The Risk of Social Media on Individual Autonomy and Solutions to Fix It

Introduction:

Social media is a popular technology used today, but engaging in it requires accepting the application's data use policies. This often appears under the term 'data privacy policies', though there is not always a clear definition for the meaning of that term, which involves sacrificing autonomy over personal information. This information can include demographic details, how each user engages with the app, what type of content the user prefers, search and message history, etc. Social media companies use this personal information they acquire from users for their own economic benefits. Companies can use user data to customize each user's feed with posts and advertisements to increase user engagement and time-spent on the app. Information can also be sold to third-parties and other organizations outside of the application it was collected in. Common violations of autonomy in social media occur in the use of personal data without being informed, surveillance, and manipulation and coercement practices. By using and exchanging user data on social media without clearly informing the user, companies take advantage of their users by violating their privacy and autonomy.

These infringements can limit and influence the choices individuals make, impacting one's professional and personal life by limiting their freedom of speech and ability to make informed decisions. Having their data shared can cause many issues for users such as harassment and bullying, being presented undesirable or unreliable information, and re-identification. If social media companies are sharing data to outside parties, users could be targeted by individuals which could result in physical or mental harm. When users are seeing customized content without realizing that it was purposely shown to them, it can affect users' beliefs and opinions without them realizing. Sometimes, content is generated for users that can have a negative impact on user well-being, if it is about a topic that the user is sensitive about. If users know that their data is being used and sold to third-parties, they could limit how they interact with the application and what information they choose to share on it, or choose to reshape their identity online.

Social media users are not often aware of these consequences that come with signing up for the platform. This lack of awareness can harm the users itself, because without proper knowledge of what data is being shared, how, and to whom, individuals can't best protect their privacy and autonomy. Social media companies often don't provide a clear and accessible outline of how they use the data they store, and the specifics of where it is sold and how.

Ultimately there needs to be more updated and detailed technology legislation and platform rules in order to truly protect citizens. Government legislation should prioritize having companies inform individuals of their tech policies in a clear manner, and focus on user security over data collection. By specifically addressing and outlining practices for social media companies in order to protect user privacy, it will hopefully create a shift in technology development from benefiting from the user to supporting the user.

Social Media Intro:

Social media is a beneficial tool for networking and communication, but many social media platforms collect user data to use for insights and sell to third parties. This puts the user in a difficult position to decide whether they want to protect their data, or stay informed and connected socially.

Social media is an umbrella term for the group of applications that allow users to share and engage with content, and network. Around 4.9 billion people use it today[1]. It is a central part of modern life because it allows people to make money, stay connected with friends and family, network to find jobs, and advertise their businesses. Currently, the most popular social media networks include Facebook, Youtube, WhatsApp, and Instagram[2]. Someone without social media misses out on the information updates and other benefits of being active online. These platforms are so commonly used that those who don't partake in them lose that method of connection.

However, social media does not protect individual's privacy and data well. Many of the applications store the data of individuals for their own benefits (such as marketing propaganda, selling the information to third-parties for profit, etc.). Companies can take data insights from social media to show users specific content that could sway them to believe a certain organization's views. Governments can monitor people's social media activity. This may cause people to consider opting out of social media platforms in order to protect their data and maintain their autonomy. Deciding to quit is a difficult decision for individuals because it forces them to choose between their personal privacy and the benefits that come from participating in social media. By not choosing to participate in social media and keeping their data safe, people lose access to opportunities to socialize with their peers.

