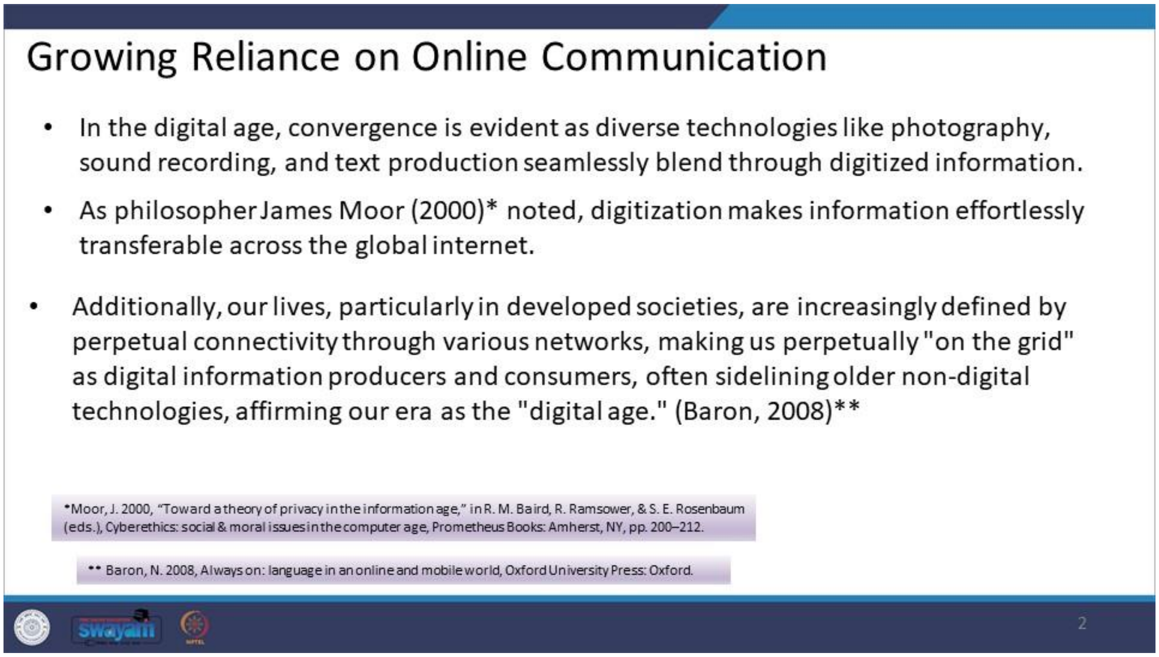
Online Communication in the Digital Age
Prof. Rashmi Gaur
Department of Humanities and Social Sciences
Indian Institute of Technology
Lecture – 47
Scammers Perils and Pitfalls of Online Communication – Part I

Good morning, dear friends and welcome to this module. In the modern digital age, the pervasive nature of online communication brings with it a range of risks and challenges that individuals must navigate. Today's module aims to expand upon the previous discussions on the potential dangers and challenges encountered in the realm of online communication. As discussed in previous weeks, the ability to connect with people worldwide, the instantaneous nature of communication, increased accessibility and the potential for reaching a vast audience are key benefits that have in fact reshaped the way we share information and engage in social, professional and educational spheres. However, understanding the advantages of online communication sets the stage for recognizing the challenges and responsibilities that come with it.



Growing Reliance on Online Communication

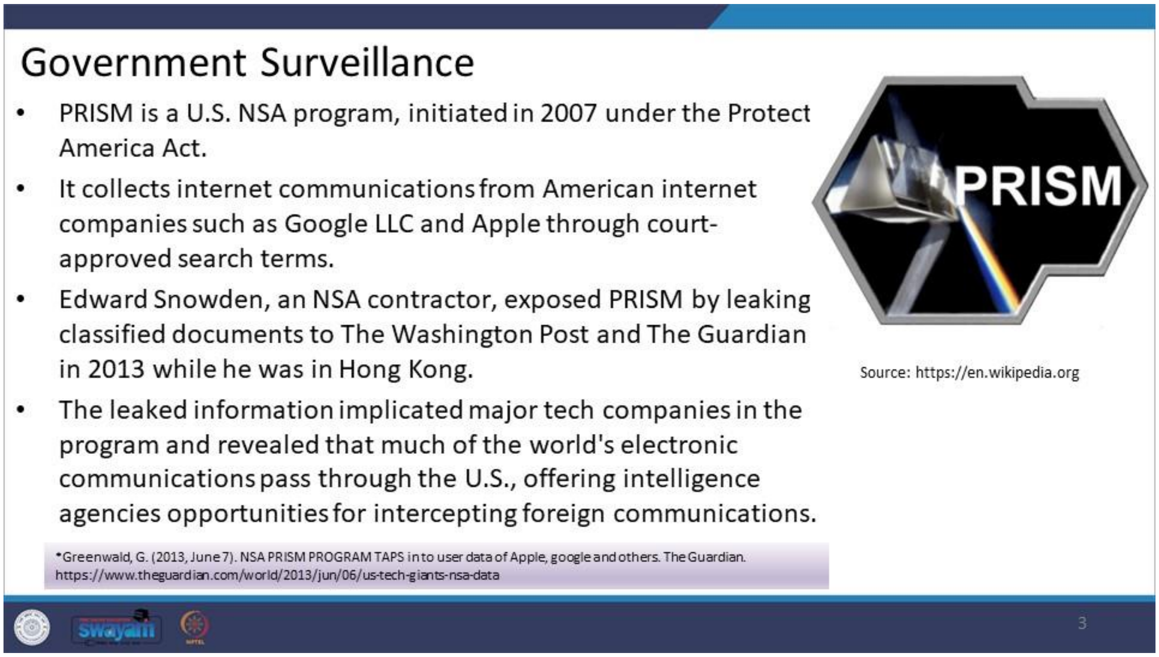
- In the digital age, convergence is evident as diverse technologies like photography, sound recording, and text production seamlessly blend through digitized information.
- As philosopher James Moor (2000)* noted, digitization makes information effortlessly transferable across the global internet.
- Additionally, our lives, particularly in developed societies, are increasingly defined by perpetual connectivity through various networks, making us perpetually "on the grid" as digital information producers and consumers, often sidelining older non-digital technologies, affirming our era as the "digital age." (Baron, 2008)**

*Moor, J. 2000, "Toward a theory of privacy in the information age," in R. M. Baird, R. Ramsower, & S. E. Rosenbaum (eds.), Cyberethics: social & moral issues in the computer age, Prometheus Books: Amherst, NY, pp. 200–212.

** Baron, N. 2008, Always on: language in an online and mobile world, Oxford University Press: Oxford.

We find that in today's age, convergence is very evident as different technologies like photography, sound recording and text production seamlessly blend through a digitalized information. As James Moore, a philosopher has noted, digitization makes information effortlessly transferable across the global internet. Additionally, our lives, particularly in the developed societies are increasingly defined by perpetual connectivity through various networks, making us perpetually so to say on the grid as digital information procedures and consumers often sidelining older non-digital technologies, forming our era as the digital age.

The increased reliance on the internet has provided different multinational companies as well as governments with vast data resources enabling more extensive surveillance and data collections on consumers. Government surveillance of a citizen is notably exemplified by PRISM and brought to our attention through Edward Snowden's disclosures. It raises significant concerns about privacy as well as the ethical modes behind it. It involves covert data collection from internet companies and poses a potential threat to individual freedoms and civil liberties in the American society.



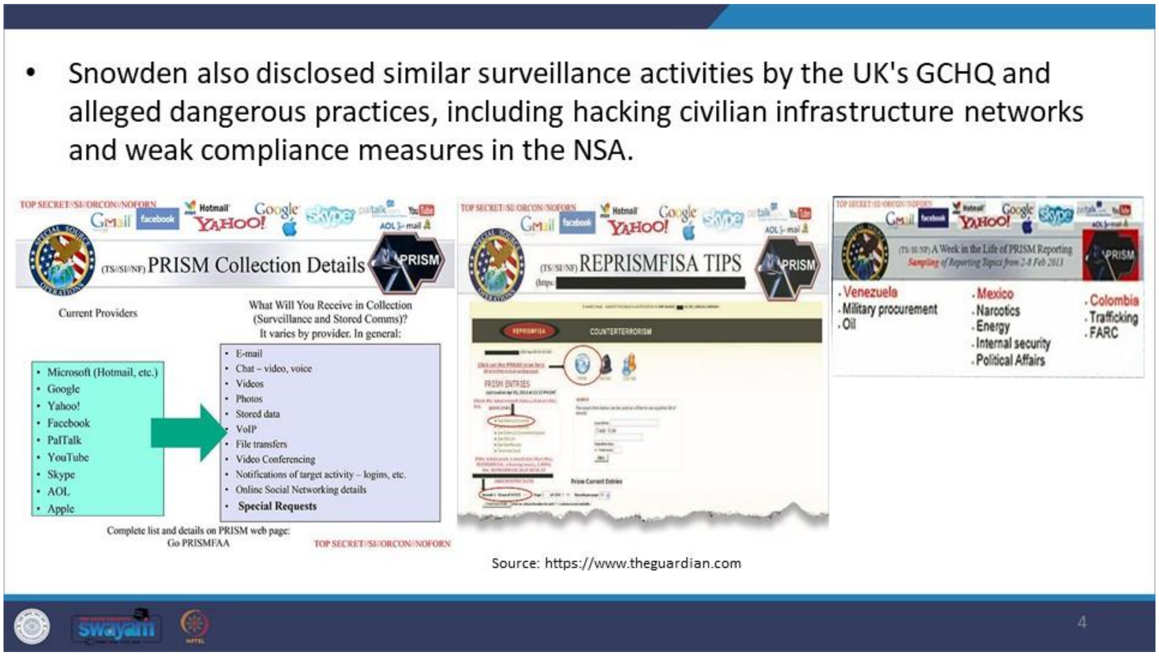
Government Surveillance

- PRISM is a U.S. NSA program, initiated in 2007 under the Protect America Act.
- It collects internet communications from American internet companies such as Google LLC and Apple through court-approved search terms.
- Edward Snowden, an NSA contractor, exposed PRISM by leaking classified documents to The Washington Post and The Guardian in 2013 while he was in Hong Kong.
- The leaked information implicated major tech companies in the program and revealed that much of the world's electronic communications pass through the U.S., offering intelligence agencies opportunities for intercepting foreign communications.

