The Ethicality of User Privacy in the Digital Age

Team 1:

Mareed Alam, Edison Chen, Tai Dinh,

Sparsh Guruwacharya, Cali Maier,

Natalia Matys, Justin Oh

University at Buffalo

MGT 401: Public Policy, Law & Management

Professor Alfonso Bax

December 3, 2024

Introduction

"It used to be expensive to make things public and cheap to make them private. Now it's expensive to make things private and cheap to make them public."

- Clay Shirky, former CIO at NYU Shanghai

Imagine a time before the internet which includes social media, emails, smartphones, or any online services. It sounds crazy, right? But back then, privacy was quite simple as your personal data was kept through physical methods like diaries, mailing envelopes, paper records, or files by your financial and health institutions. Oftentimes, this seemed to feel more secure as it relied on direct interaction between the two parties to collect the customer's data. But of course, just like everything else in life, nothing is perfect and people's private data are not entirely private. Think about it, back then you would have financial institutions storing your financial accounts, credit statements, or loans in physical ledgers. And on the topic of related industries, let's not forget that insurance companies would keep records of your life and health policies on file or when employers would physically track their worker's information. Regardless of the different types of entities or systems, they all rely on people handling your personal information. But remember, nothing is perfect. What if someone's file went missing? It probably did. Or what if someone shared it, unintentionally or intentionally? A two hundred percent chance that has happened before. Privacy breaches happened regardless of whether you were aware of how things worked back then, but they did, just like the privacy breaches you're accustomed to in our modern digital age. Now sure, back then, breaches probably did occur on a smaller scale and often involved human mistakes or intentional acts.

Now let's fast forward to our modern age. Your personal data in digital applications is no longer stored in physical filing cabinets but is most likely somewhere in a bunch of sophisticated online databases. Think about the last time you shared your information. Was it when you signed up for social media? Posted a life event to that social media? Signed up for a streaming service? Bought a new phone and used its biometric features? Well, these ideas aren't new. Larger entities such as the government and businesses will always have a need for personal data to provide services. Back then, it took greater effort and time to collect and store people's information. The main difference in today's age is in speed and scale since data collection can be instant, digital, and even collected without one's awareness.

In our digital world, our privacy is without a doubt, becoming one of the most pressing ethical concerns even if we're led to believe that it isn't. As human technological advancements (artificial intelligence, smartphones, internet, social media, big data-driven applications, etc) continue to merge into our daily lives, the collection and use of personal data becomes more vulnerable to misuse and raises ethical questions. Just take a minute to really think about your digital footprint which includes your social media activity, text and image data you upload, online purchases, websites you visit, and so much more. Most of us probably unlock our phones with a face scan or a fingerprint scan, and have probably never thought about where that biometric data goes or who could have access to it. And why would we? Well, we often turn a blind eye to these questions because of the sheer convenience we're able to obtain as a digital user. It makes sense right? It's quite the human nature to prioritize simplicity. If these digital actions were any more inconvenient than it is, we'd naturally stop and assess the worthiness of the effort. This relates to the simple idea that when something is harder to do, it naturally forces us to think twice, therefore raising potential questions in the process. Imagine if social media hypothetically required everyone to submit multiple forms of ID, or complete a 20-minute questionnaire, we'd stop and ask ourselves if this effort is worth putting our personal information out there. Aside from biometric data, we all most likely left a trace of our personal data such as location tracking, personal messages, shopping habits, etc. But wait, where does our personal data go and who would have access to it? Some of the largest key players include the government, and of course, the corporations that provide the online services on which your personal information is collected. Government entities may monitor online platforms under the impression of security and corporations may mine users' data to influence what type of content a user can and can't see. However, whether through the monitoring of users' online presence or the collection of people's personal data, questions concerning how much privacy individuals are entitled to and how much access the government or corporations should have continued to be significant in such debates.

Some noteworthy practices that illustrate the ethicality of user privacy in our digital world are social media surveillance, data collection by private entities and/or government, and the overall data security obligation. With these practices comes certain ethical dilemmas which will be explored in this paper. This analysis paper explores these ethical dilemmas surrounding user privacy, focusing on the pros and cons of the aforementioned practices. Arguments can include that ethical boundaries are not always well-defined, as practices that appear harmful may potentially yield beneficial results and vice versa.

This industry is relevant to data collection under the broader topic of user privacy. A focus is put on protecting the personal data of individuals by preventing the use, access, and sharing by third-party individuals. The industry of data privacy currently has general laws that govern fair use and protection of individuals. There are federal-level laws such as HIPAA and state-level laws like the CCPA (California Consumer Privacy Act) in regard to the United States. The CCPA published in 2018 for example, ensures that people have the right to know about the personal information a business collects from them and that they may request for that information to be deleted (with exception). There are multiple stakeholders as one would expect. The government targets the use of this data to enforce security throughout the nation, public health, and improve current infrastructure. On the other hand, corporations attempt to collect this data so they may read consumer behavior and improve their marketing strategies. In the end, activists for privacy are interested in the reach of data collection and advocate for stronger protection of individuals and their data.

Data Collection and the User Experience

With technology advancing as fast as it is, companies are innovating in order to remain relevant and provide their users with cool new features. Back in 2013, Apple came out with touch ID, allowing iPhone users to unlock their phones with just the tap of their fingers. Although this did raise some concerns about data collection, the general public loved it. Being able to unlock their phones by just holding their finger was revolutionary, until Apple's Face ID implementation in 2017. In just four years, Apple was able to implement a feature that quickly authenticates a user just by looking at the phone. This felt like something out of an old sci-fi movie, except now it's a reality. The face ID significantly enhanced user convenience while providing better security for their devices. According to Forbes, this feature was not only user friendlier, it was also more secure and more accurate. The false acceptance rate of face ID was 1 in a million compared to the 1 in 50,000 rate by touch ID. The introduction of this technology shook Apple's biggest competitor, Samsung. Samsung listened to all the concerns of this new feature and created the Nexsign system. Not only was this system the only PKI-based infrastructure to have attained the Common Criteria certification, the platform also brings biometric authentication to enterprise mobile management, supporting voice, fingerprint, and facial recognition. This allowed users to choose whichever method of unlocking their devices they wanted while offering a high level of security because of their PKI-based infrastructure since it uses public and private key cryptography. "The biometric template and the private key are encrypted and stored in the OS of the customer device, where hackers can't intercept them. The encrypted public key is [then] sent to the FIDO server located behind the corporate firewall." (Forbes) Their security features were so impressive, they won "a Global Mobile Award (or 'Glomo' Award) in the category of Best Mobile Security or Anti-Fraud Solution, for its Samsung Mobile Security Management Suite." (IDtechwire)

Most data collections are used by companies to provide personalized content that will increase user engagement on their platform such as Tiktok and their video recommendation algorithm or Spotify and its personalized playlists. These types of features take personal data such as what types of videos do the user like, shorts vs longer videos, what genre, what topic, etc. Spotify is a great example of this. They have personalised playlists generated based on your music playlists and what genres seem to be popular. They offer playlists such as "your day" playlist, discover weekly, blend playlists where you combine your music taste with one or more friends into one playlists, smart shuffle generating similar songs to your playlists, and more. Their blend playlists are the most impressive in my opinion since it takes into consideration multiple people's taste and not just an individual's. According to Spotify's engineering page, it looks into attributes such as "Relevant: Does the track we're selecting for that user reflect their taste? Or is it just a song they accidentally listened to once? Coherent: Does the playlist have flow, or do the tracks feel completely random and unrelated to each other? Equal: Are both users in the Blend represented equally? Democratic: Does music that both users like rise to the top?" Combining all of these attributes, Spotify is able to create a playlist that "maximizes the joy." This means the playlist selects songs that are most personally relevant to a user rather than what's more democratic and coherent. This feature that tracks and creates based on the listening habits of users has given a new way to connect with others through their music.