Privacy Harms Background:

Though social media has many benefits, it can negatively impact one's personal and professional life through privacy violations. The ways that an individual can be harmed by privacy violations are categorized into groups called privacy harms. These categories include physical harms, economic harms, reputational harms, psychological harms, and autonomy harms[3]:

- Physical harms are harms that result in death or injury. These harms are easily identifiable as legal causes of action. For example, Strava's release of GPS data points for runners could result in certain runners being targeted, stalked, and put

[1] Forbes Advisor. "Social Media Statistics for 2023." Forbes, https://www.forbes.com/advisor/business/social-media-statistics/.
[2] Forbes Advisor. "Social Media Statistics for 2023." Forbes, https://www.forbes.com/advisor/business/social-media-statistics/.
[3] The George Washington University Law School. "Restatement (Second) of Torts." The George Washington University Law School, https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2104&context=faculty_publications#:~:text=Restatement%20of%20Torts%2C%20in%20which,%2C%20false%20light%2C%20and%20appropriation.

at risk. In 2017, when Strava published their running routes[4], they gave away the locations and maps of military bases, which were visible through the running routes of soldiers inside of the bases. Many people were not fully aware of how much data Strava was collecting until this event happened, which is dangerous for individuals because they are put at risk unknowingly.
    - This sharing of data by Strava could have resulted in the harm of soldiers or individuals, whose routes were easily accessible to the public.

- Economic harms, losing something of monetary value, include identity theft, and sharing of credit card and financial information. Many economic harms stem from data breaches, which creates difficulty for a court to see the link between a data breach and the theft of a specific identity.

- Reputational harms injure one's reputation, which can result in loss of employment, business, or social standing. Reputational harms are often the result of data being unorganized, incorrect, and incomplete. In Perkins v. Linkedin[5], the app downloaded users' contacts, and sent the contacts invitations to connect without the users' permission. Linkedin was sued on the grounds of sending repeated invites which could harm the reputation of the user because the fake invites could change how the user is perceived by their contacts.

- Emotional distress, or physiological harm, is one of the most common types of privacy harms that occur, and entails causing certain emotions (fear, embarrassment, anger, frustration, anxiety, etc.) or distress. For example, if a social media's algorithm repeatedly generates emotionally harmful content, it could lead to depression, anxiety, or other mental health disorders. The user is not able to directly control what type of content is presented on their social media page. They are subjected to the consequence of seeing the algorithmic-generated content without knowing beforehand if the content could be harmful and the choice of being able to opt-out of viewing it.

- Autonomy harms are when people are denied the ability to freely make choices or their choices are influenced and limited. There are six different types of autonomy harms: coercement, manipulation, failure to inform, thwarted expectations, lack of control, and chilling effects. These types of autonomy harms demonstrate how one's autonomy can impact different aspects of someone's life, which stresses how important it is for the protection of individual privacy to be prioritized by government legislation and social media company policies.

---

[4] Forbes. "Strava Fitness Data's Location Privacy Scare: What You Need To Know." Forbes, 29 Jan. 2018, https://www.forbes.com/sites/thomasbrewster/2018/01/29/strava-fitness-data-location-privacy-scare/?sh=6093600c55c3.
Map of Strava Running Routes: https://www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/

[5] The George Washington University Law School. "Restatement (Second) of Torts." The George Washington University Law School, https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2104&context=faculty_publications#:~:text=Restatement%20of%20Torts%2C%20in%20which,%2C%20false%20light%2C%20and%20appropriation.

Different harms can impact many aspects of individual wellbeing, which stresses the importance of why there needs to be legislation that protects individual privacy regarding social media. Without this legal update, individuals are more easily susceptible to the following types of harms due to their data shared by social media use. Autonomy harms are especially notable, because they take away the ability to make choices and free will, which are fundamental values in the United States. The lack of concreteness and specificity around the privacy laws demonstrates why there needs to be revisions to the federal privacy laws, similar to the GDPR in Europe. Without these revisions, core American values such as free will are violated through autonomy harms.

Autonomy Harms:

Autonomy harms are consequences and violations of individual autonomy. Autonomy is violated in social media because the freedom for people to control their data and choices is tampered by surveillance, manipulation, and use of data without consent. These harms are breaches of individual privacy, which can result in the loss of personal information and exposure to manipulative influence and content. This effect could influence someone's decision-making in their day-to-day life. Different types of these autonomy harms include coercement, manipulation, failure to inform, thwarted expectations, lack of control, and chilling effects. Surveillance and data breaches are two causes of these autonomy harms[6].