Source: https://en.wikipedia.org

*Greenwald, G. (2013, June 7). NSA PRISM PROGRAM TAPS in to user data of Apple, google and others. The Guardian. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

PRISM is a US NSA program. It was initiated in 2007 under the Protect America Act. It collects internet communications from American internet companies such as Google LLC and Apple through court approved search teams. Snowden, an NSA contractor exposed PRISM by leaking classified documents to the Washington Post in the Galgian in 2013 while he was in Hong Kong. The leaked information implicated major tech companies in the program and revealed that much of the world's electronic communications passed through the US offering intelligence agencies opportunities for intercepting foreign communications also.



- Snowden also disclosed similar surveillance activities by the UK's GCHQ and alleged dangerous practices, including hacking civilian infrastructure networks and weak compliance measures in the NSA.

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Collection Details

Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) REPRISMFISA TIPS
(https:[redacted]

REPRISMFISA COUNTERTERRORISM

PRISM ENTRIES

Prism Current Entries

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) A Week in the Life of PRISM Reporting
Sampling of Reporting Topics from 2-8 Feb 2013

- Venezuela
- Military procurement
- Oil

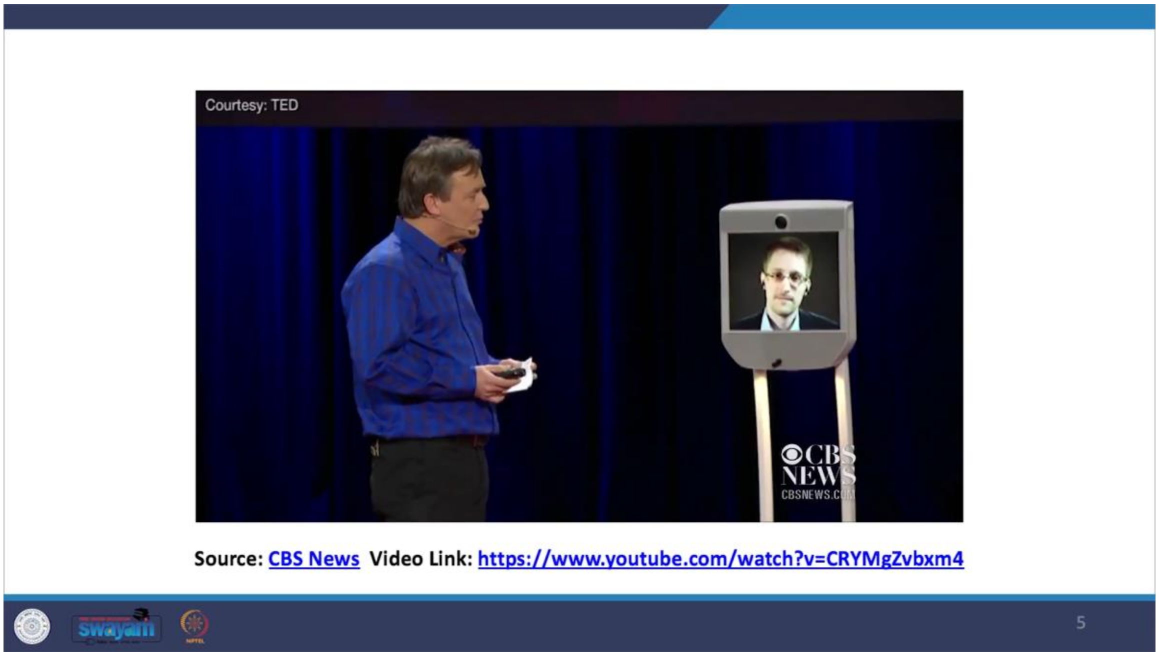
- Mexico
- Narcotics
- Energy
- Internal security
- Political Affairs

- Colombia
- Trafficking
- FARC

Source: https://www.theguardian.com

Snowden had also disclosed similar surveillance activities by the UK's GCHQ and alleged dangerous practices including hacking civilian infrastructure networks and weak compliance measures in the NSA.

Snowden's revelations shed light on the extent of mass data gathering and ignited a global debate about the balance between national security and privacy rights of an individual in the digital age. In the following video, Snowden discusses the PRISM program.



Source: CBS News **Video Link:** https://www.youtube.com/watch?v=CRYMgZvbxm4

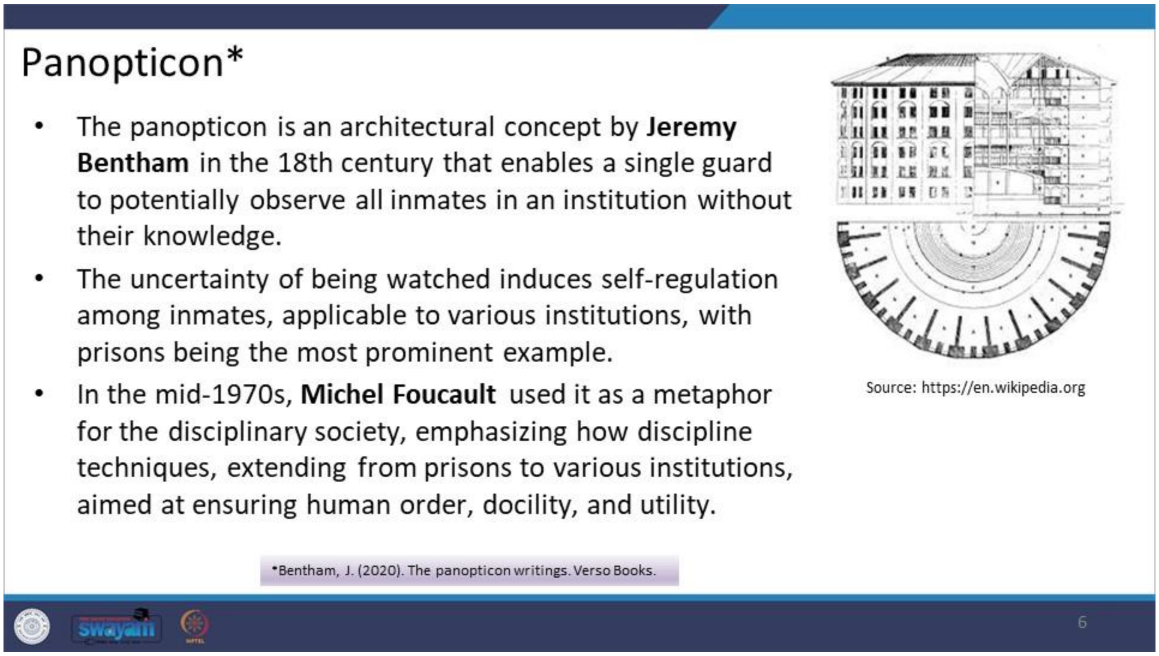
Let me show the audience a couple of examples of what you revealed. If you can have a slide up and Ed, I do not know whether you can see. The slides are here. This is a slide of the PRISM program and maybe you could tell the audience what that was that was revealed. The best way to understand PRISM, because there's been a little bit of controversy, is to first talk about what PRISM is.

Much of the debate in the US has been about metadata. They've said it's just metadata. It's just metadata and they're talking about a specific legal authority called Section 215 of the Patriot Act. That allows sort of a warrantless wiretapping mass surveillance of the entire country's sort of phone records, things like that. Who you're talking to, when you're talking to them, where you travel, these are all metadata events.

PRISM is about content. It's a program through which the government could compel corporate America. It could sort of deputize corporate America to do its dirty work for the NSA. Even though some of these companies did resist, even though some of them, I believe Yahoo was one of them, challenged them in court, they all lost because it was never tried by an open court. They were only tried by a secret court.

Something that we've seen, something about the PRISM program that's very concerning to me is there's been a talking point in the US government where they've said 15 federal judges have reviewed these programs and found them to be lawful. What they don't tell you is those are secret judges in a secret court based on secret interpretations of law that's considered 34,000 warrant requests over 33 years and in 33 years only rejected 11 government requests. These aren't the people that we want deciding what the role of corporate America in a free and open internet should be.

PRISM primarily focuses on content rather than just metadata, allowing the government to compel corporations to cooperate with the NSA in conducting surveillance activities. The video sheds light on concerns about secret court proceedings, lack of transparency and the influence of corporate America on the freedom of the internet. Government surveillance as depicted by Snowden in his case shares similarities with the concept of the panopticon as both involve pervasive monitoring. The panopticon's design seeks compliance through the perception of constant scrutiny reflecting the control of surveillance agents over others through the simple fear of being watched continuously.



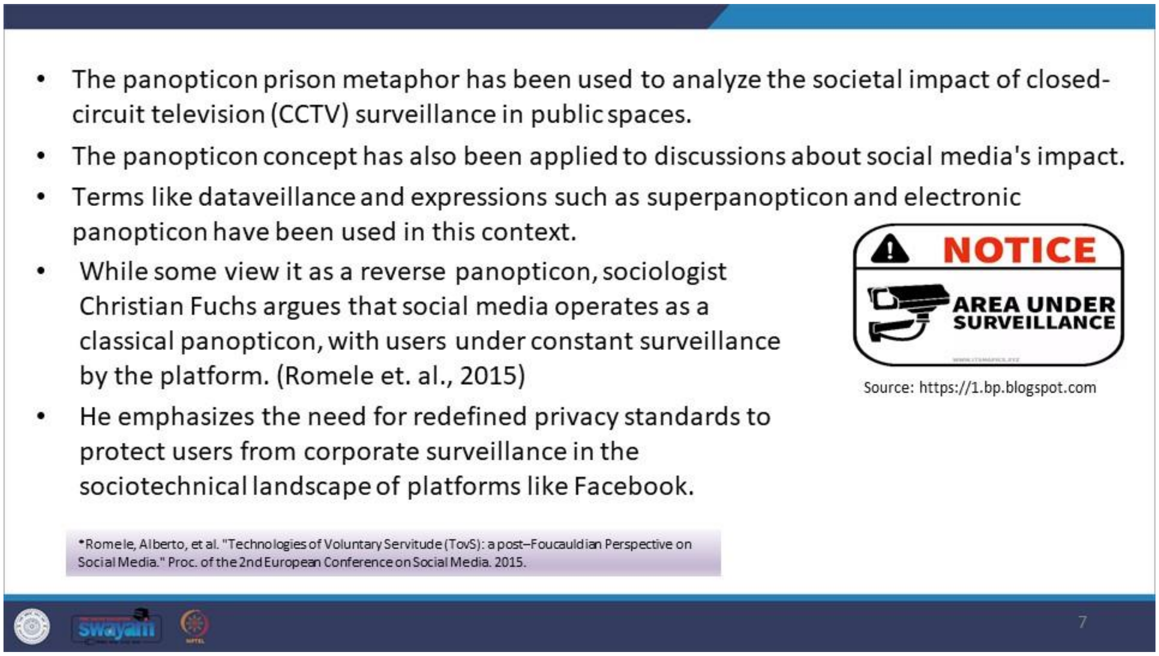
Panopticon*

- The panopticon is an architectural concept by **Jeremy Bentham** in the 18th century that enables a single guard to potentially observe all inmates in an institution without their knowledge.
- The uncertainty of being watched induces self-regulation among inmates, applicable to various institutions, with prisons being the most prominent example.
- In the mid-1970s, **Michel Foucault** used it as a metaphor for the disciplinary society, emphasizing how discipline techniques, extending from prisons to various institutions, aimed at ensuring human order, docility, and utility.