On the other hand is Amazon's Alexa. The product is amazing, having feature such as: smart home integration, allows Alexa to control lights, cameras, and thermostats; accessibility features, allows those with limited mobility to perform tasks without needing to interact with a touch screen; entertainment, can stream content when paired with Alexa's Echo Show; and even shopping convenience, users can shop on amazon without needing a device. The features are made possible because Alexa collects the user's personal data. According to PC mag, Amazon's Alexa collects and stores this information about a user: name, time zone, address, phone numbers, payment information, age, personal interests, personal descriptions, and IP address. This amount of stored information is already a bit concerning, but the bigger issue is with Alexa listening and storing audio recordings. Since Alexa is activated by voice, it is passively always listening for the word "Alexa" which may lead to unintentional recordings of other conversations. Back in 2023, Amazon had to settle a $30 million civil lawsuit because of unlawful storage of children's voice and location data. Amazon kept the kid's data as a way to improve the AI voice recognition algorithm behind Alexa. According to what FTC Commissioner, Alvaro Bedoya, told PBS News, “when parents asked Amazon to delete their kids’ Alexa voice data, the company did not delete all of it.” In this case, data collection can be helpful and provide convenience for its users, but does that outweigh the potential of unauthorized surveillance?

Niantic’s Pokémon Go and Data Collection

Pokémon Go was developed and published by Niantic in 2016 in collaboration with Nintendo and The Pokémon Company. It is a free mobile game using GPS to locate, capture, train, and battle virtual Pokémon. By 2017, the app was downloaded over 650 million times, and Trainers collectively covered 15.8 billion kilometers — roughly the distance from Earth past the edge of the solar system (*The Niantic Story*, n.d.). The app has been said to promote physical activity, and help local businesses grow due to increased foot traffic. Pokémon Go contributes to AI advancement as a whole and can help other navigation systems like Apple Maps for safer travel. Yet, if Niantic collected user data illegally or inconspicuously, then it could not only violate user privacy but more importantly user trust.

After establishing a game account, players create and customize their own avatars. Once created, an avatar is displayed on a map based on the player's geographical location. Features on the map include 'PokéStops' and 'Pokémon Gyms'. These PokéStops can be equipped with items called 'Lure Modules', which attract additional wild, and occasionally rare, Pokémon (Ungureanu, 2016). Players must physically travel to explore the game's map and visit PokéStops and gyms. The game is regularly updated with new Pokémon, and as of October 2024 there are 871 Pokémon in the game (including regional varieties) out of a total 1025 within the complete Pokémon franchise (Michael, 2024).

When you look at a familiar type of structure— whether it’s a church, a statue, or a town square, it’s fairly easy to imagine what it might look like from other angles, even if you haven’t seen it from all sides. As humans, we have “spatial understanding” which means we can fill in these details based on countless similar scenes we’ve encountered before. But for machines, this task is extraordinarily difficult. Even the most advanced AI models today struggle to visualize and infer missing parts of a scene, or to imagine a place from a new angle. Spatial intelligence is the next frontier of AI models (*Building a Large Geospatial Model to Achieve Spatial Intelligence*, n.d.)

Niantic has announced that it’s building a new Large Geospatial Model (“LGM”) that combines millions of scans taken from the smartphones of players of Pokémon Go and other Niantic products. This AI model could allow computers and robots to understand and interact with the world in new ways. Scans of the world from Pokémon Go and Ingress (a similar game) are the backbone of Niantic’s AI model, which aims to navigate the world like ChatGPT spits out text (Davis, 2024). In a blog by Niantic, the company says this scanning feature is completely optional— people must visit a specific publicly-accessible location and click to scan. Merely walking around playing the company’s games does not train an AI model. (*Building a Large Geospatial Model to Achieve Spatial Intelligence*, n.d.). Niantic has already mapped 10 million locations globally.

When you install Pokémon Go, you are allowing the app to access data such as Identity, Contacts, Location (Precise and Approximate), Photos/Media/Files (the ability to modify, delete, or read contents of USB storage), Storage, Camera, and many others. Based on your device and information, the game theoretically should have no problem interpreting where you are, where you were, what route was taken in between locations, when you were at such locations, how long it took to get to each location, what you are currently and previously looking at, what you look like, and what files are on your device and its contents thereof (Bryan Lunduke, 2016).

Before Niantic Labs, CEO John Hanke ran Google's Geo division, responsible for nearly everything locational at a time when the company was turning into much more, expanding away from cataloging the web and towards cataloging every city block on the planet. Hanke landed at Google after his wildly popular CIA-funded company—Keyhole, which collected geographic imagery, was acquired in 2004 and relaunched as Google Earth in 2005 (Biddle & Biddle, 2016). At an event held by the investigative journalism group Bellingcat on November 14, 2024—Niantic's Senior Vice President of Engineering Brian McClendon, formerly the co-creator of Google Earth, Street View, and Google Maps was asked by Bellingcat's open source analyst (and ex-British Army officer Nick Waters) said that LGMs would be "unbelievably useful" to the military and asked if McClendon could see governments and militaries purchase LGMs from Niantic. "I could definitely see it," McClendon said. "I think the question is would there be anything that they would do with it that would be outside of what a consumer or a Bellingcat want to do with it. If the use case is identical then that seems completely fine. If the use case is specific to the military and adds amplitude to war, then that's obviously an issue." (Sheehan, 2024).

This type of data collection is unique because it is taken from a pedestrian perspective from locations inaccessible to cars, such as the Google mapping vehicles (Maiberg, 2024). This is an ethical issue that users should be aware of. Not only for use of Pokémon Go, but for anything requiring access to a mobile device. McClendon's comment basically suggests that all the individual data collected by users and players, to a degree, could be sold to practically any government agency. Your personal data and experience can help them out in a military aspect without even asking permission (Sheehan, 2024). This has privacy concerns written all over it. Users who simply wanted to download a fun and interactive game, are now faced with the ethical dilemma of their data being used for potentially nefarious reasons. A LGM like this could have dozens of military applications, particularly for urban combat.

While the AI models are still far from such capabilities, this is a possible end-use for the data. This type of data collection is revolutionary and very well designed and conceived. Google was gathering geographic information at its own expense, yet Niantic has gathered this information basically for free and with incredible accuracy whilst being disguised as a fun interactive game, aiming for physical movement and connectedness towards individuals. If there was a specific area Niantic would like explored or navigated, there would be a Pokémon placed in that location, enticing users to catch it, and navigate the areas to capture images for use. Players are unknowingly using this app for free geo-navigation, all to create a massive geospatial mapping product to sell to the highest bidder. If there were to be a military application, Nintendo would inherently be collecting your data for the government. Nobody who downloaded Pokémon Go in 2016 could have predicted their data would one day be used for this type of AI product.

This type of data collection is used for an enhanced gameplay experience, whereas location data can be used to capture region-specific Pokémon by providing a sense of freshness and excitement for players in different areas. Another positive impact of being a geo-navigator is health and fitness. The game encourages users to explore their surroundings and increase exercise ergo leading to increased benefits. Pokémon Go also has social implications as well and encourages players to connect and network with other players in the community by training and battling Pokémon together. Yet, one of the most notable issues of the game is privacy and transparency. This can lead to a sense of mistrust and uneasiness as to how their data is truly being used if not handled responsibly. While the game encourages users to explore, there are also concerns about public spaces and safety, where users might trespass private property or gather in numbers at a sensitive location.