Manipulation can occur when social media can influence users to believe a certain viewpoint without showing them all the facts. This happens by showing users content that best represents their views or the views in their area. When users only see media that aligns with their preferences, it could cause them to make decisions with only the information they acquired through social media and not with all the facts at hand.

Social media can also cause thwarted expectations, another type of autonomy harm. When users send direct messages that are labeled as encrypted, the app often does not clearly communicate that it is storing information. This causes the user to assume that their messages are truly private. Social media applications should clarify what information they are storing, because otherwise users are not aware of how much of their information the application has.

Surveillance and monitoring are also causes of autonomy harm, because they can limit individual freedoms and influence how people act, especially when people are aware of the surveillance happening. Monitoring and surveillance cause the chilling effects[7], which is when individuals change their behavior due to suspected violations of privacy. Examples of these behavior changes include censoring what one posts online and stores on their devices, which can limit one's freedom of speech, political participation, freedom of belief, and freedom to share ideas. The chilling effects impact the choices an individual makes, which may result in them changing or suppressing their beliefs and being detrimental to their mental health and

---

[6] The George Washington University Law School. "Restatement (Second) of Torts." The George Washington University Law School, https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2104&context=faculty_publications#:~:text=Restatement%20of%20Torts%2C%20in%20which,%2C%20false%20light%2C%20and%20appropriation.

[7] The George Washington University Law School. "Restatement (Second) of Torts." The George Washington University Law School, https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2104&context=faculty_publications#:~:text=Restatement%20of%20Torts%2C%20in%20which,%2C%20false%20light%2C%20and%20appropriation.

well-being. For example, data from TikTok, a video-sharing social media app, is being accessed by the Chinese government in order to identify the locations and communications of pro-democracy Hong Kong protestors[8]. This information being publicly available may impact how people share and communicate with others on TikTok, which can be limiting to their freedom of speech. Another example of this phenomena is the Cambridge Analytica scandal[9], where the company used Facebook data to better target political messages in order to influence people to be more sympathetic to the 2016 Trump Campaign. This is another example of how individual autonomy can be harmed, because people are being influenced and coerced without their knowing or consent. When this tracking is revealed, many users may choose to opt-out of using that social media for their own protection. If social media companies do not make changes to protect user privacy, they could lose users who value those qualities.

Data breaches, another cause of autonomy harm, are when information is stolen or taken from a system unknowingly. This event can result in unauthorized access to personal information, loss of privacy, and data misuse. All of which could cause autonomy harm. People should always act with caution by assuming their data will be breached and everyone can see their information, because data can be breached unknowingly. In order to prevent data from being misused by companies, the amount of data shared with those companies should be limited by reviewing and changing privacy settings, limiting permissions granted to third-party applications, and checking access to applications frequently (sometimes companies automatically reset privacy settings when the application is updated).

By learning about what data breaches are and how to act when one happens, individuals can better understand how to protect their data and prevent autonomy harm. Even when a data breach is not confirmed, there are still ways to address it and apply caution to the situation. These ways include changing passwords regularly, using two-factor authentication, checking accounts for suspicious activity, using a password manager, limiting the amount of data shared online, and staying on top of news updates from different technology and security places for information about larger data breaches and advice on how to address them.

Though there are actions individuals can take to mitigate the consequences of a data breach, companies should do a better job of addressing, educating, and communicating information on data breaches with their users. Especially since companies can sell user information without the permission, which is entirely out of the user's control and responsibility. Also, there should also be federal legislation that can protect people's privacy in a court of law when data breaches occur[10].

Autonomy harms can impact the decisions and freedoms of users unknowingly. By learning about autonomy harms, individuals can better understand the ways social media can

---

[8] Euronews. "China Used Data from TikTok to Track Hong Kong Protesters, Says Former ByteDance Executive." Euronews, 8 June 2023, https://www.euronews.com/next/2023/06/08/china-used-data-from-tiktok-to-track-hong-kong-protesters-says-former-bytedance-executive.

CNN. "China Used Data from TikTok to Track Hong Kong Protesters, Former Exec Claims." CNN, 8 June 2023, https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html.