Source: https://en.wikipedia.org

*Bentham, J. (2020). The panopticon writings. Verso Books.

The panopticon is an architectural concept by the famous 18th century utilitarian philosopher Jeremy Bentham. It enabled a single guard to potentially observe all inmates in an institution without their knowledge. The uncertainty of being watched induces self-regulation among inmates. It may be applicable to various institutions like schools, a mine where several workers are working, different types of organizations for security purpose. But it was with prison that it became the most prominent example of discipline simply by observation. In the mid-1970s Michel Foucault used it as a metaphor for the disciplinary society emphasizing how discipline techniques extending from prisons to various institutions are aiming at ensuring human order, docility as well as utility.



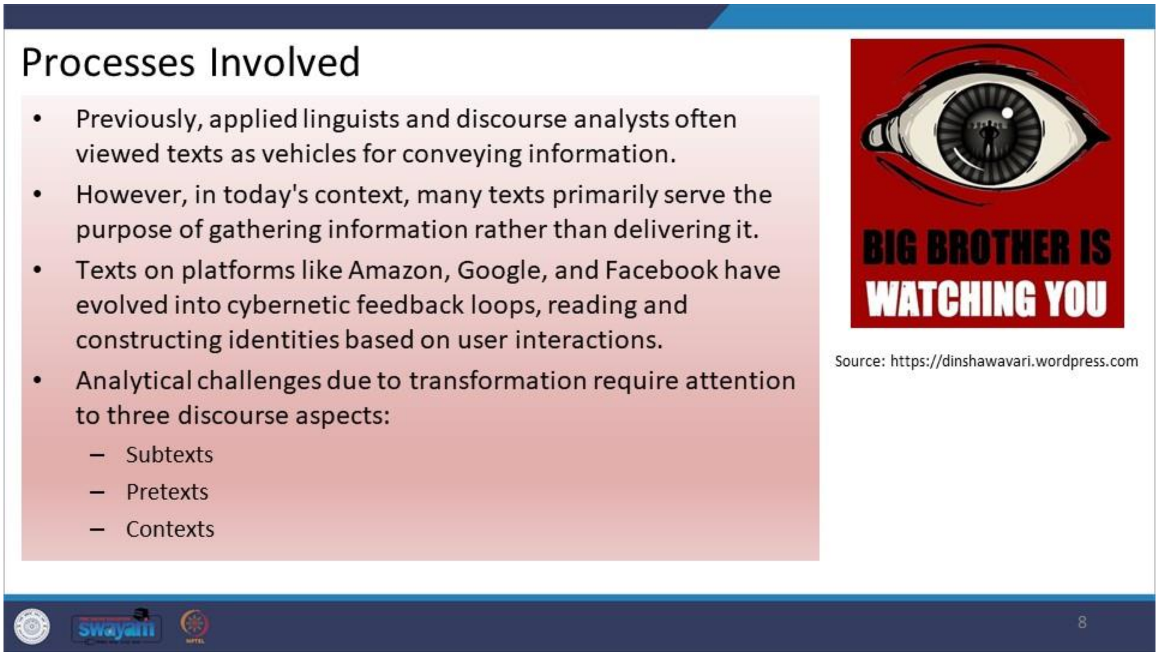
- The panopticon prison metaphor has been used to analyze the societal impact of closed-circuit television (CCTV) surveillance in public spaces.
- The panopticon concept has also been applied to discussions about social media's impact.
- Terms like dataveillance and expressions such as superpanopticon and electronic panopticon have been used in this context.
- While some view it as a reverse panopticon, sociologist Christian Fuchs argues that social media operates as a classical panopticon, with users under constant surveillance by the platform. (Romele et. al., 2015)
- He emphasizes the need for redefined privacy standards to protect users from corporate surveillance in the sociotechnical landscape of platforms like Facebook.

Source: https://1.bp.blogspot.com

*Romele, Alberto, et al. "Technologies of Voluntary Servitude (TovS): a post–Foucauldian Perspective on Social Media." Proc. of the 2nd European Conference on Social Media. 2015.

The panopticon prison metaphor has been used to analyze the societal impact of closed circuit television surveillance in public spaces. The panopticon concept has also been applied to discussions about the impact of the social media. Terms like data valence and expressions such as super panopticon and electronic panopticon have also been used in this context. While some people view it as a reverse panopticon, sociologist Christian Fuchs argues that social media operates as a classical panopticon with users under constant surveillance by the platform. He emphasizes the need for redefined privacy standards to protect users from corporate surveillance in the socio-technical landscape of platforms like Facebook.

Christian Fuchs suggested that on digital platforms, audience are turned into productive users as they continuously create social use values. In turn, social use value is objectified in user generated content that includes textual postings, videos, images, comments, etc. These postings are done on advertising based platforms and this data is then sold to advertising clients who are enabled to present targeted ads on our social media platforms. The more time we spend on such targeted ad platforms, the more data we produce that is commodified. Consequently, commercials, search engines and social media texts construct discourse positions and social identities based on user interactions.



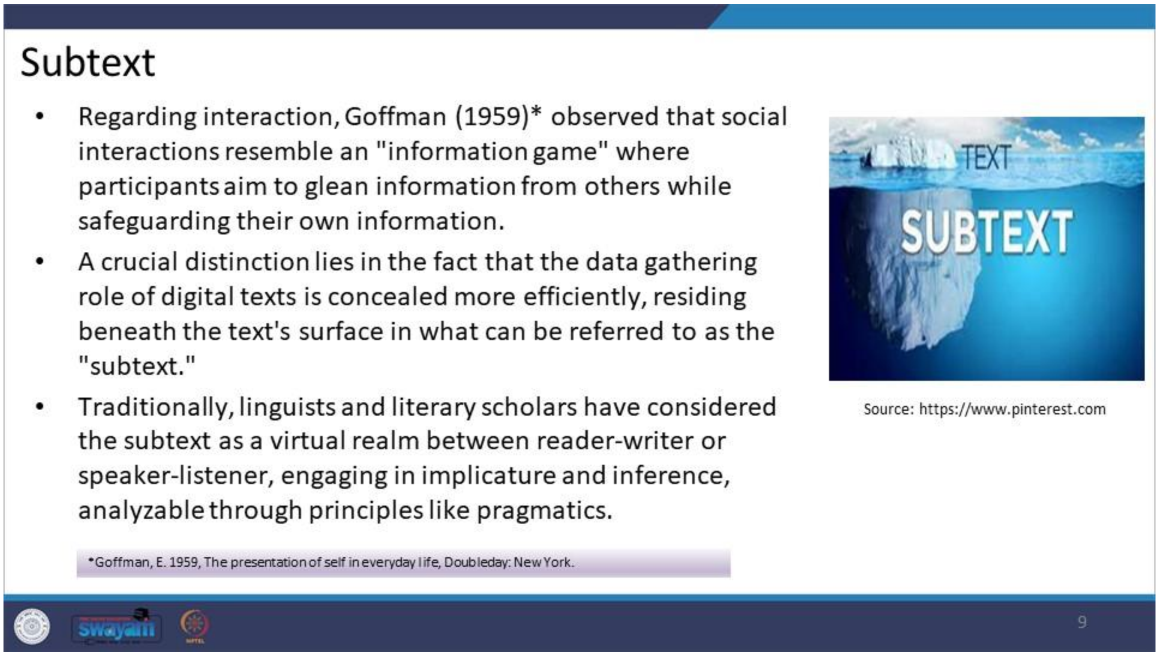
Processes Involved

- Previously, applied linguists and discourse analysts often viewed texts as vehicles for conveying information.
- However, in today's context, many texts primarily serve the purpose of gathering information rather than delivering it.
- Texts on platforms like Amazon, Google, and Facebook have evolved into cybernetic feedback loops, reading and constructing identities based on user interactions.
- Analytical challenges due to transformation require attention to three discourse aspects:
  - Subtexts
  - Pretexts
  - Contexts

Source: https://dinshawavari.wordpress.com

Previously, it was applied linguists and discourse analysts who often viewed texts as vehicles for conveying information. However, in today's digital context, many texts primarily serve the purpose of gathering information rather than delivering it. Text on platforms like Amazon, Google and Facebook have evolved into cybernetic feedback loops, reading and constructing identities based on user interactions. Analytical challenges due to transformation require our attention to three different aspects of the discourse, namely subtexts, pretexts and contexts.

Subtext and surveillance refers to the hidden underlying messages and intentions that surveillance activities convey. While overtly about data collection, subtext often involves control, power dynamics and intrusion into the privacy of the audience.



Subtext

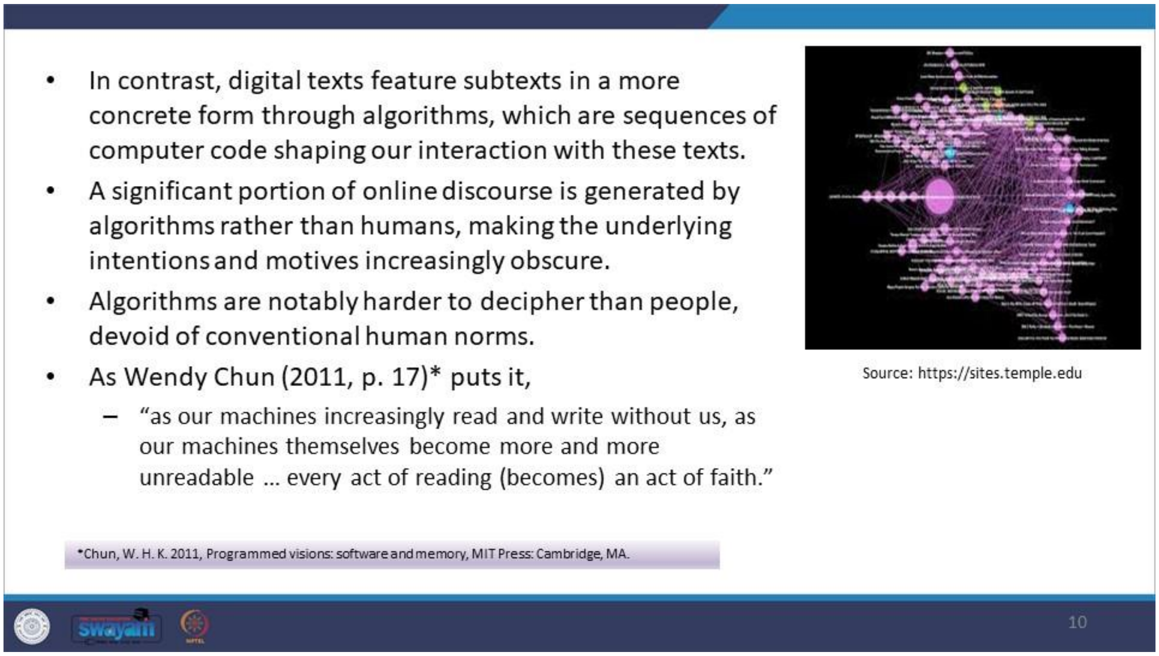
- Regarding interaction, Goffman (1959)* observed that social interactions resemble an "information game" where participants aim to glean information from others while safeguarding their own information.
- A crucial distinction lies in the fact that the data gathering role of digital texts is concealed more efficiently, residing beneath the text's surface in what can be referred to as the "subtext."
- Traditionally, linguists and literary scholars have considered the subtext as a virtual realm between reader-writer or speaker-listener, engaging in implicature and inference, analyzable through principles like pragmatics.