This type of collection does contribute overall to AI capabilities, yet one must consider to what extent a user is participating and contributing, and if this contribution is what it seems at face value. If Niantic had mentioned this usage when the app was released, it most likely would not have been so successful. This feeling of mistrust may make users not want to play the game at all, ergo, ceasing Niantic's free data mining system. Niantic may also face repercussions for future projects where users may not want to participate if they know their data is not private. While Pokémon Go and similar games offer unprecedented opportunities for connection and engagement, it also presents challenges related to privacy and misinformation. By considering both positive and negative impacts, we can better understand the broader implications of data collection.

Data Collection and COVID-19

There are several arguments supporting both for and against data collection. This section will highlight the pros of data collection and how stakeholders such as the government can benefit from the use of individual data. For instance, COVID-19 was a pandemic that caused many people worldwide to be infected. Many methods were implemented to track points of contact, personal data, to identify and trace people who were exposed to the virus. According to the "MIT Internet Policy Research Initiative," contact tracking apps helped to "disrupt" infection and transmission chains. This was valuable information at the time because it allowed the government to further investigate the disease as well as increase speed and efficiency for tracing COVID-19 transmission. In the article Thomas Jarzombek, Commissioner Federal Ministry for Economic Affairs and Energy for the Digital Industry and Start-Ups, mentioned the app used in Germany was with respect to the protection of people's data. This shows that the government and other companies can practice use and still be aware of user privacy. He explained that the app used a "..decentralized server and Bluetooth, and was created by Google." This was the plan to have a less invasive approach for people with three important factors. The first is privacy and ensuring that the app is based on proximity and not exact location. Second was design flexibility and making sure it was compatible with all providers and the data being collected aligned with current public health goals. Lastly, integration so that officials could integrate with the manual contacting tracing.

Similarly, during the COVID-19 pandemic, other countries such as Australia and Singapore used contact tracing apps with concerns of user privacy being present. Australia's app known as CovidSafe has federal privacy protections according to the article "Do privacy concerns impact CovidSafe app use?” by Victoria Ticha. The article mentions that approximately seven million people downloaded the app around the time of January 2021, and as a result, 17 close contacts were traced by June. This population is one-third of Australia, with access to the internet. This shows that the use of data and geolocation via Bluetooth was used in a useful way in the midst of an outbreak. In addition, Singapore’s contact tracing app known as TraceTogether worked in a similar fashion by using Bluetooth to help users stay anonymous and protect their privacy. The article “To mitigate the costs of future pandemics, establish a common data space” by Stephanie Chin and Caitlin Chin-Rothmann, supports the idea that collecting user data is valuable, specifically in times like a pandemic. An example stated in the article mentions how in the 2015 Ebola epidemic and COVID-19 pandemic sharing genomic sequencing data in public data centers was valuable. It is supported by international policies such as the 1996 Bermuda Principles and the 2010 Nayoga Protocol. Furthermore, there was a pre-covid push to make data more available. The OPEN Government Data Act required that federal agencies post their data online, information that is now available on the federal website data.gov. User data collection is beneficial because it allows the government and companies to identify public outbreaks faster and more reliably if there is more data available. In addition to creating specialized treatments in times of emergency, since there is an abundance of epidemiology, genome sequencing, etc data accessible.

Amongst the concerns of user privacy and data collection are privacy and trust for individuals. In the same article, “MIT Internet Policy Research Initiative,” Louis Ivers (Executive Director, Center for Global Health, Massachusetts General Hospital, Associate Professor of Medicine & Global Health and Social Medicine, Harvard Medical School, and lead Senior Medical Advisor on the PACT team), says that “trust in an app is not all that is needed” and that is should be apart of the whole process. This highlights the importance of transparency and how people should feel when it comes to their data. People want to be aware of the “trade-off” that is happening, in exchange for their data, and what service is being provided.

Although the article by Victoria Ticha states the CovidSafe app was rapidly downloaded, there were still fears among the population. Experts were concerned about the use of user data beyond COVID-19 tracing. There was a fear that the U.S. government would gain access to the data, which shows that people do not have full trust in how their data is being utilized. In addition to this, the article “To mitigate the costs of future pandemics, establish a common data space” mentioned above, speaks about the challenge of creating a shared data space. It may cause concerns if done incorrectly since it is a compiled place of individual data.

Security is an issue along with disparities in data from different methods. Further heightening the concerns of people. Moreover the Per Research Center article “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information” by Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner takes an in-depth look at why the majority of people believe that their data is less secure now and are consistently tracked. “Six in ten U.S. adults say they do not think it is possible to go through daily life *without having data collected about them* by companies or the government.” (Auxier, et al.) These adults believe that although data driven products can help people, the risks outweigh the benefits. The article shows 81% believe this about companies, and 66% about the government regarding data collection. Also, 79% of Americans admit that they don’t believe companies will admit mistakes if their data is misused or mishandled. This is a concern in people allowing the use of their data because they are unsure of the long term uses. This relates to many crimes that have occurred against them. The survey shows that three in ten Americans (28%) have suffered from some form of fraud such as identity theft within the past 12 months, fraudulent credit or debit card charges, names used for loans, and even social media hacking.

Many examples of data misuse begin with employees or third party vendors, where the points of concern are for individuals. Data is vulnerable the moment it transfers away from the "secure perimeter" since it can be transferred to less intensive security features. For instance, in 2020 cyber criminals hacked 5.2 million Marriott guest records according to the article "7 Examples of Data Misuse in the Modern World" by Invisibly. In this attack they were able to access personal information, customer contacts, birthdays, etc. It was successful because employer credentials were accessed via a third party application. Another example of data misuse occurred in 2018 and involves Facebook and Cambridge Analytica (UK political consulting firm). The firm used personal data, which Facebook initially obtained from a third party with the intention of academic research. However, Cambridge Analytica had gained access to data from 87 million Facebook users, many who did consent to permission. Within a couple months, the UK firm went bankrupt while Facebook paid a hefty $5 billion fine to the FTC (Federal Trade Commission).

Lastly, a data breach in 2015 occurred at Morgan Stanley from an employee's wrongdoing. An advisor moving to a new company attempted to take approximately 730,000 accounts to a competitor. It was data of 900 users that hackers stole from the employee's home character. The examples mentioned above show why people have concerns about their data. Through the case of Marriot it was a lack of awareness from the company that allowed sensitive information to be compromised. Facebook provided data that was not consented to in the first place, confirming the data above that companies will not willingly admit their misuse unless caught. In the Morgan Stanley data breach, an employee was able to misuse and access company data which should have protective barriers to prevent it from happening and keep client trust. The risks of data misuse can cause negative financial impacts on companies but more importantly breaks the trust between company and audience. People are worried about how their data is misused because according to past cases and data, it is safe to assume that companies allow data access without our knowledge.

Data Collection and Law Enforcement

The usage of data collection is also highly debated when it comes to its legal implications such as its application in law enforcement. Back in 2011, a man named Timothy Carpenter was arrested because he was a part of string robberies that happened in Detroit Michigan. During the initial arrest, four suspects were arrested and Carpenter was not one of the four. After confessing, one of the four gave their phone to the FBI for investigation where the FBI reviewed made calls during the time of the robberies. The historical cell site data found on the arrestee's phone confirmed that Timothy Carpenter was a part of the operations. In *United States vs Carpenter,* Carpenter appealed "his conviction and sentence to the United States Court of Appeals for the Sixth Circuit, arguing that the CSLI evidence used against him should be suppressed because the police had not obtained a warrant pertaining to **his** CSLI records." The Court upheld the conviction based on the Smith v Maryland precedent stating that Carpenter voluntarily used telephone networks and his data is no exception to be private. This conviction was upheld all the way up to the Supreme Court because the FBI agents were acting in good faith and it was within the laws of the time. There are still debates on the decision, with Justice Samuel Alito stating: "I fear that today's decision will do far more harm than good. The Court's reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely." The Supreme Court also realized the contradiction with *United States v Jones*, where “the Court had ruled that GPS tracking could constitute a search under the Fourth Amendment as a violation of a person's reasonable expectation of privacy” GPS and CSLI both track an individual’s past movement, yet the ruling differed despite the fact that CSLI data presents a greater privacy risk with the prevalence of cellphones. Despite the concerns, if data collection was not used here, part of the group could have remained hidden and waited for another opportunity to strike. Data collection enabled the FBI to find the criminals and ensure community safety.