[9] (Nicholas Confessore) "Cambridge Analytica and Facebook: The Scandal and the Fallout So Far", *The New York Times*, The New York Times Company, 4. Apr. 2018, https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

[10] Millar, Sheila A., and Tracy P. Marshall. "SEC Finalizes New Data Breach Reporting Rule; NIST Releases Cybersecurity Framework 2.0." *The National Law Review*, 25 Aug. 2023, https://www.natlawreview.com/article/sec-finalizes-new-data-breach-reporting-rule-nist-releases-cybersecurity-framework.

influence their thoughts and choices. The government also uses social media for surveillance, which can cause autonomy harm. The connection between companies, the government, and the impact technology can have on individual users demonstrates how individuals aren't solely responsible for protecting their privacy through social media. Companies and governments need to be clear about their role and update their rules and legislation to better adapt to modern day social media and to protect the privacy of individuals. Social media is a positive tool, but the negative impact on autonomy needs to be addressed.

History of Privacy:

Comparing past privacy laws and developments to current privacy laws demonstrates the amount of legislative change for privacy enacted in response to the rise of social media.

Some of the privacy beliefs that apply to social media today were developed by Louis Brandeis in the 1890s. His ability to do this demonstrates that modern day legislators should be able to create privacy legislation that is applicable to social media today and any technology developments in the future. It also shows how there needs to be an update to privacy laws, if the United State's only general legislation for privacy was created and based on ideas from before the development of social media. Though the general laws developed about personal privacy can be loosely applied to individuals while using social media, they don't address the extent or specifics that are needed to prevent technology spaces from breaching the privacy of individuals. Social media companies developed this technology that went beyond what Brandeis could've imagined, especially in terms of privacy ideals. There is not enough legislation to address what harms are a result of the social media company vs. which are the fault of users. Also, there were no rules about privacy and social media development that were in place when these platforms were engineered. This means that social media companies were allowed to directly focus on what would benefit them the most, without having to worry about user privacy.

The foundation of the privacy laws that apply to social media today was created before social media existed. The following developments[11] helped develop privacy as a human right, but in the United States, social media organizations and other companies often collect data at the expense of this human right.

- Brandeis's article "The Right to Privacy"[12] in the Harvard Law Review started this consideration of individual privacy in the United States. In 1948, the United Nations declared, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks", making privacy a human right. This right should be respected by social media companies, and more legislation on social media is needed for this to happen. This statement of Brandeis' should also include

[11] Safe Computing - University of Michigan. "History of Privacy Timeline." Safe Computing - University of Michigan, https://safecomputing.umich.edu/privacy/history-of-privacy-timeline.

[12] Brandeis University. "The Right to Privacy." Brandeis University, https://www.brandeis.edu/now/2013/july/privacy.html.

interference to decision-making, which is a common autonomy harm in social media today.

- In 1960, William Prosser[13] outlined four torts that were reasons for someone to sue for privacy violations. These four causes of action are intrusion, disclosure, false light, and appropriation. The torts of Prosser exist as a basis for how a violation of privacy can be defined, and are still used today in legal systems. These torts should be examined to better define and understand how these causes of action could happen through social media usage. Autonomy harms should also be added as a cause of action, because of their restriction on individual free will, which is a violation of a core United States value.
- Alan Westin's book, *Privacy and Freedom*, defines what privacy is, and is often seen as a basis for the development of privacy laws today. Though these examples show how privacy was defined and declared important, this same standard is not being upheld with the development of social media today. The concept of privacy should also be re-adjusted to include how it can be violated in social media.

These developments started conversations in the U.S. for defining privacy and its importance. These works above directly contributed to some of the basic privacy laws in the United States, such as the Privacy Act of 1974, which establishes a code of Fair Information Practice on federal agencies and how they use the information of individuals. Unfortunately, the forward progress on privacy legislation in the United States slowed after that event. From then on, the government passed privacy legislation with the intentions of addressing specific issues (like HIPAA addressing healthcare, and COPPA addressing child privacy online). No federal legislation was created to address privacy as a whole and to protect individual privacy rights. This circumstance leaves a gap in the U.S. privacy laws because there are many unaccounted scenarios that exist between the legislations of COPPA, HIPAA, and other similar laws.

The EU has legislation for privacy and data protection that can act as a model for what the U.S. should adapt. The EU's GDPR (General Data Privacy and Regulation) deals with data protection and privacy, focusing on keeping the data of individuals safe while also giving them a say in how it is used.

The U.S. privacy legislation system may have been manageable in the past, but falls short of properly protecting the privacy of citizens with the variety of new challenges that social media poses. It is difficult for old privacy laws to be applied to social media because there is no specific legislation to discern what is the social media company's fault and what is the user's fault. Without new legislation to address this issue, there is a gray area that makes it difficult to apply old privacy laws to social media cases. Especially for cases of autonomy harm, where the user's free will is being influenced as a result of the social media that the user agreed to[14].

---

[13] University of Chicago. "Prosser on Privacy: A Half-Century Later." Chicago Unbound, https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=10315&context=journal_articles#:~:text=In%201960%2C%20William%20Prosser%20wrote,%2C%20appropriation%2C%20and%20false%20light.

[14] The New York Times - Wirecutter. "The State of Privacy Laws in the US." The New York Times, https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

Solutions for Individuals

There are actions individuals can take to lessen their privacy being breached, but these actions are not long-term or guaranteed solutions.

Social media users should be educated on some of the different factors for autonomy harms related to their social media use: manipulation of content, filters/targeted preferences that could limit one's exposure to unbiased and diverse perspectives, targeted advertising, and assumption of personal data being exploited for profit. These actions are happening because tech companies are benefiting from it financially. By leveraging this personal data they can optimize their algorithms, which can result in better targeted advertisement, increased user engagement, and increased revenue. This data could also be sold to other companies for similar purposes. This cycle can result in individuals losing parts of their free will, such as their choices, behaviors, and experiences, through manipulation and extortion for financial gain.

In order to lower the risk of autonomy violation through social media use safely, individuals should know the basics of how data is collected, stored, and shared, and the guidelines of different platforms. This knowledge helps users make smart decisions about how they interact with social media such as what they consume, share, and what platforms they use. Individuals should also be able to know and enable the best privacy settings for them, limit the personal information shared through the content they posted, and evaluate and know the extent of the information they provide to companies. There is a low chance that someone can prevent their data from being used and avoid autonomy harm on social media, but acting with caution and being informed can mitigate some of those effects.

There are also tech solutions that individuals can use to combat autonomy harms. These include browser extensions, VPNs to encrypt internet traffic, ad-blockers, password managers, and other tools for managing and controlling online identities. Though these solutions exist, they are not permanent, definite, nor a replacement for the systemic change that needs to happen.

Also, there are digital spaces out there that remedy these harms and reduce the exposure of an individual to them. There are apps in the app store that are advertised as not collecting user data. Some digital spaces that are privacy-conscious include Mastodon, and Wire. Yet they are not nearly as popular as other platforms, which lessens their desirability and purpose. Also, even if an application seems safe, there would still need to be legal protections and safeguards in place to protect someone's rights and from other future circumstances.

Though there are actions that individuals can take to lessen the risk of their privacy being breached, it ultimately is up to companies and governments to make regulations and to make it easier for the average person to make informed choices on social media.

Solutions for Social Media Companies

In order for fair data insights while still protecting the privacy of the user, companies should prioritize their communication with individuals regarding their data collection.

Companies should explain to users how their data is being used and how this usage benefits the user. This way, users have more trust and willingness to share information with companies. By keeping users more informed about how their data is being used, they are able to see if content is being generated to manipulate them, and maintain more control over their free will. Additionally, users should be given different privacy options (such as consent mechanisms and options for data deletion) so they are able to personalize how much information they want to share with a company. This action would lessen the impact of surveillance and monitoring, because users can choose which parties have access to their information. Everyone has the right to their own data, but if companies are clear about how they use data and the benefits of their actions, people can choose to opt-in and share their data.