Source: https://www.pinterest.com

*Goffman, E. 1959, The presentation of self in everyday life, Doubleday: New York.

We may refer to the work of Goffman in the context of digital interaction. Goffman had observed that social interactions resemble an information game where participants aim to glean information from others while safeguarding their own information. A crucial distinction lies in the fact that the data gathering role of digital texts is concealed more efficiently residing beneath the text surface in what can be referred to as the subtext. Traditionally, linguists and literary scholars have considered the subtext as a virtual realm between reader-writer or speaker-listener engaging in implicature and inference, analyzable through principles like pragmatics.

While in conventional communication, we have talked about messages and meta messages, digital communication is entirely different as it uses algorithms for this purpose. Digital text features subtexts in a more concrete form through algorithms which are sequences of computer code shaping our interaction with these texts.



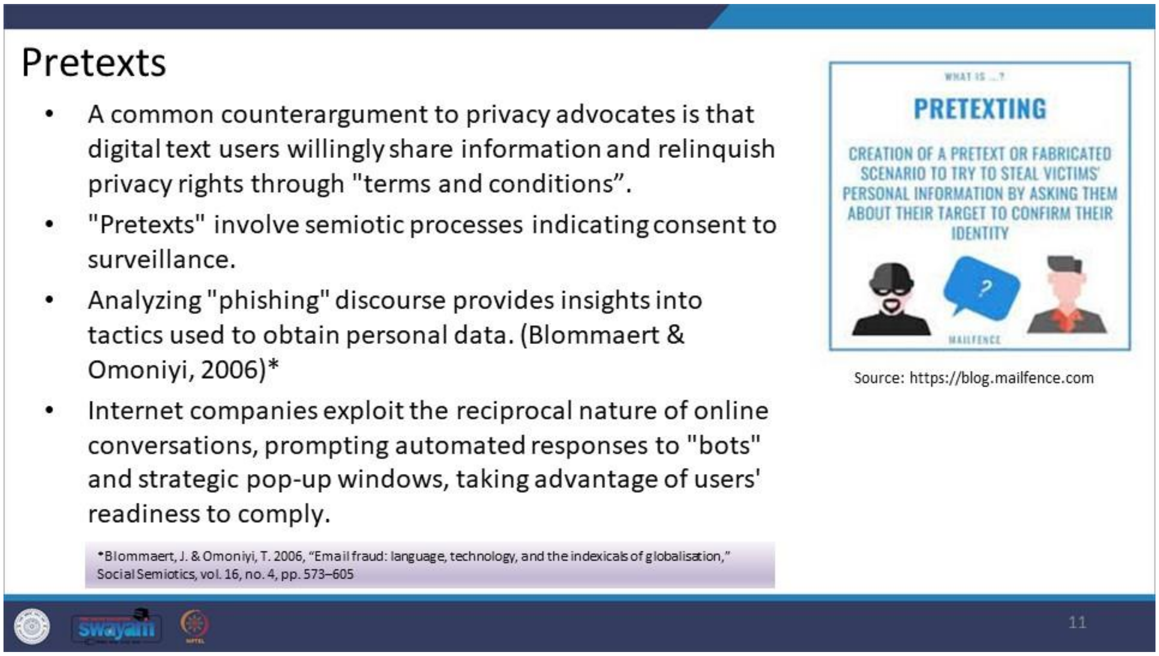
- In contrast, digital texts feature subtexts in a more concrete form through algorithms, which are sequences of computer code shaping our interaction with these texts.
- A significant portion of online discourse is generated by algorithms rather than humans, making the underlying intentions and motives increasingly obscure.
- Algorithms are notably harder to decipher than people, devoid of conventional human norms.
- As Wendy Chun (2011, p. 17)* puts it,
  - "as our machines increasingly read and write without us, as our machines themselves become more and more unreadable ... every act of reading (becomes) an act of faith."

Source: https://sites.temple.edu

*Chun, W. H. K. 2011, Programmed visions: software and memory, MIT Press: Cambridge, MA.

A significant portion of online discourse is generated by algorithms rather than by humans making the underlying intentions and motives increasingly obscure. Algorithms are notably harder to decipher in comparison to the deciphering of the people and it is devoid of conventional human norms. As Van Der Schoen has pointed out and I quote, as our machines increasingly read and write about us, as our machines themselves become more and more unreadable, every act of reading becomes an act of faith, unquote.

Similarly, pretext in surveillance involve using fabricated or misleading reasons to justify data collection. It is a way for entities to gain access without revealing their true intentions and it often violates the basic concepts and the ethical considerations regarding the privacy of the social media users.



Pretexts

- A common counterargument to privacy advocates is that digital text users willingly share information and relinquish privacy rights through "terms and conditions".
- "Pretexts" involve semiotic processes indicating consent to surveillance.
- Analyzing "phishing" discourse provides insights into tactics used to obtain personal data. (Blommaert & Omoniyi, 2006)*
- Internet companies exploit the reciprocal nature of online conversations, prompting automated responses to "bots" and strategic pop-up windows, taking advantage of users' readiness to comply.

*Blommaert, J. & Omoniyi, T. 2006, "Email fraud: language, technology, and the indexicals of globalisation," Social Semiotics, vol. 16, no. 4, pp. 573–605

WHAT IS ...?

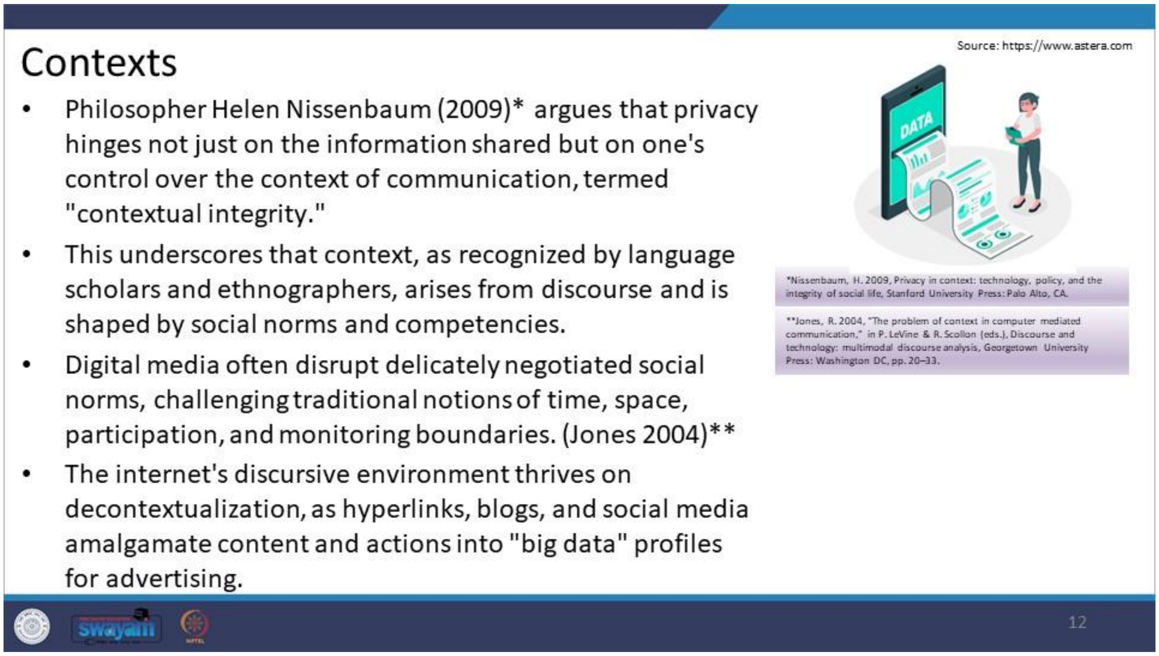
PRETEXTING

CREATION OF A PRETEXT OR FABRICATED SCENARIO TO TRY TO STEAL VICTIMS' PERSONAL INFORMATION BY ASKING THEM ABOUT THEIR TARGET TO CONFIRM THEIR IDENTITY

Source: https://blog.mailfence.com

Let us look at pretext now. A common counter argument to privacy advocates is that digital text users willingly share information and relinquish privacy rights through terms and conditions. Texts involve semiotic processes indicating consent to surveillance. Analysing phishing discourse provides insights into tactics used to obtain our personal data. Internet companies exploit the reciprocal nature of online conversations prompting automated responses to bots and strategic pop-up windows taking advantage of the user's readiness to comply.

And finally, context in surveillance refers to various circumstances and environments in which monitoring and data collection occur. These settings and situations play a crucial role in shaping the surveillance process and its implications.



Contexts

- Philosopher Helen Nissenbaum (2009)* argues that privacy hinges not just on the information shared but on one's control over the context of communication, termed "contextual integrity."
- This underscores that context, as recognized by language scholars and ethnographers, arises from discourse and is shaped by social norms and competencies.
- Digital media often disrupt delicately negotiated social norms, challenging traditional notions of time, space, participation, and monitoring boundaries. (Jones 2004)**
- The internet's discursive environment thrives on decontextualization, as hyperlinks, blogs, and social media amalgamate content and actions into "big data" profiles for advertising.