Another example would be with Andrew Grantt Conlyn and the death of his friend, Colton Hassut. Back in March of 2017, Conlyn was a passenger in Colton Hassut’s car. Hassut was driving over 100 miles per hour in a 35 miles per hour zone, occasionally swerving into the other lane to pass slower cars. At some point, Hassut crashed the car and Conlyn blacked out. When Conlyn became conscious again, the car was on fire and Hassut was no longer there. Luckily, a random good samaritan passed by and dragged Conlyn out of the car. Hassut’s body was found in some bushes nearby since he was ejected after the crash. Conlyn and the cops who arrived later on the scene never learned the man’s name. In November 2019, Conlyn was arrested for vehicular manslaughter because the court believed he was the one driving since his blood was found on both the passenger and driver side, the passenger door was blocked by a tree, and Hassut’s body was not in the car. Despite body-cam footage of the good samaritan saying he pulled Conlyn from the passenger side, the evidence contradicted the statement, leading to the footage holding little to no weight. After losing a civil lawsuit and facing up to 15 years in jail, Conlyn and his lawyers were desperately searching for the man that saved him. They asked local news stations for help, searched the local area and social media to no avail. One day, one of Conlyn’s lawyer, Patrick Bailey, found out about Clearview AI, a company that matches facial recognition data in order to aid law enforcement. In a few seconds, they were able to find the exact guy at a club in Tampa. According to the New York Times, “the prosecutor in the case deposed Mr. Ramirez on a Thursday afternoon in July, and dropped the vehicular homicide case against Mr. Conlyn that evening.” Clearview AI saved an innocent man from 15 years of wrongful imprisonment within seconds. Even though other countries such as Canada, Australia, Britain, France, Italy and Greece have banned Clearview AI, we can see the clear benefits and potential of data collection in law enforcement.

In terms of national security, data collection is used for counterterrorism efforts and to enhance national security. According to History.com, prior to 9/11, the US government was mainly concerned about international terrorism rather than domestic. This was true, until April of 1995 when the Oklahoma city bombing occurred. This was significant because this attack was coordinated by American citizens, raising concerns regarding domestic terrorism and the potential need to monitor citizens more. In April 1996, Clinton wanted to pass the “Antiterrorism and Effective Death Penalty Act of 1996,” giving the government more surveillance power, but was ultimately refused because many believed it to be unconstitutional. This changed after 9/11, when they passed the Patriot Act. This act enhanced law enforcement and the surveillance power of the federal government. This included things such as expanded surveillance, intelligence sharing, stricter penalties, streamlined warrant processes, and support for victims and responders. So after it was passed, did it prevent terrorism? That's still up for debate depending on where someone gets the information. A Washington Post article stated that the Department of Justice admitted to not being able to appoint a single one of their success, of preventing any terrorism, to the Patriot Act. Yet, a 2012 report, from the conservative Heritage Foundation, says 47 out of 50 attacks were prevented directly due to the powers granted by the Patriot Act to law enforcement and intelligence agencies. The public is concerned; "they claim they could be spied on without due process, their homes would be searched without consent, and it increases the risk of ordinary citizens being accused of crimes without just cause." (History.com) The federal government ensured that there are safeguards put in place in order to protect American citizens' rights. Which is funny because "some parts of the law were found illegal by the Courts. For instance, in 2015 the United States of Appeals for the Second Circuit found Section 215 of the Patriot Act could not be used to validate the bulk collection of Americans' phone records." In order to help prevent infringing citizens' rights any further, in 2015, Obama signed the Freedom Act. This ended bulk collection of all records and allowed challenges to national security letter gag orders. The act also "required better transparency and more information sharing between the United States Foreign Intelligence Surveillance Court and the American people." The freedom act allowed for tracking of suspected foreign terrorists upon U.S. entry for 72 hours, imposed stricter penalties for supporting terrorist organizations, and permitted emergency bulk data collection. Balancing national security and an individual's right to privacy is very difficult. What would be considered too far? What if it isn't far enough? Most believe federal surveillance is going too far and the NSA's creation of the PRISM program did not help.

Back in 2017, after the passage of the Protect America Act, the Bush administration began the PRISM program. This program was discovered when it was leaked by a NSA contractor by the name of Edward Snowden. Snowden wanted to warn the public of the mass data collection that happens behind the public's eye, describing it as "dangerous" and "criminal." According to wikipedia, PRISM "collects stored internet communications based on demands made to internet companies such as Google LLC and Apple under Section 702 of the FISA Amendments Act of 2008 to turn over any data that match court-approved search terms. Among other things, the NSA can use these PRISM requests to target communications that were encrypted when they traveled across the internet backbone, to focus on stored data that telecommunication filtering systems discarded earlier,and to get data that is easier to handle." US government officials claim the program is used for counterterrorism efforts and to enhance our national security, defending the usage saying that, without a warrant, it can't be used on domestic targets and is monitored by all three branches of government. Companies such as Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, AOL, Skype and Apple have participated in this program, providing data. Domestically, this has raised public concerns because almost everyone on this planet has an account on one or more of these companies. It's disturbing knowing that the everyday person's calling and texting habits are a part of the NSA's database. Communication is typically routed through the least expensive way rather than the most direct route so much of the world's electronic communication passes through the United States since most of the internet's infrastructure is based in the US. This has allowed the FBI to intercept foreign communication.

This collection has supported the US's counterterrorism efforts and enhanced our national security, but other countries are fearful and against it. They claim the NSA is participating in dangerous and criminal "activity by 'hacking' civilian infrastructure networks in other countries such as ‘universities, hospitals, and private businesses’, and alleged that compliance offered only very limited restrictive effect on mass data collection practices (including of Americans) since restrictions ‘are policy-based, not technically based, and can change at any time.’” (Wikipedia) Incidents such as the boston marathon bombing have led to the discrediting of the PRISM program. Although Tamerlan Tsarnaev “had visited the Al Qaeda-affiliated magazine website, Inspire, and even though Russian intelligence officials had raised concerns with U.S. intelligence officials about Tamerlan Tsarnaev, PRISM did not prevent him from carrying out the Boston attacks.” (Wikipedia) If the main benefit of this program is to help with national security, how could they have missed such a thing?

Black Lives Matter (BLM) Protest Surveillance

Social media's rise has influenced the way people organize, protest, and communicate. Also, it provided governments with new tools for monitoring public behavior, especially during times of social unrest. This section will explore the event of government surveillance of BLM protests, while stating the pros and cons of social media surveillance.

The BLM movement surfaced in 2013 in response to racism and police violence. This movement gained a lot of awareness after many high-profile incidents, such as the deaths of George Floyd, Oluwatoyin Salau, and Breonna Taylor. Social media became an important platform in terms of organizing protests, raising awareness, and sharing updates as they happen. As a result, the government began to keep an eye on social media platforms after recognizing the usefulness these digital tools could be for tracking protests, spotting possible threats, and maintaining public order.

During BLM protests, the government has used a variety of surveillance strategies, such as monitoring geolocation data, social media hashtags, along with live video streaming. To analyze social media behavior, agencies such as the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and local police agencies have used modern techniques. They collected and analyzed information about protesters and organizers using technologies like drones, facial recognition software, and data tools like Geofeedia.

A key argument in favor of social media surveillance is the potential in enhancing public safety. By monitoring social media, law enforcement can recognize the potential threats, such as illegal activities, which allows them to respond ahead of time. For example, during a BLM protest, authorities were able to detect individuals who had the intentions to incite violence, which helped prevent riots and property damage.

