UNIT III SOCIAL MEDIA POLICIES AND MEASUREMENTS

Social Media Policies-Etiquette, Privacy- ethical problems posed by emerging social media technologies - The road ahead in social media- The Basics of Tracking Social Media - social media analytics- Insights Gained From Social Media- Customized Campaign Performance Reports - Observations of social media use.

SOCIAL MEDIA PRIVACY

Social media platforms have become vast and powerful tools for connecting, communicating, sharing content, conducting business, and disseminating news and information. Today, millions or billions of users populate major social networks including Facebook, Instagram, TikTok, Snapchat, YouTube, Twitter, LinkedIn, and dating apps like Grindr and Tinder.

But the extraordinary growth of social media has given platforms extraordinary access and influence into the lives of users. Social networking companies harvest sensitive data about individuals' activities, interests, personal characteristics, political views, purchasing habits, and online behaviors. In many cases this data is used to algorithmically drive user engagement and to sell behavioral advertising—often with distortive and discriminatory impacts.

The privacy hazards of social networks are compounded by platform consolidation, which has enabled some social media companies to acquire competitors, exercise monopolistic power, and severely limit the rise of privacy-protective alternatives. Personal data held by social media platforms is also vulnerable to being accessed and misused by third parties, including law enforcement agencies.

Social media privacy issues

1. Data mining

Data is the bread and butter of social media platforms. They do everything based on your information – tailor their services, serve ads, analyze the market, build business models, etc. Some data you've given to them is personal, like your name, email addresses, date of birth, or where you live. But other kinds of data, like your likes and dislikes, photos, and posts, can paint a picture of who you really are too. This type of data is a gold mine for social media platforms. So this is where data mining comes in.

Once you willingly give away data by agreeing to their Terms and Conditions, it belongs to them. They can do almost whatever they please with it. They can:

- Use this data to create an accurate user profile and serve you targeted ads
- Share data with their partners
- Sell data to third parties

- Transfer your data to different countries where privacy laws might be more lenient
- Use your photos or other types of data in their campaigns
- Influence your opinion based on your likes and dislikes (this happened in the Cambridge Analytica scandal)

2. Privacy setting loopholes

Data privacy is an important issue. Most social media companies amended their privacy policies in response to stricter privacy laws and regulations in Europe. They now allow you to tweak your settings and make your accounts more private. However, changing your privacy settings doesn't always guarantee privacy. How?

Most of the time, something you shared with a closed group of friends gives them the ability to share it with others. Your friend's friends can then see the content you posted, which might not be your intention. Your friends might not even have stringent privacy policies, meaning that others can now access information that was supposed to stay within your friends' circle.

The same applies to closed social groups and forums. Sky News has previously found that comments and user lists in private health groups on Facebook could be easily searchable and discoverable by insurance companies and employers. So think twice before posting or commenting about controversial issues. That information could ruin your reputation or lead to identity theft.

3. Location settings

Pay attention to location settings when you use social media sites and apps. Some might be tracking your whereabouts even when you told them not to like Google was caught doing last year. Your location might not seem like a very valuable piece of data. However, when paired with your other personal information, it could help to create an even more accurate user profile.

Real-life thieves and stalkers could also use location data. Imagine if a criminal knew where you are at all times. They could easily break into your house when you weren't there or follow you home.

4. Hacking

Social media accounts are an excellent target for hackers for many reasons. For example, they can:

- Gather information from your social media profiles and use it to break into your accounts. Posting photos of your dog and then using his name as a password is one of many easy tricks
- Gain a better understanding of who you are and use social engineering attacks such as phishing or pretexting

- Spread malware and viruses through your accounts. Once they're in, they can send messages to your friends with a link that hides malware. Such phishing techniques tend to be much more effective compared to email phishing as people trust messages that come from their friends.
- Use your information to impersonate you or even steal your identity

5. Harassment, cyberbullying, and impersonation

Social media can also be used for cyberbullying or cyberstalking. The perpetrators don't even need to be hackers. They can be infatuated colleagues sending threatening messages or your kid's classmates bombarding them with inappropriate comments. It could also be your ex-partner who shared private information about you online or even hacked into your account and messaged your colleagues and friends to ruin your reputation. This can be a privacy nightmare, especially if the information was sent from your account. Explaining that it wasn't you could be close to impossible.

6. Addiction and the psychological consequences

Social media is addictive and can impact your personal, social, and professional life if overused. Users tend to spend significant time on social networks, which sometimes affect their real lives. So make sure you have a healthy balance between your real life and your virtual lives.

7. False information

Social media is widely used to spread misinformation and propaganda. Trolls, which have a noticeable presence online, also intentionally provoke useless discussions and manipulate others' emotions. So make sure to double-check every fact you find suspicious on social media and don't share it without being sure it's genuine.

How to Protect Your Privacy on Social Media

Social networking sites such as Facebook, Twitter, Instagram, and Snapchat have become digital billboards for internet users. People love sharing their personal views and news about what's going on in their lives.

But stop and think about social media privacy for a moment. This information — some of which is very personal — is going up on the internet. Outside of your trusted circle of friends and relatives, who else is viewing what you post? Could you make yourself more vulnerable to social media scams?

Here are some tips and hints to help you protect your social media privacy and make your social networking a more rewarding experience.

1. Read the social media site's terms

Your personal information is valuable. You wouldn't just hand out your bank account information, so why would you give away your privacy rights on social networking

sites? Pay attention to what information you are agreeing to share when you sign up for a social media account.

Take a moment to wade through the legal information contained in the Privacy Policy and Terms of Service before you click "Accept." You may find that some of the terms are in the best interest of the platform, but may not be the best for your privacy.

Some of the conditions may exceed your personal comfort limit. For instance, some free sites may gather and sell data related to what you look at to third parties for marketing purposes. Make sure your permission choices are right for you.

2. Don't share private information like your full name and address

Keep your full name and address to yourself. Same advice also applies to posting your children's or grandchildren's full names. As innocent as it may seem to share people's full names, you never know how a stalker or cybercriminal might use that information to their advantage.

For instance, with a combination of your first name and last name, cybercriminals may be able to guess your email address, or purchase your email address from the dark web. With this information, they could send you a phishing email that could potentially lead to injecting malware and collecting data from your devices.

Remind the teens in your life to adopt the same practices, as they may be more likely to share personal information. Your kids may not be thinking about privacy in social media when giving their name and address, or other personal details, when entering an online contest. It's a good idea to keep social media privacy top of mind.

3. Be careful about posting photos on social media sites

Think twice about posting photos. Even if you don't post a child's name, you may be revealing too much information in what you thought was a harmless photo.

Consider this scenario: You want to post a digital photo of your grandchild in their new sports uniform at the big game. What's wrong with this, you ask? If the photo contains the school's name, either on uniforms or in the background, a stranger wouldn't have too much trouble tracking down your grandchild's location and identity. Consider blurring or cropping such revealing details, if you know how. If not, maybe that isn't the best photo to share.

And what about that picture of your expensive new TV? Advertising its location could make your home a tempting target for thieves. When in doubt, just share your photos privately with a trusted few.

4. Adjust the social media platform's privacy settings

Each social media platform has a different process to control privacy settings. Before you share your post or pics, always be mindful of who can see, react, or comment.

Carefully decide whether you want your social media posts and pictures to be visible to everyone, only friends, or friends of friends, when reviewing your privacy settings for each platform. You can also make a custom list for each post.

Tagging friends can be a lot of fun, but also an invasion of privacy. Also, you don't want to be tagged in something inappropriate. Always opt to review when somebody else tags you in a post before it is published. Keep in mind, however, just because you may not approve the post to be published on your social media page, it may still be visible on theirs, publicly.

5. Know what types of personal data social media sites store and share

Upon signing up for a social media site, most users willingly give their name, gender, date of birth, and email address. Some social media sites don't stop at that. They go on to collect other information like an IP address or the types of things you have liked, shared, or commented on.

Sometimes you're given the choice to use your Facebook credentials to log in to other, third-party apps. While this may be convenient, you could unwittingly allow other apps to access more of your personal information than necessary.

One way to make sure that you are not oversharing information is to always read the fine print. When modifying your privacy settings on any social media platform, look for the "Apps and Websites" option under "Settings." Carefully review which websites are using your information.

6. Consider carefully what personal details you provide in your profile

Social media and networking sites may ask for additional information when you sign in. You can often include your hometown, schools you've attended and when, your current and former workplace, political affiliations, and general interests. All this information can be stored and tracked.

As harmless as it may seem, this information could be used to serve you ads and news items. Many sites may also include permissions to access your friends list, personal preferences, and more in their terms of use.

7. Don't display the names of the people in your network

Here's another aspect of social media privacy. While you may not be victimized directly, your connections might be. Spear-phishing scams rely on cybercriminals gathering enough personal information to send out convincing emails, seemingly from people known by the target. With access to the names of your connections, your friends may start to get bogus emails from somebody pretending to be you.

8. Avoid social media site posting regrets

It's possible that your employer, or the recruiter at that company you just applied to, could review your social media profile. If you're posting views that your company wouldn't appreciate — like talking about how much you dislike your boss — then you

might want to step away from the keyboard. Once information is out there, it can spread. Don't let what you share today come back to haunt you tomorrow.

Social media and networking sites can be a great way to stay connected with old friends and help you make new ones, or to land that next big job. Just keep your privacy shades drawn to the right level.

9. Always log out when you're done.

Here's a basic to remember for your social media privacy. If you're using a public computer, make it a ritual to log out — but log out of private devices from time to time as well. Logging out helps ensure that other people won't "commandeer" your social media profile and use it to attack your friends, change your personal information to embarrassing or slanderous comments, or worse, change your password and lock you out of your own account entirely.

10. Create strong, private passwords.

Another basic? A strong password uses a combination of words, numbers, upper- and lowercase letters, and special characters that is easy for you to remember, but tough for other people to guess. Skip common password elements like birthdates, anniversaries, and the names of your children or pets. Keep passwords private by memorizing them or using a trusted password manager — and never write them on the device itself.

It's smart to stay on top of your social media practices and try to avoid risky behavior online. That means taking steps to consider privacy when you post on your digital billboards.

Why is ethics important in technology?

Ethics in technology plays an important role in today's worlds as it ensures that technology is used appropriately to benefit the society, without any unintended consequences and bias. It ensures accountability and builds trust between companies, individuals and, governments enabling the effective adoption of technology.

Ethical issues in technology

While businesses face several ethical challenges owing to the ever-evolving technologies and its fast-paced implementation, it is critical that they ensure personal data is protected and used appropriately. While there could be several ethical issues, here are some of the important ones:

1. Misuse of personal data

With businesses gathering huge amount of our personal data from various internet sites such as shopping sites, social media or any other business platforms, etc., misuse of personal information becomes one of the primary ethical concerns. While companies extract the information to personalize our experiences, to understand what kind of products

consumers are looking for, what type of content are we interested in, or just to reach out to a larger customer base. However having access to all our personal information could also be considered as a breach to our right to privacy and can lead to negative circumstances such as data breaches and cyberattacks. In some cases, our personal data can be misused for targeted advertising, shared with third-party partners.

2. Spread of misinformation

With information/news being available real-time thanks to constant access to the internet, there are high chances of it being misinterpreted or simply spread without fact checking. This kind of inaccurate or distorted information is capable of causing havoc in the society. Information that's being freely spread on the internet does not undergo any validation and therefore carries high chances of turning into misinformation. With deepfake technology coming into picture, even videos cannot be claimed to be real and truthful. This technology allows manipulation of digital images, giving an output that may have never happened. Deepfake technology also carries a lot of ethical concerns such as misuse of identity or privacy invasion.

3. Lack of accountability

When it comes to ways in which businesses operate, often there are third-parties and shared technology involved. There arises confusion about which party is responsible for data governance. For concerns on big data, cybersecurity and other data being used by both parties, there is usually a lack of responsibility or even awareness. While ideally, businesses need to share these responsibilities collectively to ensure data security.

4. Liability for autonomous technology

From robotic surgeons to self-driving cars or unmanned drones for delivery, all come with ethical concerns. While from the business perspective, it holds immense potential, however allowing programmed technology to control itself without human oversight can be concerning. Some level of human intervention is always needed for safety and ethical purposes.

5. Artificial Intelligence (AI) bias & accountability

AI is yet another transformative technology that has a huge potential, however it also comes with its own set of ethical issues. AI technologies such as facial recognition, health tracking etc. result in risking our personal data and has the possibility of being misused. Another ethical issue AI poses is the concern of bias as AI algorithms are based on training data that tend to have a human bias, therefore AI has the issue of inheriting the bias of its creators.