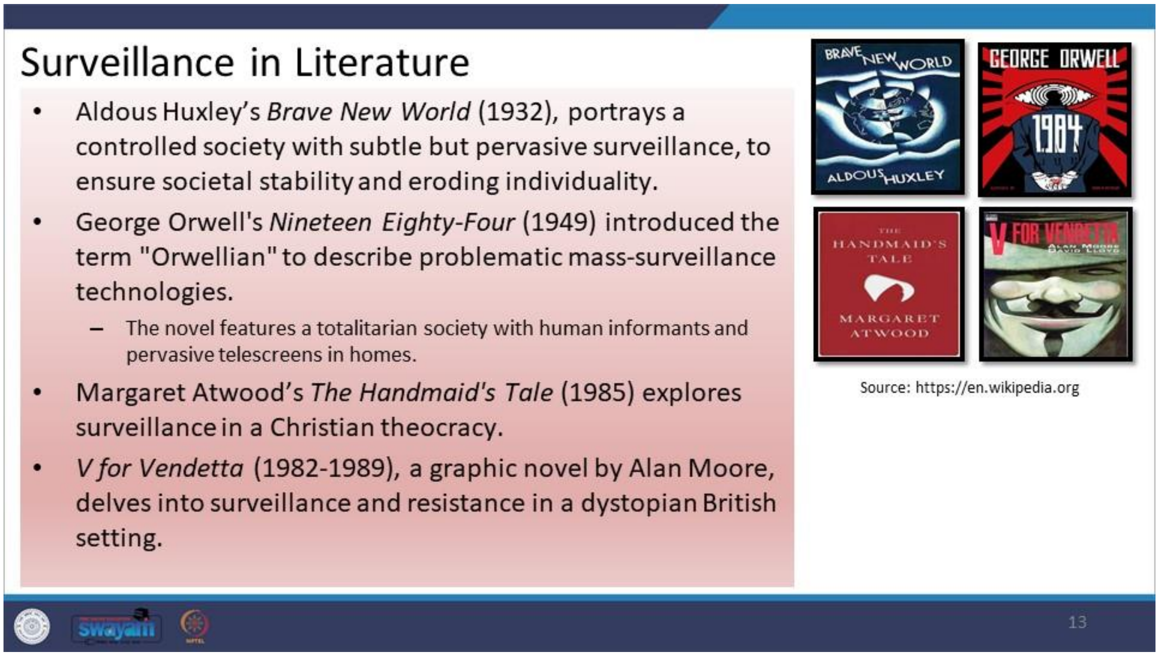
Source: https://www.astera.com

*Nissenbaum, H. 2009, Privacy in context: technology, policy, and the integrity of social life, Stanford University Press: Palo Alto, CA.

**Jones, R. 2004, "The problem of context in computer mediated communication," in P. LeVine & R. Scollon (eds.), Discourse and technology: multimodal discourse analysis, Georgetown University Press: Washington DC, pp. 20–33.

Helen Nissenbaum had argued that privacy hinges not just on the information shared but on one's control over the context of communication termed as contextual integrity. This underscores the context as recognized by language scholars and ethnographers arises from discourse and is shaped by social norms and competencies. Digital media often disrupt social norms which are rather delicately negotiated and it challenges the traditional notions of time, space, participation as well as how do we monitor the boundaries. The internet's discursive environment thrives on decontextualization as hyperlinks, blogs and social media amalgamate content and actions into big data profile for advertising.

In literature, surveillance serves as a powerful tool for exploring the dynamics of power and control within a society while raising essential questions about privacy. It often delves into the manipulation and oppression that can result from extensive monitoring.



Surveillance in Literature

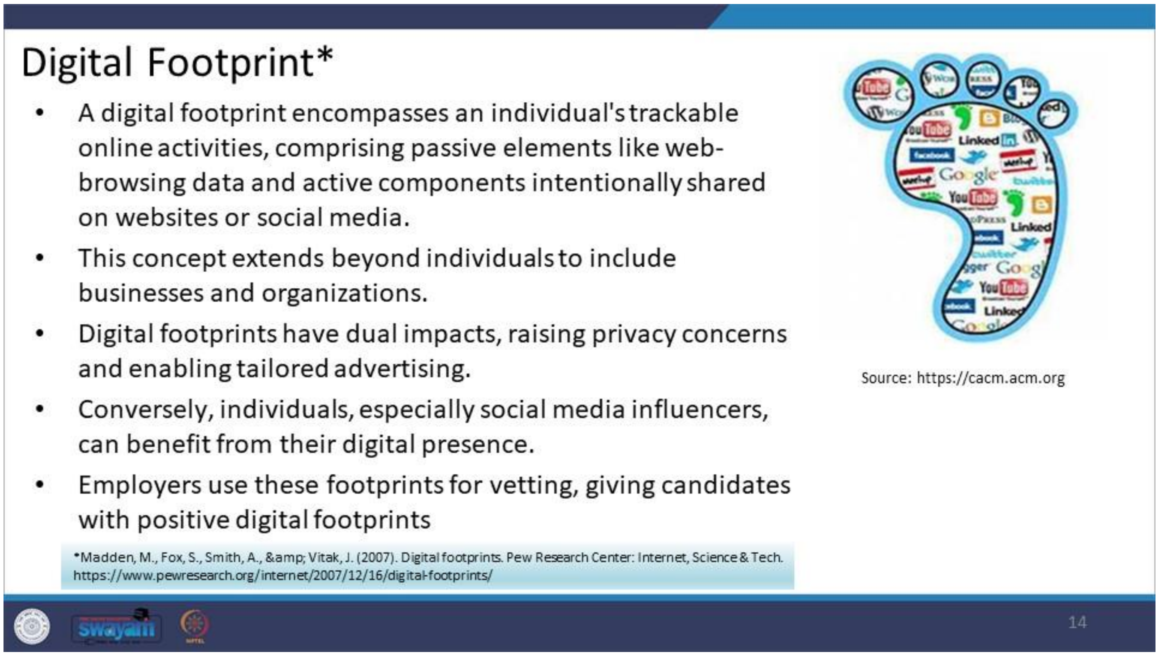
- Aldous Huxley’s *Brave New World* (1932), portrays a controlled society with subtle but pervasive surveillance, to ensure societal stability and eroding individuality.
- George Orwell's *Nineteen Eighty-Four* (1949) introduced the term "Orwellian" to describe problematic mass-surveillance technologies.
  - The novel features a totalitarian society with human informants and pervasive telescreens in homes.
- Margaret Atwood’s *The Handmaid's Tale* (1985) explores surveillance in a Christian theocracy.
- *V for Vendetta* (1982-1989), a graphic novel by Alan Moore, delves into surveillance and resistance in a dystopian British setting.

Source: https://en.wikipedia.org

We can refer to several famous texts in this context. Aldous Huxley's Babe New World published in 1932 had portrayed a controlled society with subtle but pervasive surveillance to ensure social stability and eroding individuality. One of the most famous examples is perhaps George Orwell's 1984 published in 1949 which had introduced the term Orwellian to describe problematic mass surveillance technologies. Atwood's Handmaid's Tale published in 1985 also explores surveillance in a Christian theocracy. V for Vendetta which is a graphic novel by Ellen Moore also looks into surveillance and resistance in a dystopian British setting.

These dystopian literary works anticipated a world where surveillance technology is used to control and manipulate individuals, eroding personal freedoms and the concept of privacy. These literary warnings serve as cautionary tales and continue to be relevant in today's society.

Digital footprints also wield significant influence in shaping perceptions and also conditioning the opportunities available to us. A positive digital footprint can open doors while a negative one may close them. As technology advances understanding and managing digital footprints has become vital.



Digital Footprint*

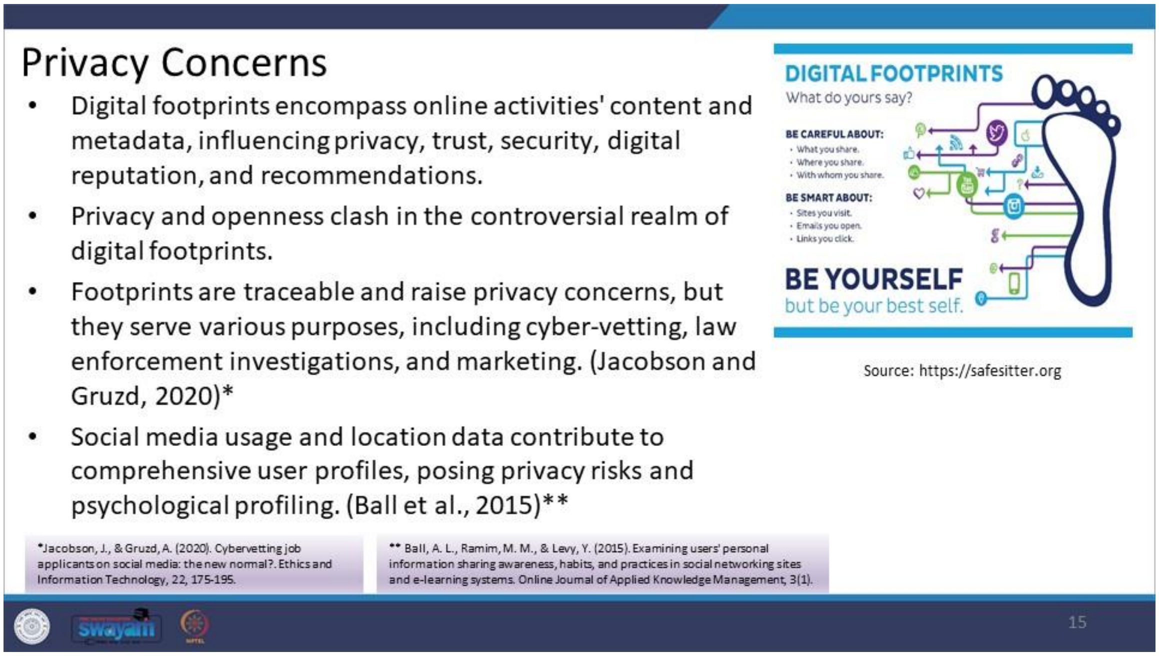
- A digital footprint encompasses an individual's trackable online activities, comprising passive elements like web-browsing data and active components intentionally shared on websites or social media.
- This concept extends beyond individuals to include businesses and organizations.
- Digital footprints have dual impacts, raising privacy concerns and enabling tailored advertising.
- Conversely, individuals, especially social media influencers, can benefit from their digital presence.
- Employers use these footprints for vetting, giving candidates with positive digital footprints

Source: https://cacm.acm.org

*Madden, M., Fox, S., Smith, A., &amp; Vitak, J. (2007). Digital footprints. Pew Research Center: Internet, Science & Tech. https://www.pewresearch.org/internet/2007/12/16/digital-footprints/

So, what are the digital footprints? They encompass an individual's trackable online activities comprising passive elements like web browsing data and active components intentionally shared on websites or social media platforms. This concept extends beyond individuals to include businesses and organizations. Digital footprints have dual impacts raising privacy concerns and enabling tailored advertising. Conversely, individuals especially social media influencers can benefit from their digital presence. Possible employers use these footprints for vetting imparting candidates with positive digital footprints a better chance.