Another key benefit is that social media surveillance provides law enforcement real-time situational awareness. This benefit is valuable during large scale protests, where situations can change very quickly. Social media posts, live videos, and real-time updates allow authorities to gauge the crowd's movements based on the level of tension, enabling them to allocate resources more effectively and protect both protesters and the public. With the information they have, police departments are able to assign personnel in high priority areas, such as locations that they can assume may become violent. Social media is an essential tool to ensure that protests can remain peaceful and that threats can be taken care of rapidly.

The role in evidence collection for criminal investigations is another advantage of social media surveillance. After the BLM protests, law enforcement is able to use publicly available content, such as photos and videos to identify individuals who are involved in criminal activities. For example, if a person were to engage in vandalism or violence in a protest, their actions can be taken and shared on platforms such as Facebook and Instagram. These evidence can be used to take legal actions against offenders, ensuring that offenders face consequences for their actions. By utilizing social media as an investigatory tool, law enforcement can make their investigations more efficient and comprehensive.

Despite the many benefits, there are drawbacks to social media surveillance, such as concerns about privacy and civil liberties. The concern that people have is the violation of privacy as many individuals do not expect their social media posts to be under government surveillance. Even though social media platforms are public spaces, users like to share their personal thoughts and opinions with the intention to communicate their feelings to a community, and not be monitored by government agencies. When law enforcement observes these platforms, people may feel like it is a violation of their personal privacy, especially to those that didn't commit any criminal activity.

In addition, social media surveillance has the potential for abuse. Governments and law enforcement agencies may misuse surveillance tools by targeting individuals who are exercising their constitutional rights, instead of legitimate security threats. For instance, during the 2020 BLM protests, some law enforcement agencies were accused of using social media data to observe peaceful protestors instead of those who are involved with criminal activity. There were cases when protesters were flagged as potential threats even though they were exercising their right, making the surveillance not only over the top, but unjust. Also, surveillance tools such as the facial recognition software raises concerns when it comes to false identifications and racial profiling, making existing biases in law enforcement practices worse.

A case that demonstrates the risks of surveillance during the BLM movement is *Williams v. San Francisco*. The lawsuit was filed on October 27, 2020 by BLM activists, which includes the lead plaintiff Hope Williams who accuses the San Francisco Police Department (SFPD) of accessing a private surveillance camera network that was managed by the Union Square Business Improvement District unlawfully. The plaintiffs made an argument that SFPD used over 400 cameras to monitor BLM protests, which violates San Francisco's Surveillance Technology Ordinance, which means that they would need to disclose to the public their intent, and obtain a formal approval. This case highlights the risk of the government's abuse of power, since the peaceful protesters were being monitored without their consent. Overall, the lawsuit showcased the tension between maintaining public order and protecting civil liberties during large-scale protests.

Ultimately, even though social media surveillance is a valuable tool for enhancing public safety and investigating crimes, it can pose a risk towards privacy, civil liberties, and public trust as well. Balancing these conflicting interests would require clear laws and proper oversight, while upholding democratic principles. As technology continues to evolve, careful attention will be needed to make sure that surveillance practices are beneficial to the public without violating their basic rights.

The Equifax Data Breach of 2017: Ethical and Financial Implications

In this new era, the rise of technology has transformed how personal data is collected, stored, and used which has created ethical dilemmas. The collection of data is an essential part of any business, government, or even individual as every click leaves a digital footprint that can be used to optimize innovation if used correctly. There are mainly two kinds of data collection methods which are General and Biometric data collection. General data collection gathers and deals with information such as users' browsing habits, purchase history, and other personal interactions that users might make through websites or any other applications. Whereas biometric data collection deals with unique physical characters of individuals such as face ID, retina, fingerprint, or even voice pattern where data is collected through devices and is stored in the cloud. Although this data offers great benefits such as better security, privacy, and personalized services it also raises ethical concerns that increases the risk of data breaches and the potential misuse of sensitive information.

Equifax, one of the largest credit reporting agencies in the United States, became the center of a major data breach that exposed the financial and personal information of nearly 150 million consumers. This situation took place in 2017 when the company failed to address a known vulnerability in its database system despite the availability of a security patch. The delay in disclosing the breach introduces a public outage as well as raises serious ethical concerns from Equifax in terms of data privacy and transparency. In 2019 the company agreed to pay around $650 million in terms of the settlement with the Federal Trade Commission as well as with the Consumer Financial Protection Bureau, The consequences and ethical implications on Equifax data-related concerns are supported by various insights and analyses.

The breach was caused due to a vulnerability in the Apache Strut framework which is a web-based application. Although the web-based application launched a patch for the vulnerability in March 2017 Equifax had failed to fix the known vulnerability promptly where this negligence allowed hackers to exploit the flaws and access sensitive information including consumer's social security numbers, date of birth, and credit card information. This settlement case was a landmark in data breach showcasing accountability and exposing systemic issues that lie in the data security systems. Many people or critics also believe that the settlement amount was insufficient given the number of individuals affected and other long-term risks associated with data breaches and the obligation to inform about the situation promptly. These data are highly sensitive and cannot to easily changed like passwords increasing perpetual vulnerability to identity theft and fraud (Kovacs,2019)

The company has highlighted one of the critical gaps in data security obligations while handling sensitive information which are meant to be safeguarded from unauthorized access and misuse. These responsibilities of Equifax are more about its ethical values rather than other aspects that highly reflect the trust of consumers towards the institution. One of the primary obligations of Equifax is to implement security measures that include regular security updates, vulnerability assessment, and adopting any encryption method but due to issues in corporate governance or not prioritizing cybersecurity Equifax failed to maintain user-client agreement. At the same time, other obligations include handling incident protocol where companies usually act swiftly in the event of a breach, minimizing harm that affects any individuals. Incident handling includes immediate disclosure of the breach, transparent communication, and the impact of the breach. In this case, Equifax delayed prioritizing incident handling leading to a data breach and undermining public trust which has a higher consequence for consumers. Similarly, Equifax failed to comply with data protection regulations such as the California consumer privacy act (CCPA), which sets a standard for data security and consumer rights.

The Equifax case provided us with detailed information and serious issues underlying data security, which highly emphasize the need for taking a more active approach to safeguarding sensitive information. This data breach also forced regulatory bodies to modify and change data protection laws. For example, various states have introduced policies that notify consumers within a certain period of a data breach. Similarly, the breach has also raised a concern regarding the loss of privacy in the digital era and highlights the risk of data storage and the challenges of managing sensitive consumer information. In addition to the fallout of financial and social reputation, Equifax has also faced numerous lawsuits from consumers and the attorney general which highlights the company's failure to protect personal data and lack of adequate response to the data breach.

Overall the 2017 Equifax breach has caused a negative impact on all stakeholders and caused significant harm to consumers' privacy. Its failure to protect consumers and delayed handling of incidents led the company to lose its reputation. Most importantly this breach has shown the importance of stronger privacy protection and better cyber security practices to safeguard personal information. Learning from the Equifax class action lawsuit businesses can focus more on creating a safer digital ecosystem that prioritizes the protection of personal information as well as setting priority to inform consumers regarding changes that occur which are related to consumer’s personal data.

Meta’s $1.4B Unauthorized Biometric Data Collection Settlement

Meta, previously known as Facebook is a global leader in the social media world as well as in the technological field. There is a high chance that you have created an account on one of their platforms such as Facebook, Instagram, and WhatsApp. Meta strives to connect people and ultimately improve the digital experience. This can be seen from their mission statement “Build the future of human connection and the technology that makes it possible.” However, this ambition has often clashed with ethical and legal concerns about user privacy, especially regarding data collection techniques. One such example is Meta’s fairly recent $1.4 billion settlement over their unauthorized capture of the personal biometric data of millions of Texans under Illinois’ Biometric Information Privacy Act (BIPA). This particular case demonstrates the ethical challenges in balancing technical advancement with user privacy because while the collection of biometric data might enhance user experiences, it also raises serious questions regarding consent, the misuse of data, and any potential privacy violations.