Currently, data insights are shared by sending personal identifiable information, which is not private nor secure for the user. But, if companies used methods like federated learning, algorithms, or trust networks, they would only have to share non-identifiable information and the users would be better protected. Also, because companies would only be sharing insight and not data, they could switch their focus from trying to control the data to maximizing insight which would benefit the user.

Legislative Solutions

As United States citizens, people have the right to privacy and unwarranted surveillance but the current federal laws do not properly address these harms in a way that can fully protect citizens from it. Currently, there is a patchwork of specific data laws in the United States that aren't adequately protecting the data of citizens. Despite most of these data laws being designed to protect citizens from infringements by the government, there should also be legislation protecting individuals from data violations by corporations. Also, there should be a singular data-protection mandate[15].

Many other countries have implemented singular data-protection legislation. In the EU, the General Data Protection Regulation (GDPR) focuses on protecting the data of individual citizens. It should be used as a model for the legislation that the United States should implement.

In this new U.S. data-protection mandate, the gaps should be filled in between the current data-protection laws such as HIPAA, FERPA, and COPPA, in order to protect the security of individuals in every aspect of their lives.

The regulations should not only cover all aspects of data-protection, but should be strengthened through creating stricter regulations on data collection, storage, and sharing practices that companies, and governments need to abide by. In order to make sure that companies follow this mandate, the U.S. could implement another tactic similar to the GDPR: fining companies significantly for non-compliance. This tactic, along with having companies

[15] O'Connor, Nuala. "Reforming the U.S. Approach to Data Protection and Privacy." 30 Jan. 2018, https://www.cfr.org/report/reforming-us-approach-data-protection.

provide regular reports on their data-collection practices, could promote transparency and accountability in company data-collection.

There should also be improved legal definitions of different privacy harms and violations. Though the harm of breaches is recognized, the legal definition of privacy harm types is unclear and difficult to apply in court of law. Some types of harms, such as emotional harm, don't always have clear, physical evidence, so addressing what qualifies legally could make dealing with it easier.

In order to create the best privacy laws to protect the rights of citizens, there should be more collaboration with the public. By increasing public awareness and digital literacy on privacy risks and policy, people can understand their digital rights better and more clearly communicate what data they are satisfied with companies collecting.

Conclusion

Social media is an important aspect of life today. It allows people to connect with loved ones, make money, network to find jobs, and advertise their businesses. However, many of the applications store the data of individuals for their own benefit, which does not protect individual's privacy and data well. This may result in people opting out of social media platforms in order to maintain their autonomy and protect their data. Though by choosing to not engage in social media, people lose access to chances to connect with their peers.

Despite social media's benefits, the privacy violations it causes can be detrimental to one's personal and professional life. Different harms can impact many aspects of individual wellbeing, which stresses the importance of why there needs to be legislation that protects individual privacy regarding social media. Autonomy harm is an especially notable type of harm, because it takes away the ability to make choices and free will, which are fundamental values in the United States. Autonomy is violated in social media because the freedom for people to control their data and choices is tampered by surveillance, manipulation, and use of data without consent. These harms are breaches of individual privacy, which can result in the loss of personal information and exposure to manipulative influence and content.

Many privacy violations happen today because of the lack of specificity in federal laws for privacy in social media. Without new legislation to address this issue, there is a gray area that makes it difficult to apply old privacy laws to social media cases. There needs to be changes made in order to update and modernize the laws so they are adaptable to society today. Also, social media companies should respect user privacy more. In order for fair data insights while still protecting the privacy of the user, companies should prioritize their communication with individuals regarding their data collection.

The connection between companies, the government, and the impact technology can have on individual users demonstrates how individuals aren't solely responsible for protecting their privacy through social media. Companies and governments need to be clear about their role and update their rules and legislation to better adapt to modern day social media and to protect the privacy of individuals. Social media is a positive tool, but the negative impact on autonomy needs to be addressed.