Digital footprints raise substantial privacy concerns as they encompass a wide array of personal information. These traces of online activities can be exploited for surveillance, identity theft or even manipulation.



Privacy Concerns

- Digital footprints encompass online activities' content and metadata, influencing privacy, trust, security, digital reputation, and recommendations.
- Privacy and openness clash in the controversial realm of digital footprints.
- Footprints are traceable and raise privacy concerns, but they serve various purposes, including cyber-vetting, law enforcement investigations, and marketing. (Jacobson and Gruzd, 2020)*
- Social media usage and location data contribute to comprehensive user profiles, posing privacy risks and psychological profiling. (Ball et al., 2015)**

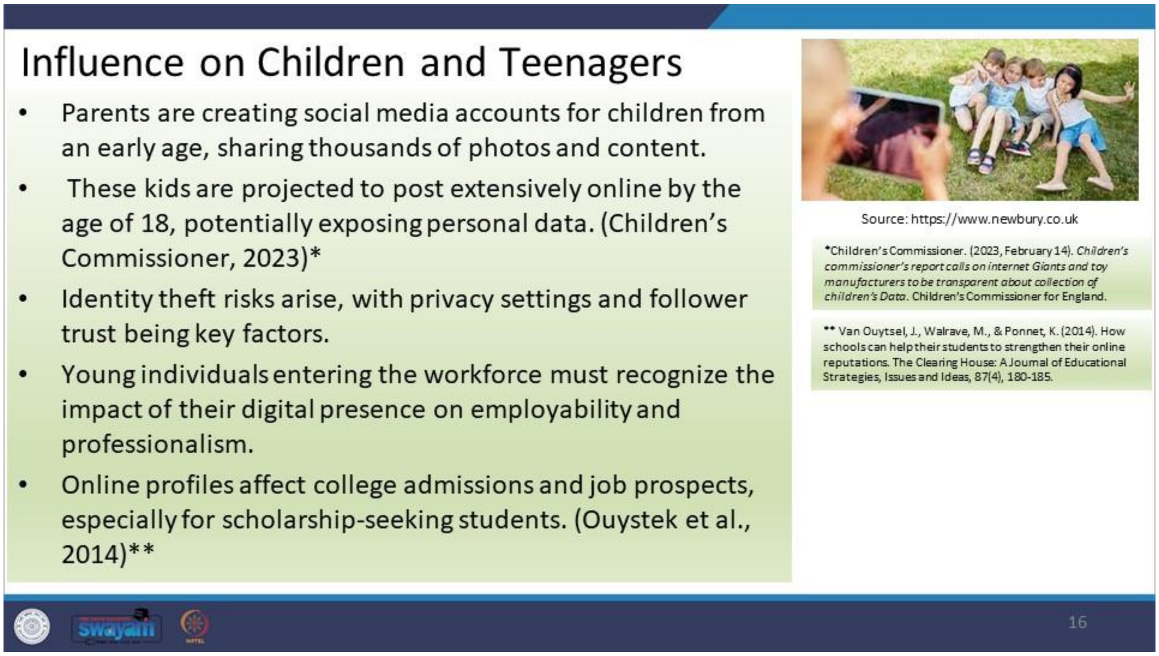
Source: https://safesitter.org

*Jacobson, J., & Gruzd, A. (2020). Cybervetting job applicants on social media: the new normal?. Ethics and Information Technology, 22, 175-195.

** Ball, A. L., Ramim, M. M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. Online Journal of Applied Knowledge Management, 3(1).

Digital footprints encompass online activities content and metadata influencing privacy, trust, security, digital reputation and recommendations. Privacy and openness clash in the controversial realm of digital footprints. These footprints are traceable and raise privacy concerns but they serve various purposes including cyber vetting, law enforcement investigations as well as marketing. Social media usage and location data contribute to comprehensive user profile posing privacy risk and psychological profiling.

Digital footprints significantly influence children and teenagers as their online activities are more closely observed by colleges and potential employers, underscoring the importance of responsible online behaviour at a young age.



Influence on Children and Teenagers

- Parents are creating social media accounts for children from an early age, sharing thousands of photos and content.
- These kids are projected to post extensively online by the age of 18, potentially exposing personal data. (Children's Commissioner, 2023)*
- Identity theft risks arise, with privacy settings and follower trust being key factors.
- Young individuals entering the workforce must recognize the impact of their digital presence on employability and professionalism.
- Online profiles affect college admissions and job prospects, especially for scholarship-seeking students. (Ouystek et al., 2014)**

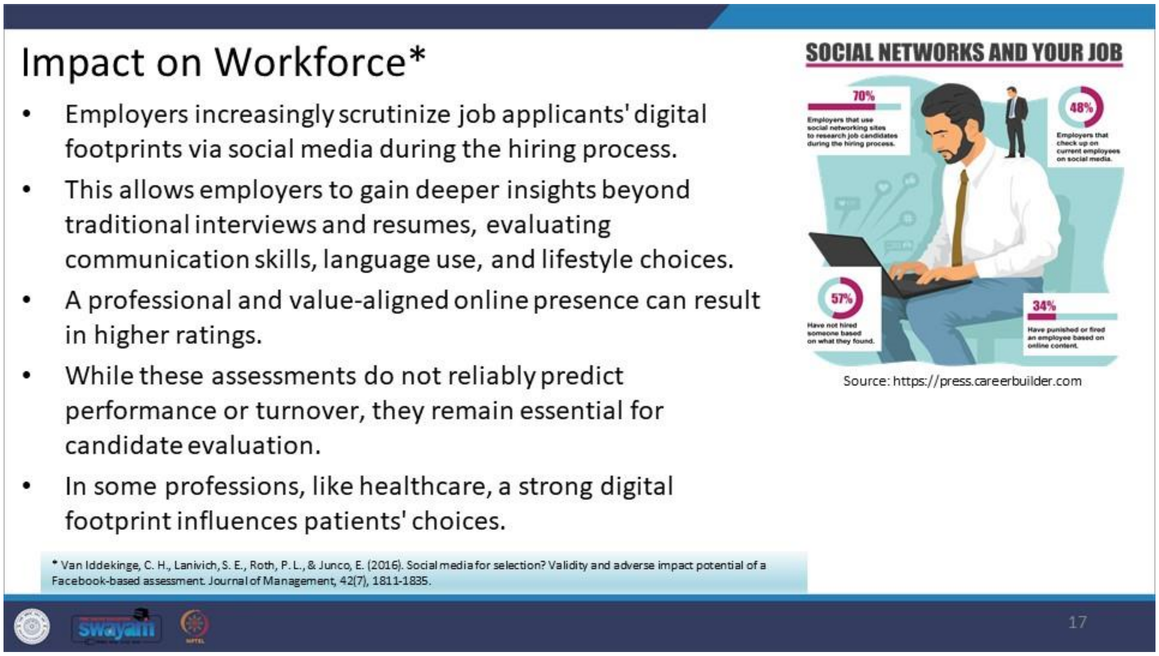
Source: https://www.newbury.co.uk

*Children's Commissioner. (2023, February 14). *Children's commissioner's report calls on internet Giants and toy manufacturers to be transparent about collection of children's Data*. Children's Commissioner for England.

** Van Ouytsel, J., Walrave, M., & Ponnet, K. (2014). How schools can help their students to strengthen their online reputations. The Clearing House: A Journal of Educational Strategies, Issues and Ideas, 87(4), 180-185.

So, what is the influence of digital footprints on young children as well as teenagers? We find that nowadays parents are creating social media accounts for children from a very early age sharing thousands of photographs and content. These kids are projected to post extensively online by the age of 18 potentially exposing their personal data. Identity theft risk with privacy settings and follower trust being the key factors in this context. Young individuals entering the workforce must recognize the impact of their digital presence on employability and professionalism. Online profiles affect college admissions and job prospects especially for those students who seek scholarships.

Similarly, digital footprints significantly affect the workforce with employers increasingly scrutinizing applicants' online profiles.



Impact on Workforce*

- Employers increasingly scrutinize job applicants' digital footprints via social media during the hiring process.
- This allows employers to gain deeper insights beyond traditional interviews and resumes, evaluating communication skills, language use, and lifestyle choices.
- A professional and value-aligned online presence can result in higher ratings.
- While these assessments do not reliably predict performance or turnover, they remain essential for candidate evaluation.
- In some professions, like healthcare, a strong digital footprint influences patients' choices.

SOCIAL NETWORKS AND YOUR JOB
70%
Employers that use social networking sites to research job candidates during the hiring process.
48%
Employers that check up on current employees on social media.
57%
Have not hired someone based on what they found.
34%
Have punished or fired an employee based on online content.

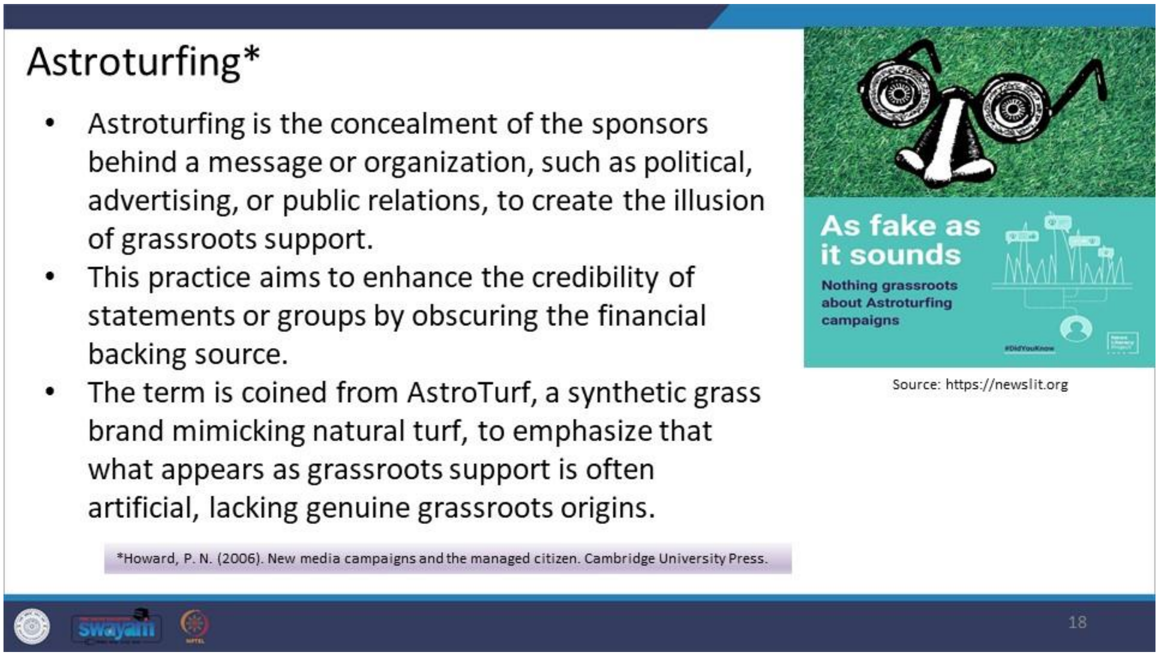
Source: https://press.careerbuilder.com

* Van Iddekinge, C. H., Lanivich, S. E., Roth, P. L., & Junco, E. (2016). Social media for selection? Validity and adverse impact potential of a Facebook-based assessment. Journal of Management, 42(7), 1811-1835.