On February 14, 2022, the State of Texas filed a lawsuit, alleging that “Meta violated the Texas Capture or Use of Biometric Identifier Act (“CUBI”) and the Texas Deceptive Trade Practices-Consumer Protection Act (“DTPA”) by building an artificial intelligence empire using Texans’ biometric data without their knowledge or permission.” (*Texas Biometrics Case Highlights Need for Consent: Meta Settles for $1.4 Billion | Insights | Vinson & Elkins LLP*, n.d.). It claimed that Meta collected biometric identifiers from images and videos that users and even non-users posted to its social media platforms and exploited this kind of data to train its facial recognition program, “DeepFace”, in which they did not notify or ask for consent from the users whose biometric data was collected from. The lawsuit argued that these practices jeopardized Texan civilians' safety and privacy because biometric data is permanent and susceptible to misuse. In terms of Texas' Capture or Use of Biometric Identifier Act ("CUBI") state law, "it prohibits a person from capturing an individual's biometric identifiers (retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry) for a commercial purpose unless that person informs the individual and obtains the individual's consent prior to the capture." (*Biometric Identifier Act | Office of the Attorney General*, n.d.). And the Texas Deceptive Trade Practices-Consumer Protection Act ("DTPA") prohibits deceptive practices in trade or commerce (*Consumer Rights | Office of the Attorney General*, n.d.).

Meta's biometric data collection can be justified by looking through different lenses or rather an iceberg. For example, on the tip of the iceberg in terms of benefits, one could argue that biometric data collection can enhance user experience on social media platforms. In this case, Meta's facial recognition program, DeepFake, has a strong potential to improve user experience on its own platforms like Facebook. Having the ability to automatically tag photos and suggest friends can save their users a lot of time and effort. A use case for this would be to think about scrolling through the thousands of photos on one's mobile device, with each photo instantly labeled with the names of friends, family, or acquaintances. Through a social lens, this sheer convenience can really enhance one's social life and lead to a more personalized online experience.

However, this "Tag Suggestions" feature was discontinued in 2021, with Meta claiming that they deleted over 1 billion individual facial recognition data (Motley, 2024). If we take a step down on the iceberg or simply look beyond social media, we can argue that if Meta conducted such practice ethically and responsibly, then DeepFake, or facial recognition technology, in general, can be extremely effective for advanced security applications. Take a look at human trafficking as a whole. According to the U.S. Bureau of Justice Statistics, " A total of 1,912 persons were referred to U.S. attorneys for human trafficking offenses in fiscal year 2022, a 26% increase from the 1,519 persons referred in 2012." (*Human Trafficking Data Collection Activities, 2024 | Bureau of Justice Statistics*, n.d.). In other words, human trafficking is increasing every year and a majority of victims are never found. If facial recognition technology improves at the ideal rate, law enforcement could identify not only victims of human trafficking but also criminal investigations. Aside from law enforcement security, biometric authentication has the potential to take over traditional passwords as well, reducing the risks of fraud and unauthorized access. This is paramount in healthcare and financial transactions, where vigorous authentication security is essential. Looking beyond transaction applications is also noteworthy. We must not forget that biometric data can serve as an instrument in AI advancement. Going back to healthcare, AI has the potential to use these biometric data to turn them into patterns to assist in diagnosing diseases. Even in psychology, would it not be far-fetched to argue that facial recognition can be used to study human behavior and emotions, producing valuable insights?

Despite the numerous benefits, Meta's biometric data collection practice raises serious ethical concerns, especially regarding privacy. To address the elephant in the room, Meta's lack of informed consent is a huge concern. Collecting biometric data without adequately informing users or even non-users (people that can be seen in the background of a photo), means that Meta basically dug their own grave when it comes to retaining user trust. This practice not only violated legal standards but also ignored individual's rights to control their personal information, in this case, it is the action of sharing one’s pictures on the platform. Let’s not forget that biometric data is quite sensitive because it is permanent; unlike your traditional typed passwords, it cannot be changed once compromised. A data breach like this, where the corporation has an obligation to protect its users, could result in long-term harm, such as fraud or identity theft.

Additionally, we cannot exclude the fact that bias and discrimination do exist in facial recognition technology. There was a case, where a black Uber Eats driver was unable to go through a facial recognition scan which prevented him from accessing the app to secure work shifts (McCallum, 2024). Studies have demonstrated that these algorithms can be less accurate in recognizing people of color, resulting in discrimination. If this is applied to law enforcement security, then the potential of unlawful arrests would be fairly high. Financially, developing any sort of biometric technology can be quite expensive. The cost to develop a “Facial Recognition System” can range from $40,000 to $150,000, influenced by factors like project complexity, team expertise, feature integration, platform selection, and geographical location” (Singh & Shivang, 2024). And if you consider the financial risks associated with non-compliance with privacy regulations in conjunction with an already expensive tech development, then one should think twice about their ethical practices in data management.

Biometric Data Collection and Sephora

Finally, the digital age has revolutionized how retail businesses interact with consumers, specifically personalization becoming a key component of marketing strategies. However, the collection and use of consumer data, especially biometric data, have raised significant ethical concerns for all. Sephora is a prominent beauty retailer that became a focal point in the debate when the company faced legal scrutiny over its alleged misuse of biometric data. This data includes facial recognition and other sensitive identifiers, all increasingly used to enhance customer experiences. Sephora employed such technology for virtual try-on features and personalized recommendations. However, the company faced accusations of collecting and sharing biometric data without adequate transparency or customer consent, allegedly violating California's Consumer Privacy Act (CCPA).

In 2022 Sephora was sued by the California Attorney General Rob Bonta under the California Consumer Privacy Act (CCPA). Rob Bonta was the attorney general in this case who prior to the lawsuit “warned more than 100 companies that they were out of compliance and sent more than a dozen new notices on Wednesday. The “vast majority” complied, he said, but not Sephora” (Thompson). The lawsuit alleged that Sephora failed to disclose to customers that it was selling their data to third parties, including data collected through biometric tools. These third parties were then able to create profiles with the information they gathered from tracking and monitoring Sephora customers with unrelated information such as the device they use, the vitamins they purchase, and even their precise location. The claim highlighted that Sephora's partnerships with advertising and analytics firms may have involved sharing sensitive information without proper consent or transparency. As a result, Sephora was required to pay 1.2 million dollars in a settlement to resolve the allegations. As part of the agreement, Sephora was also required to improve transparency regarding its data collection and sharing practices, implement mechanisms allowing consumers to opt out of the sale of their data, and provide regular reports to ensure compliance with the CCPA. (Bonta). This situation highlights an ethical conflict between innovation and privacy protection. Furthermore, it illustrates the ongoing efforts to enforce CCPA.

Sephora's use of biometric technology can be justified by its ability to enhance the customer experience and drive innovation in a highly competitive industry. By incorporating tools like virtual try-on features, Sephora allowed customers to visualize how products would look on their skin tone or facial features without needing to physically test the products. This not only saved time but also provided a personalized shopping experience, which has become essential in the beauty industry. Furthermore, leveraging such technology-enabled Sephora to maintain its position as a market leader by offering innovative solutions that catered to modern consumer demands. In addition to the benefits for consumers, the technology helped Sephora refine its marketing strategies and improve customer engagement, ultimately boosting sales. Another consideration is the complexity of regulatory compliance in an evolving legal landscape. Privacy laws, such as the California Consumer Privacy Act (CCPA), are relatively new and require businesses to adapt quickly to remain compliant. The allegations against Sephora could be viewed as a result of the company grappling with the intricacies of these emerging laws rather than a deliberate intent to violate consumer rights. This highlights a broader challenge businesses face in keeping up with fast-paced regulatory changes while continuing to innovate and deliver value to their customers.

