tool-to-spy-on-celebs/>. Accessed: Mar. 15, 2025.
- [32] C. Welch, "Uber will pay \$20,000 fine in settlement over 'God View' tracking," The Verge, 2016. [Online]. Available: <https://www.theverge.com/2016/1/6/10726004/uber-god-mode-settlement-fine>. Accessed: Mar. 15, 2025.
- [33] A. Hern, "Uber employees 'spied on ex-partners, politicians and Beyoncé'," The Guardian, 2016. [Online]. Available: <https://www.theguardian.com/technology/2016/dec/13/uber-employees-spying-ex-partners-politicians-beyonce>. Accessed: Mar. 15, 2025.
- [34] J. Bhuiyan, "'God View': Uber investigates its top New York executive for privacy violations," BuzzFeed News, 2014. [Online]. Available: <https://www.buzzfeednews.com/article/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy#.eyoM7RdDZv>. Accessed: Mar. 15, 2025.
- [35] M. Farber, "Uber tracked Lyft drivers with secret 'Hell' program," Fortune, 2017. [Online]. Available: <http://fortune.com/2017/04/13/uber-lyft-hell/>. Accessed: Mar. 15, 2025.
- [36] B. M. Wolfe, "Uber's 'God View' is alive and well, say former employees," AppAdvice. [Online]. Available: <https://appadvice.com/post/ubers-god-view/731803>. Accessed: Mar. 15, 2025.
- [37] R. L. Trope and L. L. Hantover, "Reckoning with the hacker age: Cybersecurity developments," Bus. Law., vol. 73, p. 227, 2017.

- [38] C. Page, "Uber facing criminal probe over data-mining Greyball software – V3," 2017. [Online]. Available: <https://www.v3.co.uk/v3-uk/news/3009582/uber-facing-criminal-probe-over-data-mining-greyball-software>. Accessed: Mar. 15, 2025.
- [39] R. Felton, "Uber employees use secret tools to target drivers and undercut competition," Jalopnik, 2017. [Online]. Available: <https://jalopnik.com/uber-employees-use-secret-tools-to-target-drivers-and-u-1793495814>. Accessed: Mar. 15, 2025.
- [40] C. Doctorow, "Uber uses data-mining to identify and block riders who may be cops, investigators or regulators / Boing Boing," 2017. [Online]. Available: <https://boingboing.net/2017/03/04/sounds-legit.html>. Accessed: Mar. 15, 2025.
- [41] Wikipedia contributors, "Controversies surrounding Uber – Wikipedia, The Free Encyclopedia," 2018. [Online]. Available: [https://en.wikipedia.org/wiki/Controversies\\_surrounding\\_Uber](https://en.wikipedia.org/wiki/Controversies_surrounding_Uber). Accessed: Mar. 15, 2025.
- [42] M. Isaac, "How Uber deceives the authorities worldwide," 2017.
- [43] M. Isaac, "Uber faces federal inquiry over use of Greyball tool to evade authorities," 2017.
- [44] A. Sulleyman, "Greyball: What is the creepy feature that got Uber banned in London?," 2017.
- [45] G. Harrison, "What is Greyball and why is the Uber software so controversial?," 2017.
- [46] Reuters, "Uber: Portland probe finds Greyball used to evade officials," 2017.
- [47] T. G. Siracusa Jr, "The Equifax breach: What we learned and how we can protect consumer data," Loy. Consumer L. Rev., vol. 30, p. 460, 2017.
- [48] LastWeekTonight, "Equifax: Last Week Tonight with John Oliver (HBO) - YouTube," 2017. [Online]. Available: <https://www.youtube.com/watch?v=mPjgRKWJmk>. Accessed: Mar. 18, 2025.
- [49] B. Fung, "Equifax's massive 2017 data breach keeps getting worse," 2018.
- [50] Federal Trade Commission, "Equifax data breach settlement – Federal Trade Commission," 2017. [Online]. Available: <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement>. Accessed: Mar. 25, 2025.
- [51] Federal Trade Commission et al., "The Equifax data breach: What to do," 2017
- [52] J. W. et al., "How the Equifax data breach happened: What we know now," 2017
- [53] H. Green, "How the massive Equifax data breach happened," SciShow, 2017. [Online]. Available: <https://www.youtube.com/watch?v=6Qbslgpw8U>. Accessed: Mar. 19, 2025
- [54] J. Luszcz, "Apache Struts 2: how technical and development gaps caused the Equifax breach," Network Security, vol. 2018, no. 1, pp. 5–8, 2018
- [55] Y. Swamynathan, "Equifax reveals hack that likely exposed data of 143 million customers," 2017
- [56] L. Nicholson et al., "Does the Equifax Inc breach have implications for Australian companies?," Governance Directions, vol. 70, no. 3, p. 134, 2018
- [57] J. Chrisos, "Credit agency mistakenly sends 300 confidential reports to Maine woman – State," 2015
- [58] Bank of America, "Core Checking® Account - Before You Apply," 2018. [Online]. Available: <https://tinyurl.com/bofarequirements>. Accessed: Mar. 19, 2025
- [59] Federal Trade Commission, "The Equifax data breach: What to do," 2017. [Online]. Available: <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>. Accessed: Mar. 20, 2025
- [60] LifeLock, "Identity theft protection," 2018. [Online]. Available: <https://www.lifelock.com/>. Accessed: Mar. 20, 2025
- [61] Federal Trade Commission et al., "LifeLock will pay 12 million to settle charges by the FTC and 35 states that identity theft prevention and data security claims were false," 2010
- [62] L. Vetter, G. Schuepfer, S. P. Kuster, and M. Rossi, "A hospital-wide outbreak of *Serratia marcescens*, and Ishikawa's 'fishbone' analysis to support outbreak control," Quality Management in Health Care, vol. 25, no. 1, p. 1, 2016
- [63] G. Ilie and C. N. Ciociu, "Application of fishbone diagram to determine the risk of an event with multiple causes," Management Research and Practice, vol. 2, no. 1, pp. 1–20, 2010
- [64] T. Armerding, "The 17 biggest data breaches of the 21st century," CSO Online, 2018. [Online]. Available: <https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html>. Accessed: Mar. 24, 2025
- [65] J. Wakefield, "eBay faces investigations over massive data breach," BBC News, 2014
- [66] S. Coty, "The eBay breach explained," SC Magazine. [Online]. Available: <https://www.scmagazine.com/the-ebay-breach-explained/article/537762/>. Accessed: Mar. 24, 2025
- [67] J. Bort, "How the hackers broke into Sony," Business Insider, 2014. [Online]. Available: <https://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12>. Accessed: Mar. 24, 2025
- [68] I. Munro, "Whistle-blowing and the politics of truth: Mobilizing 'truth games' in the WikiLeaks case," Human Relations, vol. 70, no. 5, pp. 519–543, 2017
- [69] M. Isaac, K. Benner, and S. Frenkel, "Uber hid 2016 breach, paying hackers to delete stolen data," New York Times, Nov. 21, 2017
- [70] B. Hawkins, "Case study: The Home Depot data breach," 2015. [Online]. Available: Retrieved Jan. 19, 2016
- [71] N. Manworren, J. Letwat, and O. Daily, "Why you should care about the Target data breach," Business Horizons, vol. 59, no. 3, pp. 257–266, 2016
- [72] D. MacMillan, "Tech's 'dirty secret': The app developers sifting through your Gmail," Wall Street Journal, 2018. [Online]. Available: <https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442>. Accessed: Mar. 25, 2025
- [73] J. Constine, "Former employees say Lyft staffers spied on passengers," 2018

- [74] N. E. Weiss and R. S. Miller, "The Target and other financial data breaches: Frequently asked questions," Congressional Research Service, vol. 4, Feb. 2015
- [75] K. Zetter, "VeriSign hit by hackers in 2010," Wired, 2012. [Online]. Available: <https://www.wired.com/2012/02/verisign-hacked-in-2010/>. Accessed: Mar. 24, 2025
- [76] K. Finklea, M. D. Christensen, E. A. Fischer, S. V. Lawrence, and C. A. Theohary, "Cyber intrusion into US Office of Personnel Management: In brief," Congressional Research Service, Library of Congress, Washington, DC, 2015
- [77] B. Krebs, "Adobe breach impacted at least 38 million users," Krebs on Security, 2013
- [78] B. Krebs, "Adobe to announce source code, customer data breach," Krebs on Security, 2013
- [79] D. Green and M. Hanbury, "Companies with data breaches in 2018," Business Insider. [Online]. Available: <https://www.businessinsider.com/data-breaches-2018-4>
- [80] I. Mangla, "Macy's & Bloomingdale's data breach: What you need to know," Experian, 2018. [Online]. Available: <https://www.experian.com/blogs/ask-experian/macys-bloomingdales-data-breach-what-you-need-to-know/>. Accessed: Mar. 24, 2025
- [81] H. George-Parkin, "Macy's data breach: Customer emails, credit cards compromised," Footwear News, 2018. [Online]. Available: <https://footwearnews.com/2018/business/retail/macys-data-breach-emails-credit-cards-1202585526/>. Accessed: Mar. 24, 2025
- [82] K. Bhasin, "Adidas says millions of U.S. customers being alerted of breach," Bloomberg, 2018. [Online]. Available: <https://www.bloomberg.com/news/articles/2018-06-28/adidas-says-millions-of-u-s-customers-being-alerted-of-breach>. Accessed: Mar. 24, 2025
- [83] D. Green, "Adidas warns customers of potential data breach," Business Insider, 2018. [Online]. Available: <https://www.businessinsider.com/adidas-warns-customers-potential-data-breach-2018-6>. Accessed: Mar. 24, 2025
- [84] Indiatimes, "An online researcher hacked into Aadhaar's official Android app to show how poorly it's secured," 2018. [Online]. Available: <https://tinyurl.com/aadharbreach>. Accessed: Mar. 24, 2025
- [85] S. Ragan, "Adult Friend Finder confirms data breach, 3.5 million records exposed," CSO Online, 2015. [Online]. Available: <https://www.csoonline.com/article/551561/adult-friend-finder-confirms-data-breach-3-5-million-records-exposed.html>. Accessed: Mar. 24, 2025
- [86] J. S. Cheney, "Heartland Payment Systems: Lessons learned from a data breach," FRB of Philadelphia - Payment Cards Center Discussion Paper, vol. 10, no. 1, 2010
- [87] W. Xu, G. Grant, H. Nguyen, and X. Dai, "Security breach: The case of TJX Companies, Inc.," Communications of the Association for Information Systems, vol. 23, no. 1, p. 31, 2008
- [88] J. Leyden, "RSA explains how attackers breached its systems," The Register, vol. 4, 2011
- [89] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," IEEE Security & Privacy, vol. 9, no. 3, pp. 49-51, 2011
- [90] S. Larson, "Every single Yahoo account was hacked—3 billion in all," CNN Tech, Oct. 4, 2017
- [91] P. Paganini, "Cybercrime exploits Anthem data breach in phishing campaigns," 2015