Digital footprints of prospective candidates are assessed with a sense of scrutiny during the hiring process itself and this allows employers to gain a deeper insight beyond traditional interviews and resumes. They also get an opportunity to evaluate the semi-formal communication skills, use of language as well as lifestyle choices and ideological preferences or biases. A professional and value aligned online presence can result in higher ratings. While these assessments do not reliably predict performance or turnover, they remain essential for candidate evaluation. In some professions like healthcare etc., a strong digital footprint influences the choices of the patient.

Thus, a positive online presence can enhance one's prospects while a negative footprint may hinder certain career opportunities.

Simultaneously astroturfing that is disguised advocacy, masquerading as grassroot support poses a credible threat to honest public discourse. It undermines trust, influences opinions and hampers consumers' ability to distinguish between genuine and manipulated information ultimately impacting decision making.



Astroturfing*

- Astroturfing is the concealment of the sponsors behind a message or organization, such as political, advertising, or public relations, to create the illusion of grassroots support.
- This practice aims to enhance the credibility of statements or groups by obscuring the financial backing source.
- The term is coined from AstroTurf, a synthetic grass brand mimicking natural turf, to emphasize that what appears as grassroots support is often artificial, lacking genuine grassroots origins.

Source: https://newslit.org

*Howard, P. N. (2006). New media campaigns and the managed citizen. Cambridge University Press.

Astroturfing is the concealment of the sponsors behind a message or organization such as political advertising or public relations to create the illusion of grassroots support. The practice aims to enhance the credibility of statements or groups by obscuring the financial backing source. The term is coined from astroturf that is a synthetic grass brand mimicking natural turf to emphasize that what appears is grassroots support is often artificial lacking genuine grassroots origin.

In the next slide we have a video that discusses the practice of astroturfing where campaigns and protests are presented as grassroots movements but are often orchestrated by well funded organizations with certain aims and manipulative tendencies.

Source: KTNV Channel 13 Las Vegas **Video Link:** https://www.youtube.com/watch?v=OOWyGbxNAts

19

The natural urge to gravitate toward information that reinforces our own views most agree that people genuinely want to be well informed. But in recent years campaigns by corporations, lobbyists and also political operatives, sowing division and suspicion now have become a common problem as we are aware. This week is News Literacy Week and our company has teamed up with the News Literacy Foundation to help you battle this misinformation. The Scripps reporter Asha Qureshi now takes a look at the disinformation move known as astroturfing. Soon after the coronavirus pandemic began, small anti-stay at home protests erupted in dozens of states around the country.

When things appear to be spontaneous and exciting and especially they're happening all over the country that tends to gain a lot of media attention. But many of these protests that appeared to be generated spontaneously were in fact manufactured by well funded organizations. The practice is known as astroturfing. Astroturfing is an effort to mobilize the mass public in a way that distances that mobilization from the person who is sponsoring it or the organization that's sponsoring it. While fake grassroots campaigns have been utilized for decades, some experts traced the first documented case of astroturfing on social media to South Korea in 2012.

Jung Hwan Yang is an assistant professor at the University of Illinois whose research focuses on data science and political communication. A lot of astroturfing campaigns happen all over the internet. It's not just on Twitter or Facebook. It's on Wikipedia.

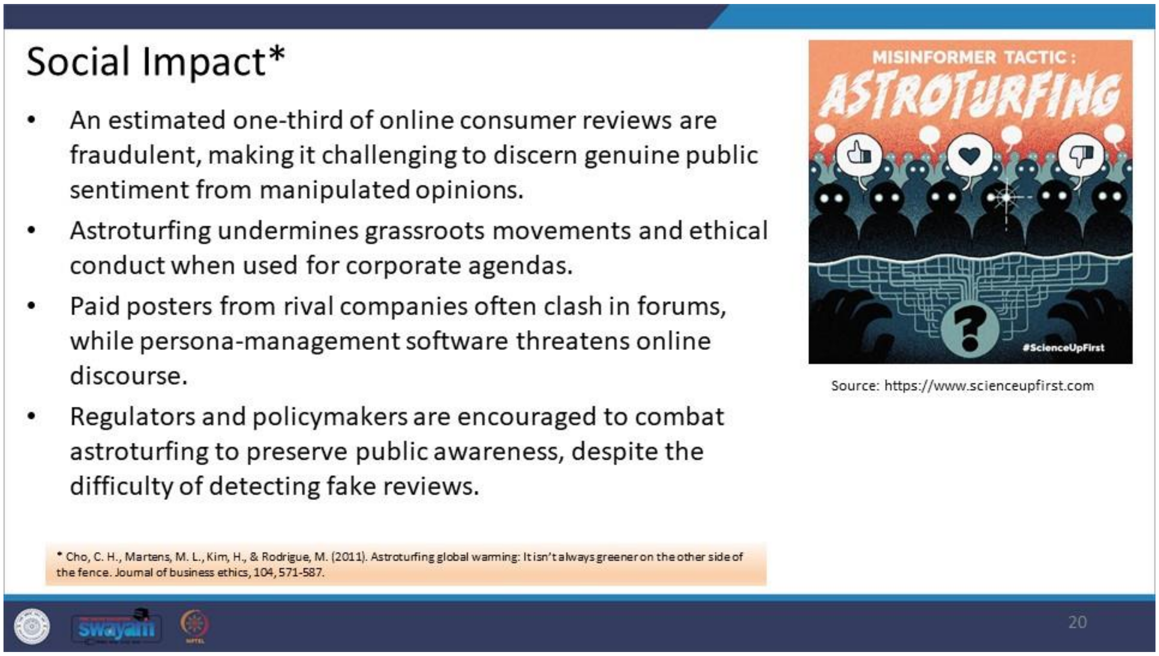
It's on the Internet Forum and everywhere. A study from Princeton University found that there were at least 53 such influence efforts targeting 24 countries around the world from 2013 to 2018. These campaigns really do try to cover their tracks. They can often do so very effectively. Even the website domains that they use can be registered privately such that you can't tell who's behind it. Multiple cybersecurity firms investigated the Reopen America movement, finding that domains were being batch registered within seconds of each other.

They were subsequently traced back to state-based firearms coalitions and ultimately to a pro-gun Iowa family. Once a couple of accounts become really popular, they can gather thousands of followers. Then they can use that platform to spread disinformation. Experts say it's difficult to identify astroturfing campaigns without deep cyber forensics. We're essentially pointing a fire hose of information at people all the time and expecting them to do a lot of heavy lifting and sifting and so on.

And that seems to be a lot to ask. One way to do that, she says, is to watch for messaging that strikes a nerve or sparks an immediate visceral response. The fact that you're having that emotional reaction means it's time to stop and think about what that message is trying to do. Experts say it's important to vet sources as much as possible. Look at account history, language and messaging. Just because an issue appears to have an organic groundswell of support doesn't mean the strings aren't being pulled by a concealed group.

Amasha Qureshi reporting.

The video highlights the challenges of identifying such efforts and the importance of vigilant source vetting to combat misinformation. Astroturfing impacts society by distorting the authenticity of public sentiment and supporting hidden agendas. It does erode trust in online interactions and also undermines the credibility of genuine grassroot movements which are essential in a healthy democratic discourse.



Social Impact*

- An estimated one-third of online consumer reviews are fraudulent, making it challenging to discern genuine public sentiment from manipulated opinions.
- Astroturfing undermines grassroots movements and ethical conduct when used for corporate agendas.
- Paid posters from rival companies often clash in forums, while persona-management software threatens online discourse.
- Regulators and policymakers are encouraged to combat astroturfing to preserve public awareness, despite the difficulty of detecting fake reviews.

Source: https://www.scienceupfirst.com

* Cho, C. H., Martens, M. L., Kim, H., & Rodrigue, M. (2011). Astroturfing global warming: It isn't always greener on the other side of the fence. Journal of business ethics, 104, 571-587.

It is suggested that an estimated one third of online consumer reviews are fraudulent and it makes it challenging to discern genuine public sentiment from manipulated opinions. Astroturfing undermines grassroot movements and ethical conduct when used for corporate agenda. Paid posters from rival companies often clash in forums while persona management software threatens online discourse. Regulators and policy makers are encouraged to combat astroturfing to preserve public awareness despite the difficulty of detecting fake reviews.

Additionally, astroturfing contributes to algorithmic radicalization by flooding social media platforms with inauthentic content that promotes extreme views.

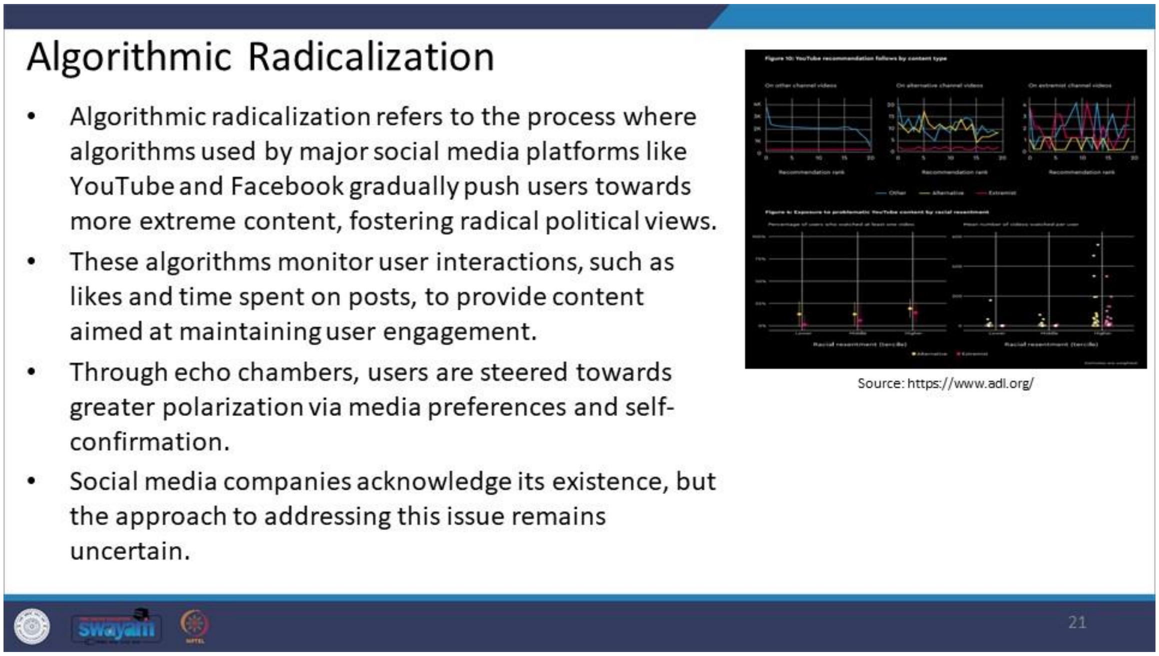


Figure 10: YouTube recommendation follows by content type
On other channel videos
On alternative channel videos
On extremist channel videos
Recommendation rank
Recommendation rank
Recommendation rank
Other
Alternative
Extremist
Figure 4: Exposure to problematic YouTube content by racial resentment
Percentage of users who watched at least one video
Mean number of videos watched per user
Lower
Middle
Higher
Racial resentment (tercile)
Racial resentment (tercile)
Alternative
Extremist

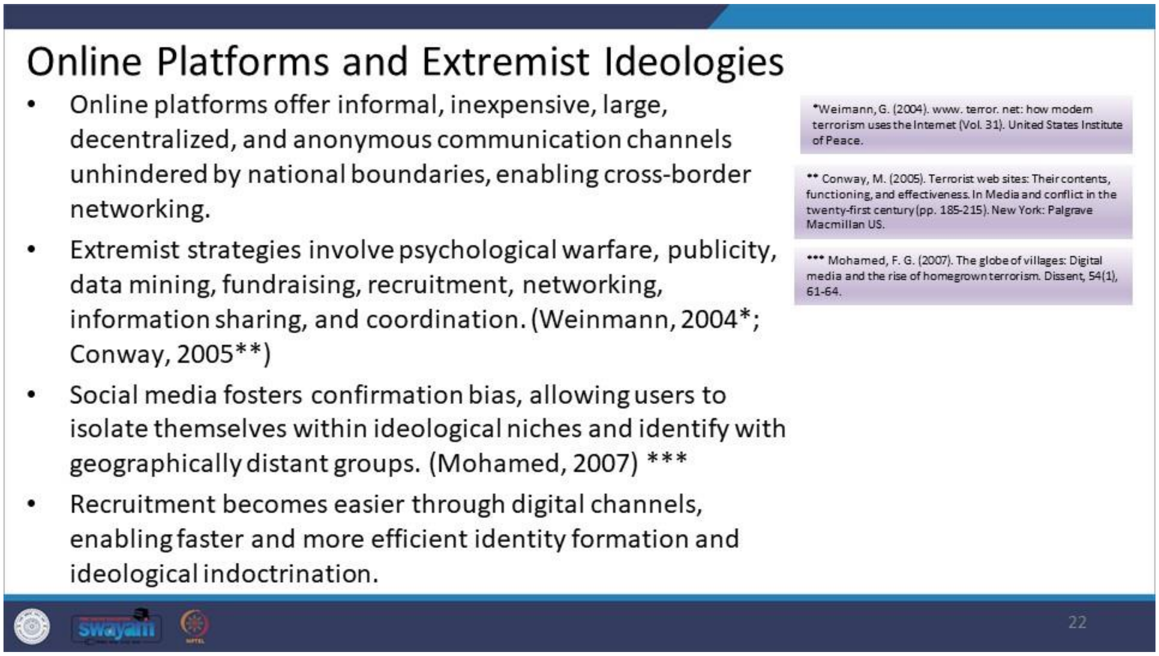
Algorithmic Radicalization

- Algorithmic radicalization refers to the process where algorithms used by major social media platforms like YouTube and Facebook gradually push users towards more extreme content, fostering radical political views.
- These algorithms monitor user interactions, such as likes and time spent on posts, to provide content aimed at maintaining user engagement.
- Through echo chambers, users are steered towards greater polarization via media preferences and self-confirmation.
- Social media companies acknowledge its existence, but the approach to addressing this issue remains uncertain.

Source: https://www.adl.org/

So how do we define algorithmic radicalization? It refers to the process where algorithms used by major social media platforms like YouTube and Facebook gradually push users towards more extreme content fostering radical political views. These algorithms monitor user interactions such as likes, and time spent on posts to provide content aimed at maintaining user engagement. Through echo chambers users are steered towards greater polarization via media preferences and self-confirmation. Social media companies acknowledge its existence but the approach to addressing this issue remains rather uncertain.

Online platforms inadvertently facilitate the spread of extremist ideologies. Platforms designed to maximize user engagement can inadvertently promote polarizing content leading users to become exposed to more extreme ideas and reinforcing pre-existing beliefs.



Online Platforms and Extremist Ideologies

- Online platforms offer informal, inexpensive, large, decentralized, and anonymous communication channels unhindered by national boundaries, enabling cross-border networking.
- Extremist strategies involve psychological warfare, publicity, data mining, fundraising, recruitment, networking, information sharing, and coordination. (Weinmann, 2004*; Conway, 2005**)
- Social media fosters confirmation bias, allowing users to isolate themselves within ideological niches and identify with geographically distant groups. (Mohamed, 2007) ***
- Recruitment becomes easier through digital channels, enabling faster and more efficient identity formation and ideological indoctrination.

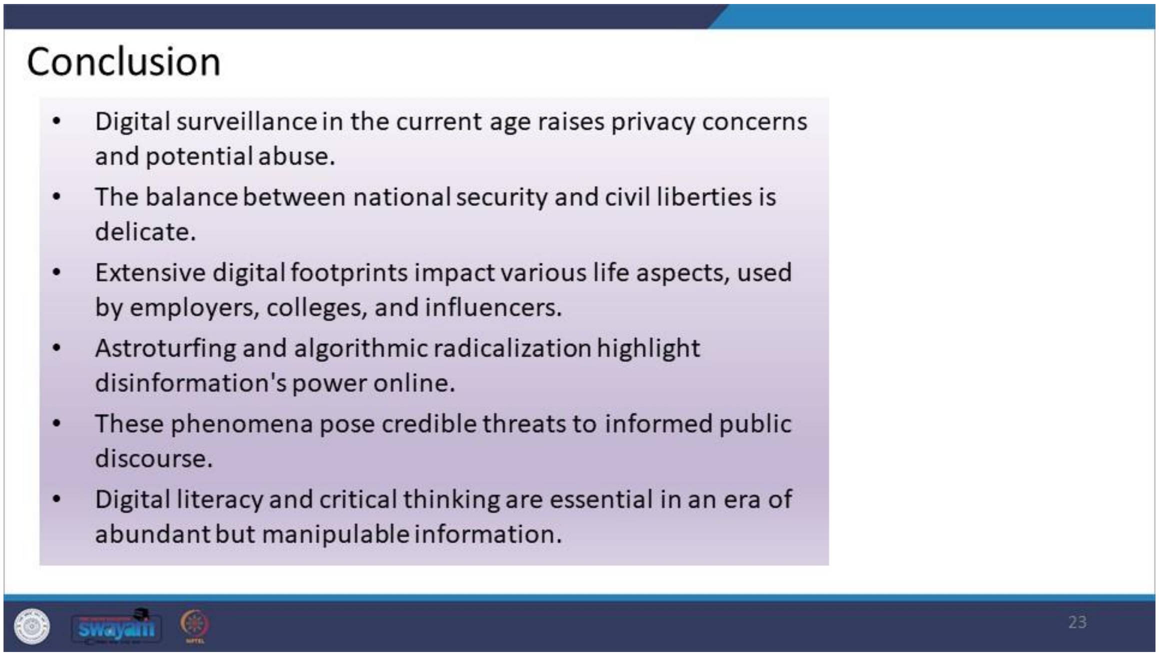
*Weimann, G. (2004). www. terror. net: how modem terrorism uses the Intemet (Vol. 31). United States Institute of Peace.

** Conway, M. (2005). Terrorist web sites: Their contents, functioning, and effectiveness. In Media and conflict in the twenty-first century (pp. 185-215). New York: Palgrave Macmillan US.

*** Mohamed, F. G. (2007). The globe of villages: Digital media and the rise of homegrown terrorism. Dissent, 54(1), 61-64.

Online platforms offer informal, inexpensive, decentralized, and anonymous communication channels which are not hindered by national boundaries and therefore cross border networking is easily enabled. Extremist strategies involve psychological warfare, publicity, data mining, fundraising, recruitment, networking, information sharing and coordination. Social media thus also fosters confirmation bias, and it allows users to isolate themselves within ideological niches and identify with geographically distant groups. Recruitment thus becomes easier through digital channels enabling faster and more efficient identity formation and ideological indoctrination.

In conclusion, the realm of online communication is captivating, but it is also a treacherous landscape. The intricate web of surveillance digital footprints, astroturfing and algorithmic radicalization weaves a complex narrative that demands our unwavering attention.



Conclusion

- Digital surveillance in the current age raises privacy concerns and potential abuse.
- The balance between national security and civil liberties is delicate.
- Extensive digital footprints impact various life aspects, used by employers, colleges, and influencers.
- Astroturfing and algorithmic radicalization highlight disinformation's power online.
- These phenomena pose credible threats to informed public discourse.
- Digital literacy and critical thinking are essential in an era of abundant but manipulable information.

To conclude we can say that digital surveillance in our age raises several concerns about privacy and also alerts us to potential abuse. The balance between national security and civil liberties remains to be a delicate one. Extensive digital footprints impact various life aspects used by employers, colleges and influencers also. Astroturfing and algorithmic radicalization highlight disinformation's power online. These phenomena pose credible threats to inform public discourse. Digital literacy and critical thinking are therefore essential in an era of abundant but manipulable information.

These threats remind us of the urgent need for media literacy, critical thinking and keen digital vigilance. In this era of boundless information the onus falls on individuals to discern the truth from the orchestrated narrative. We will be continuing our discussion on the parallels and pitfalls of communication in our digital age in the next module.

Thank you.