On the other hand, Sephora's actions raise serious ethical concerns regarding consumer trust and privacy. The company's alleged failure to disclose the extent of its data collection and sharing practices represents a significant breach of trust. Customers expect transparency and accountability when providing their sensitive information, and Sephora's lack of clarity in its practices undermined this fundamental expectation. Moreover, biometric data is highly sensitive, and its misuse poses significant risks, including identity theft and potential surveillance. By not implementing sufficient safeguards or obtaining explicit consent, Sephora failed to adequately protect its customers. Instead, the company chose the prioritization of profit over privacy and safety. From an ethical perspective, businesses have a responsibility to uphold consumer rights, even in the absence of regulations. While the law might allow certain actions, ethical business practices demand higher standards, especially in the digital age where data privacy is a growing concern. Sephora's alleged disregard for providing opt-out mechanisms and its inadequate communication with customers reflect a lapse in its ethical obligations. Companies like Sephora must consider the broader implications of their actions, as failing to respect consumer autonomy can have lasting negative impacts on both their reputation and the trustworthiness of the industry as a whole.

Overall, the ethical dilemma presented by Sephora's biometric data practices underscores the balance between technological innovation and the fundamental need to protect consumer privacy. While advancements like virtual try-on tools and personalized recommendations offer significant advantages in enhancing customer experiences and driving business growth, they cannot come at the expense of individual rights, trust, and safety. Sephora's case serves as a reminder of the ethical responsibilities companies must uphold in an era where data privacy concerns are critical. This scandal highlights the risks of inadequate transparency and consent along with the broader implications of prioritizing profits over privacy. As businesses across industries increasingly adopt advanced technologies, they must strive for compliance with evolving regulations and proactively commit to ethical practices that respect consumer autonomy. The Sephora case illustrates the consequences of failing to address these issues and offers a critical lesson for companies seeking to navigate the complexities of the digital age responsibly. Ultimately, innovation and consumer protection are not mutually exclusive. Companies that successfully integrate both will not only thrive but also contribute to a more ethical and sustainable future for digital commerce.

Overall Summary

The rapid expansion of digital technologies has fueled a heated debate about data collection. Supporters argue that it offers substantial benefits, particularly in public health and technological innovation. However, there are critics that highlight significant risks, particularly regarding privacy and trust.

Data collection supporters such as the government highlight how essential it is in addressing public health challenges and driving innovation. During the COVID-19 pandemic, contact tracing apps became vital tools for controlling the spread of viruses. Countries such as Germany, Australia, and Singapore utilized these apps to identify and notify individuals who were affected in an attempt to break the chain of transmission. The benefits from collecting user data include predicting future outbreaks faster and creating treatments. Having information available helps officials meet public health goals. However, concerns from people are reasonable in regards to how their data will be used long term. Many individuals have suffered from fraudulent events due to their information being on unsecure servers or lack of company awareness. Other examples such as Facebook sharing information without the consent of users to a third party firm contribute to public concern. Millions of users' data was shared without their knowledge. This shows how distrust forms based on past events. While there are benefits to collecting data, companies and the government must ensure there is full transparency with the public. Those in support must make it clear what the trade off is between using people's data and the benefit obtained.

From Apple's Face ID, revolutionizing device security, to platforms like Spotify using data to personalize content, companies are constantly innovating in order to offer the best versions of their product and services, oftentimes leveraging data collection. However, data collection has also raised ethical concerns, such as the lawsuit against Amazon Alexa for unauthorized storage of children’s voice and location data. Enhancing user experiences and security also poses potential violations of user privacy.

Issues regarding the use of data collection for law enforcement, national security, and privacy are still hot in debate. Even if people view data collection as unethical, cases such as *United States v. Carpenter* proves data tracking and collection can aid in capturing criminals. Similarly, in Andrew Conlyn’s vehicular manslaughter case, Clearview AI's facial recognition technology saved a man from being wrongfully imprisoned. On a broader scale, national security measures like the Patriot Act and PRISM program are still criticized for infringing on individual privacy despite its purpose of countering terrorism.

Social media surveillance played a significant role during the BLM protests, offering both benefits and raising concerns. Government agencies like the FBI and DHS began to monitor social media platforms as it played a major role in planning protests, spreading awareness, and providing updated news. Advanced technology such as drones and facial recognition were used as a surveillance approach, which includes tracking geolocation data, hashtags, and live streams. Supporters argue that social media surveillance improves public safety by identifying the potential threats in real time, while being a resource when it comes to criminal investigations. However, the critics highlight privacy and civil liberties concerns, arguing that the government is violating the individuals privacy and risks by monitoring them, targeting peaceful protestors rather than actual threats. The *Williams v. San Francisco* case is a prime example of these risks as the BLM activists accuse the SFPD for unlawfully using private surveillance to monitor the protests. The incident showcases the tension between maintaining public order and protecting civil rights. As a result, even though social media surveillance is a valuable tool for public safety, the potential risks to privacy and public trust should require clear well defined laws and supervision to make sure the democratic principles are being upheld.

In addition to the ethical challenges of biometric data collection, Meta's $1.4 billion settlement over the unauthorized biometric data collection for personal advantage demonstrates a strong example of the legal and ethical complications associated with biometric data collection. While their facial recognition technology has the potential to enhance user experiences, improve security in multiple aspects such as law enforcement and transactions, and contribute to the growth of AI as a whole, it must be deployed ethically, responsibly, and transparently. Of course, Meta's failure to obtain user consent and its management of sensitive biometric data raised serious concerns about user privacy and security. Overall, this case puts an emphasis on the balance of innovation and ethical norms, ensuring that progress does not come at the expense of individual rights. But as biometric technologies advance even beyond just one company, businesses must consider many risks such as financial and reputational risks.

The Sephora biometric scandal highlights the growing ethical tension between technological innovation and consumer privacy in the digital age. Supporters argue that tools like virtual try-ons provide significant benefits by enhancing customer experiences and driving business growth, offering convenience and personalization that are crucial in competitive markets. These innovations allow companies like Sephora to remain market leaders and cater to modern consumer demands. However, critics point to the company's alleged lack of transparency and potential violations of privacy, raising concerns about the risks associated with sharing sensitive biometric data without proper consent. In Sephora's case, third-party partners allegedly obtained detailed customer data, including biometric information, device usage, purchase history, and even precise location. This data, collected through tracking tools, was reportedly used to create comprehensive consumer profiles without explicit user awareness or agreement. The scandal not only undermined consumer trust but also highlighted broader issues about prioritizing profits over ethical responsibilities. This case illustrates the importance of businesses striking a balance between leveraging advanced technologies and ensuring the protection of consumer rights.

Data collection has significant implications across various fields and usages from Facebook to cosmetics and public health. It enables organizations and businesses to make informed decisions by providing insight into trends, habits, behaviors, and patterns. However, it raises concerns for privacy, security, and transparency, as well as the collection process and storage of personal data. The potential data breaches or misuse if not secured properly are apparent within many industries. Effective data collection can drive innovation and efficiency, but it must be balanced with ethical and legal responsibility to give consumers the ability to access, correct, or delete their information.

References

A&E Television Networks. (2017, December 19). Patriot act - USA, Definition & 2001. History.com. https://www.history.com/topics/21st-century/patriot-act

Auxier, B., & Rainie, L. (2019). Americans and privacy: Concerned, confused, and feeling lack of control over their personal information. Pew Research Center. Retrieved November 19, 2024, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Barak, D. (2021). To mitigate the costs of future pandemics, establish a common data space. Brookings Institution. Retrieved November 19, 2024, https://www.brookings.edu/articles/to-mitigate-the-costs-of-future-pandemics-establish-a-common-data-space/

Bonta, Rob. "Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act." 24 August 2022, https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement.

Cohen, J. (2022, March 30). Amazon's Alexa collects more of your data than any other Smart assistant. PCMAG. https://www.pcmag.com/news/amazons-alexa-collects-more-of-your-data-than-any-other-smart-assistant

Guariglia, Matthew, and Dave Maass. "Williams v. San Francisco." *Electronic Frontier Foundation*, 24 Sep. 2021, www.eff.org/cases/williams-v-san-francisco.

Hill, K. (2022, September 18). Clearview AI, used by police to find criminals, is now in public defenders' hands. The New York Times. https://www.nytimes.com/2022/09/18/technology/facial-recognition-clearview-ai.html

ID Tech. (2017, March 3). Samsung SDS Wins GLOMO Award With Biometrics. ID Tech. https://idtechwire.com/archive/samsung-sds-glomo-biometrics-403034/

Internet Policy Research Initiative. (n.d.). What are the advantages and disadvantages of contact tracing apps? Internet Policy Research Initiative at MIT. Retrieved November 19, 2024, from https://internetpolicy.mit.edu/what-are-the-advantages-and-disadvantages-of-contact-tracing-apps/

Invisibly. (n.d.). Data misuse: 7 examples. Invisibly Blog. Retrieved November 19, 2024, https://www.invisibly.com/learn-blog/data-misuse-7-examples/

OAG. (n.d.). California consumer privacy act (CCPA). Office of the Attorney General. Retrieved November 19, 2024, from https://oag.ca.gov/privacy/ccpa

Press, A. (2023, June 1). Amazon to pay $31 million in fines for Alexa Voice assistant and Ring Camera Privacy Violations. PBS. https://www.pbs.org/newshour/politics/amazon-to-pay-31-million-in-fines-for-alexa-voice-assistant-and-ring-camera-privacy-violations

Samples, Q. (2024, January 17). Fitbit Data insights: Understanding the tracked data. Robots.net. https://robots.net/computing-and-gadgets/wearables/fitbit-data-insights-understanding-the-tracked-data/

Spotify Engineering. (2021, December 17). A look behind blend: The personalized playlist for you...and you. https://engineering.atspotify.com/2021/12/a-look-behind-blend-the-personalized-playlist-for-youand-you/

Team, R. (2024, October 24). 10 advantages and disadvantages of Alexa. Carlos Barraza. https://barrazacarlos.com/advantages-and-disadvantages-of-alexa/

Thompson, Don. "Cosmetics giant Sephora settles customer data privacy lawsuit." 24 August 2022, https://www.pbs.org/newshour/economy/cosmetics-giant-sephora-settles-customer-data-privacy-lawsuit.

Turgeman, A. (2017, October 20). Council post: Iphone X facial recognition: Security, convenience and the user experience. Forbes. https://www.forbes.com/sites/forbestechcouncil/2017/10/20/iphone-x-facial-recognition-security-convenience-and-the-user-experience/

UNSW Newsroom. (2021). Do privacy concerns impact COVIDSafe app use? University of New South Wales. Retrieved November 19, 2024, https://www.unsw.edu.au/newsroom/news/2021/07/do-privacy-concerns-impact-covidsafe-app-use-

Wikimedia Foundation. (2024, November 21). Carpenter v. United States. Wikipedia. https://en.wikipedia.org/wiki/Carpenter_v._United_States

Wikimedia Foundation. (2024a, November 19). Prism. Wikipedia. https://en.wikipedia.org/wiki/PRISM

Texas Biometrics case highlights need for consent: Meta settles for $1.4 billion | Insights | Vinson & Elkins LLP. (n.d.). https://www.velaw.com/insights/texas-biometrics-case-highlights-need-for-consent-meta-settles-for-1-4-billion/

Biometric Identifier Act | Office of the Attorney General. (n.d.). https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint/consumer-privacy-rights/biometric-identifier-act

Consumer Rights | Office of the Attorney General. (n.d.). https://www.texasattorneygeneral.gov/consumer-protection/file-consumer-complaint/consumer-rights

Motley, D. (2024, July 30). Meta to pay Texas $1.4 billion in facial recognition case. *The Texas Tribune*. https://www.texastribune.org/2024/07/30/texas-meta-facebook-biometric-data-settlement/

Human Trafficking Data Collection Activities, 2024 | Bureau of Justice Statistics. (n.d.). Bureau of Justice Statistics. https://bjs.ojp.gov/library/publications/human-trafficking-data-collection-activities-2024

McCallum, B. S. (2024, March 26). *Payout for Uber Eats driver over face scan bias case*. https://www.bbc.com/news/technology-68655429

Singh, R. P., & Shivang. (2024, October 17). *How much does it cost to develop face recognition applications?* Richestsoft. https://richestsoft.com/blog/how-much-does-it-cost-to-develop-face-recognition-applications/

“2020 Black Lives Matter Protests " University Archives " UF Libraries " University of Florida.” *UF Monogram*, universityarchives.uflib.ufl.edu/explore-our-projects/2020-black-lives-matter-protests/#:~:text=On%20May%2025%2C%202020%2C%20White,need%20for%20solidarity%20across%20difference.

255, et al. “Social Media Surveillance by the U.S. Government.” *Brennan Center for Justice*, 30 July 2024, www.brennancenter.org/our-work/research-reports/social-media-surveillance-us-government.

The Niantic story. (n.d.). https://nianticlabs.com/about?hl=en

Ungureanu, H. (2016, July 18). Pokémon GO Tricks To Attract And Catch Pokémon: PokéStop Lure Module vs. Incense. *Tech Times*. https://www.techtimes.com/articles/170319/20160718/pokemon-go-tricks-to-attract-and-catch-pokemon-pokestop-lure-module-vs-incense.htm

Michael. (2024, November 16). *Pokemon GO: A Complete Pokedex (November 2024)*. Game Rant. https://gamerant.com/pokemon-go-a-complete-pokedex-every-pokemon/

Building a large geospatial model to achieve spatial intelligence. (n.d.). https://nianticlabs.com/news/largegeospatialmodel?hl=en

Davis, W. (2024, November 20). Niantic is building a 'geospatial' AI model based on Pokémon Go player data. *The Verge*. https://www.theverge.com/2024/11/19/24300975/niantic-pokemon-go-data-large-geospatial-model

Bryan Lunduke. (2016, July 22). The CIA, NSA and Pokémon go. *Network World*. https://www.networkworld.com/article/953621/the-cia-nsa-and-pokmon-go.html

Biddle, S., & Biddle, S. (2016, August 25). Privacy scandal haunts Pokemon Go's CEO. *The Intercept*. https://theintercept.com/2016/08/09/privacy-scandal-haunts-pokemon-gos-ceo/?utm_source=www.garbageday.email&utm_medium=referral&utm_campaign=right-wing-social-networks-don-t-work

Sheehan, G. (2024, November 26). Niantic Exec comments on governments buying Pokémon GO data. *Bleeding Cool News*. https://bleedingcool.com/games/niantic-exec-comments-on-governments-buying-pokemon-go-data/

Maiberg, E. (2024, November 26). *Pokémon Go data 'Adding amplitude to war is obviously an issue,' Niantic Exec says*. 404 Media. https://www.404media.co/pokemon-go-data-adding-amplitude-to-war-is-obviously-an-issue-niantic-exec-says/

Nytimes.com. (2019, July 22). The New York Times - Breaking News, US News, World News and Videos. https://www.nytimes.com/2019/07/22/business/equifax-settlement.html

Equifax data breach settlement. (2022, December 20). Federal Trade Commission. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement