ISSN: 2716-9189 E-ISSN: 2676-1750
Journal of Studies in Language, Culture, and Society (JSLCS). (07) 02, 2024. (PP. 182-199)
Received: 19/07/2023 Accepted: 23/10/2024 Published: 30/10/2024

THE COOKIES' QUEST: TOWARDS DIGITAL TOTALITARIAN LANDSCAPE

Yasser Sedrati [1] **Maria Wiam Sidi Athmane**[2]

[1] **Biskra University (Algeria),**
Yasser.sedrati@univ-biskra.dz
[2] **Biskra University (Algeria),**
Maria.sidiathmane@univ-biskra.dz

Abstract: This study examines the concept of Digital Totalitarianism and Consumerism within the framework of contemporary digital platforms, by exploring the role of pleasure in human interactions. The analysis aims to uncover how social media and online markets platforms leverage pleasure and surveillance to reinforce social control via consumption. The primary objective of this research is to investigate the wider societal and individual implications of digital totalitarianism, as well as how these platforms capitalize on user data and behaviour control mechanisms. It will analyze the dynamics and operational frameworks of digital totalitarianism alongside consumerism. It asks: How does digital totalitarianism influence behavior on social media platforms? What are the broader ramifications of digital totalitarianism for societal organization and personal liberties? In what ways do these platforms exploit user data for their own gain and manage user behavior? Additionally, how do the regulations and algorithms implemented by these platforms limit individual autonomy? The central focus is to examine the complex relationships that exist among pleasure, power, and governance. The research highlights significant ethical concerns surrounding digital surveillance, privacy infringement, and the commodification of human experiences. The findings underscore the risks associated with compromising personal freedom and reducing human experiences to mere commercial transactions

Keywords: Digital Totalitarianism; Surveillance; Capitalism; Commodification; Social Media.

How to cite the article:
Sedrati, Y. & Sidi Athmane, M-W. (2024). The Cookies' Quest: Towards Digital Totalitarian Landscape. *Journal of Studies in Language, Culture, and Society (JSLCS)7*(2), pp-pp. 182-199.

[1] Corresponding author:**Yasser Sedrati**
Authors' ORCID ID https://orcid.org/0009-0004-3346-0422
https://orcid.org/0009-0003-3632-7531

1. Introduction

Legend has it that Abraham Lincoln, during his upbringing in Indiana in the early nineteenth century, was willing to walk long distances just to borrow a book. The scarcity and value of literature during that time made it a precious commodity, with information in general being difficult to obtain. Accessing news, knowledge, or entertainment required significant effort and expense, whether it was through subscribing to a newspaper, purchasing one, or visiting a library. Just a few years ago, obtaining information was a much more challenging task compared to the present day. The advent of digitization and information technology has revolutionized the way information is accessed. Today, a smartphone provides instant access to a vast array of information, ranging from news and politics to literature and entertainment. The ease with which information can now be obtained is unparalleled, marking a significant shift from the past when being well-informed was a more arduous and costly endeavour.

The defining characteristic of the information age is not the relentless quest for elusive information, but rather the overwhelming abundance of information that poses the risk of inundation or overload. The proliferation of easily accessible information online has led to a significant decrease in the perceived value of information. Individuals who have been raised in the digital era anticipate receiving information at no cost and are reluctant to pay for traditional sources such as newspapers, books, or entertainment. In today's society, few would be inclined to embark on a lengthy journey to acquire a book. With information in abundance comes an attention deficit. As early as 1971, Nobel Prize Laureate in economics Herbert Simon (1971) prophetically talked about the information age to come, "…in an information-rich world, the wealth of information means a dearth of something else: a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients" (Simon, 1971, pp. 40–41).

Major corporations like Facebook, Amazon, and Google amass vast quantities of data on users' online activities. In addition to these industry giants, numerous smaller entities providing apparently free services also gather user data, which they not only use to target advertising but also to compile detailed profiles on individuals. This includes information voluntarily shared by users, such as interests, age, gender, political views, and relationship status, all of which hold significant value when analyzed collectively. Furthermore, the data collection extends to the constant stream of information generated through cookies and other covert tracking procedures, encompassing details on searches, browsing habits, social media interactions, email communications, and consumption preferences. Even the physical movements of individuals are not exempt from being monitored, provided they are not using outdated technology. The pervasive nature of data collection is exemplified by products like the Hello Barbie doll, which not only entertains children, but also as Marr, (2015) argued, it gathers and transmits data to the manufacturer, Mattel, regarding the child's conversations, preferences, and desires. This underscores the extent to which personal information is being harvested in various aspects of modern life, raising concerns about privacy and data security.

The digital transformation of our society facilitates, broadens, and hastens the commercial utilization of human existence. It places aspects of our lives under the influence of commercial interests that were previously beyond economic exploitation. The Apple flagship store located in New York can be described as a symbol of hyper-capitalism, characterized by a glass cube structure that is devoid of any internal features aside from the actual store situated in the basement. This transparent architectural design draws parallels to the black veiled Kaaba in Mecca, serving as a striking representation of modern consumer culture and technological worship. The Apple store is emblematic of a dominant authority in society. The clear cube is depicted as a representation of liberty and a symbol of unrestricted communication; however, its transparency serves as a form of authority that has evolved into

digital totalitarianism in contemporary times. This modern authority of hyper capitalism, driven by constant communication, is accompanied by extensive surveillance. The glass cube glorifies communication that saturates and scrutinizes all aspects of life, converting them into financial worth. It remains accessible to consumers around the clock

The current study seeks to investigate the dynamics and operational methods of digital totalitarianism and consumerism. It seeks to delve into inquiries such as: In what ways does digital totalitarianism influence and regulate conduct on social media channels? What are the wider consequences of digital totalitarianism on societal structures and personal freedom? How do these social media platforms exploit user data for their advantage, and manage behaviour using distinct techniques? How do regulations and algorithms imposed by platforms limit autonomy in the realm of digital totalitarianism? The central aim is to scrutinize the intricate relationships among enjoyment, authority, and regulation. This research will try to analyse pertinent scholarly literature, such as *the Neuroscience of happiness and pleasure* by Kringelbach et al. (2012), which offers scientific perspectives on the psychological dimensions of pleasure and happiness. Advocating for a hedonic perspective, it has been proposed that the most effective way to assess subjective well-being is to repeatedly inquire about individuals' current hedonic feelings. This method allows for the monitoring of hedonic experiences throughout daily life (Kahneman, 1999, pp. 5-11). Additionally, these continuous self-reports of hedonic states may facilitate the identification of more enduring neurobiological traits associated with hedonic responses, which could predispose certain individuals to experience happiness. Moreover, a hedonic framework may provide insights into the eudaimonic aspects of happiness, given the empirical overlap between these two constructs, even though a positive mood represents only a portion of the overall happiness narrative (Kringelbach et al., 2012, pp. 311-316). The experience of pleasure is regulated by a distinct region of the brain referred to as the reward system. This complex network of neurons mainly includes the ventral tegmental area (VTA), the nucleus accumbens, and the prefrontal cortex, which are linked by the neurotransmitter dopamine. Arousal, defined as the activation of the sympathetic nervous system, prepares individuals to react more vigorously to various stimuli by promoting the release of neurotransmitters such as dopamine and nor-epinephrine. Empirical studies indicate that heightened arousal enhances responses to rewarding stimuli, thereby intensifying feelings of pleasure. Conversely, it also magnifies reactions to negative or threatening stimuli, resulting in increased pain and discomfort. Thus, arousal functions as a sensitizing mechanism, equipping both the body and brain to respond more robustly to all incoming stimuli, whether they are pleasurable or aversive.

The incessant flow of information on social media, marked by rapid scrolling, eye-catching visuals, and continuous updates, has been associated with diminished attention spans and impaired cognitive functions. Research indicates that overindulgence in social media can obstruct an individual's capacity to concentrate, assimilate information, and participate in profound, focused contemplation. The phenomenon of neuroplasticity, which refers to the brain's capacity to adapt and reorganize its neural connections, is significantly affected by the use of social media. Prolonged exposure to screens and active participation in social media platforms may lead to modifications in neural pathways, thereby impacting behavior, emotional reactions, and interpersonal relationships

Furthermore, *the Age of surveillance capitalism* by Zuboff (2019) will be scrutinized, presenting a critical evaluation of the rise and influence of surveillance capitalism in the digital era. In order to elucidate the significance of these studies to the present research, it is essential to briefly examine their implications. Kringelbach and Berridge's (2010) scientific insights can help us understand how people respond psychologically to stimuli that make

them feel good in digital environments. Zuboff's (2019) analysis establishes an explorative layer that inquires how surveillance capitalism shape user behaviour and experiences through data collection and algorithmic control.

This study aims to delve into the underlying mechanisms behind pleasure experiences in its psychological and socio-economic dimensions. The main goal is to investigate how control mechanisms employed by digital platforms impact pleasure experiences, with a specific focus on social media and entertainment areas. The major aim is to elucidate these mechanisms in a straightforward manner, thereby broadening our insight into the influence of digital control on pleasure experiences in the contemporary digital landscape.

2. The Digital Panopticon and Consumerism

2.1 Defining Digital Totalitarianism

The concept of "digital totalitarianism" encompasses the potential misuse of digital technologies by authoritarian governments to exert control over their populace. This hypothetical situation involves the deployment of sophisticated surveillance systems, artificial intelligence (AI), and big data analytics to closely monitor the activities, online behavior, and communications of citizens. The term "digital totalitarianism" does not have a specific origin date, but it gained prominence in the early to mid-2010s, with influential figures such as Egeny Morozov and Zuboff contributing to its popularization. While these analysts did not explicitly coin the term, their scholarly works, including *the Net delusion: the dark side of internet freedom* (2011) by Morozov and *the Age of surveillance capitalism* (2019) by Zuboff, laid the groundwork for understanding the implications of digital totalitarianism.

The concept of Digital Totalitarianism underscores the intricate relationship between technology, society, and power dynamics, highlighting the potential ramifications of unchecked surveillance and data control. By intertwining digital tools with social structures, this system enables unprecedented levels of monitoring and manipulation, raising concerns about privacy, autonomy, and individual freedom. The utilization of sophisticated algorithms to analyze vast datasets poses challenges to notions of personal agency and societal autonomy, as predictive technologies shape and constrain human behaviors in various domains. As such, understanding and critically examining the implications of digital totalitarianism is crucial for safeguarding democratic values, human rights, and ethical principles in an increasingly digitized world.

Furthermore, the enforcement of ideological hegemony plays a crucial role in reinforcing the practices associated with digital totalitarianism, as prevailing ideologies justify the suppression of dissenting voices and critical perspectives. These socio-technical dynamics are deeply entrenched in historical contexts, reflecting a continuum of surveillance practices that underscore the intricate relationship between technology, power structures, and societal institutions in the contemporary digital landscape. The convergence of these elements underscores the complex interplay between technology, power dynamics, and societal norms in the digital era, shedding light on the multifaceted nature of digital totalitarianism and its implications for individual freedom and democratic principles. Shifting from a sociological to a psychological perspective, the analysis transitions from scrutinizing broader societal structures and power dynamics influencing digital totalitarianism to concentrating on individual experiences, cognitive processes, and psychological ramifications of surveillance and control enabled by digital technologies.

2.2 The Malvertizing Phishing

The proliferation of advanced technologies has led to the increasing sophistication of digital surveillance and manipulation mechanisms, presenting significant challenges to personal privacy. In this context, data has emerged as the new form of currency, and the control over information has become of utmost importance. Corporations and social media platforms heavily rely on data collection as a crucial mechanism. This process involves the deployment of various technologies and platforms to gather user information across digital environments. For instance, social media sites like Facebook and Instagram utilize advanced algorithms to track user interactions, habits, and preferences as they navigate through their feeds, engage with content, and interact with posts. These platforms capture a wide array of data metrics, including likes, shares, comments, and even the duration users spend consuming specific articles or videos. These platforms are known for fostering immediacy, shared presence, transience, and genuineness to gather the essential data required for their functionality.

What is commonly observed is the reinforcement of constant connectedness and active attentiveness, with the underlying pressure that something significant may occur at any moment, and that social media serves as the primary means to stay informed about this continuous flow of information. The ubiquitous structure of the infinite 'stream' symbolizes the perpetual movement, emphasizing the idea of constant change and rendering the present as uncertain and fluid (Weltevrede et al., 2014, pp. 127). Social media streams are typically organized in reverse chronological order and are consistently updated, creating a sense of immediacy and favoring real-time engagement (Gerlitz, 2016, p. 35). Amidst this continuous and unceasing flow, important events may occur, and the unsettling aspect lies in the unpredictability of when they will transpire.

Following data collection, information is consolidated, assessed, and processed to derive valuable insights and trends that can guide organizational strategies and decision-making procedures. Companies utilize advanced data analytics tools and methodologies to navigate through extensive datasets, recognizing patterns, correlations, and predictive signals. By leveraging data analytics findings, organizations adapt their products, services, and promotional efforts to meet the demands and preferences of their target audience. This often involves creating personalized experiences and targeted advertising campaigns that resonate with and influence individuals based on their distinct characteristics and behaviors. Amazon, a prominent player in the e-commerce industry, is renowned for its utilization of such strategies. The comprehensive data collection enables Amazon to tailor product recommendations and dynamically adjust pricing strategies in alignment with market trends and individual preferences. Similarly, Spotify, the music streaming platform, utilizes data gathering and analysis to transform user interactions and maintain a leading position in the fiercely competitive digital environment. Through monitoring users' music listening patterns, playlist compilations, and favorite artists, Spotify acquires comprehensive data for the purpose of creating customized playlists and suggesting new music that aligns with individual preferences. “Social networking platforms like Facebook and Twitter provide complimentary services in exchange for user information, which is subsequently marketed to businesses seeking to tailor advertisements to individuals.” (Bartlett, 2018, p. 12). This is made feasible through the implementation of predictive algorithms that scrutinize user data and forecast future actions (Palmas, 1971, p. 347). Consequently, the utilization of Big Data has made prediction and customization the most potent mechanisms for regulating consumer behavior.

Among the major issues raised in Europe and the US about the users and consumers privacy concerns is the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). The former represents the most stringent privacy and security

legislation globally. Although it was formulated and enacted by the European Union (EU), its requirements extend to organizations worldwide that engage in targeting or collecting data pertaining to individuals within the EU. This regulation came into force on May 25, 2018. The GDPR imposes severe financial penalties on entities that breach its privacy and security provisions, with fines potentially amounting to tens of millions of euros. The General Data Protection Regulation (GDPR) is Europe's resolute commitment to data privacy and security, especially as an increasing number of individuals are placing their personal information in the hands of cloud service providers amidst a backdrop of frequent data breaches. The regulation is extensive and comprehensive, yet it lacks detailed specifications, which can render compliance a challenging endeavor, particularly for small and medium-sized enterprises (SMEs).

Whereas the latter is a legislative measure focused on data privacy, which was established in California in 2018 and became effective on January 1, 2020. The primary objective of the CCPA is to strengthen the privacy rights and consumer protections for individuals residing in California. It empowers consumers by granting them the right to be informed about the personal information that businesses collect, the purposes for which this data is utilized, and the entities with whom it is shared. The CCPA confers several specific rights to consumers, including the right to access their personal information, the right to request the deletion of their data, the right to opt-out of the sale of their personal information, and the right to be free from discrimination for exercising their rights under the CCPA. Businesses that fall under the jurisdiction of the CCPA are required to adhere to these consumer rights and to implement suitable security protocols to safeguard personal information. The CCPA is applicable to profit-oriented enterprises that gather personal information from consumers, operate within California, and satisfy certain revenue or data processing criteria.

The majority of individuals may not always be fully cognizant of the various ways in which their posted information can be utilized, leading to potential gains and profits. This lack of awareness is compounded by the fact that the public nature of data does not equate to consent for unrestricted use (Boyd & Crawford, 2012, p. 673). Despite the illusion of control that websites may create, users actually relinquish control as soon as they engage online. There is no option to restrict data extraction or to use the Internet in Incognito. The level of awareness that users have regarding their online activities also influences their relationship with the "technological unconscious," which encompasses the patterns, predispositions, and responses of individuals. The monitoring of user responses and interactions can unveil more about their predispositions, thereby increasing the potential for surveillance (Hayles, 2017, p. 119). However, it remains uncertain whether users are fully aware of the information that can be derived from their online activities.

AI has become increasingly prominent in various industries in recent years, largely due to its groundbreaking advancements. AI operates by employing algorithms to scrutinize extensive sets of data and derive patterns from them. These algorithms undergo training using datasets that encompass instances of the specific task they are designed to execute, such as image recognition or language comprehension.

Within the realm of digital surveillance, AI has the capability to be employed for the purpose of surveillance and monitoring, allowing governments and organizations to observe and oversee the activities and behaviors of individuals in both digital and physical environments. An example of this is the use of AI-powered facial recognition technology, which can identify and track individuals' faces in real-time, thereby giving rise to apprehensions regarding privacy and civil liberties. Likewise, predictive analytics algorithms have the capacity to scrutinize extensive volumes of data in order to detect patterns or

irregularities that may indicate potential security risks or suspicious activities, resulting in heightened surveillance and monitoring of individuals' conduct.

The primary value of data when combined into Big Data lies in its ability to facilitate future predictions. By analyzing patterns of past behavior, data can offer insights into potential future behavior. This allows for informed assessments of risk, future financial performance, marketing impact, and communication strategies, ultimately enabling organizations to optimize their operations and potentially generate profits from this predictive capability:

> Will she be able to repay the loan in the future – and will she? Will he show up for work and contribute to productivity or is he just a "high cost" employee? Is she disposed for a disease, so the insurance company in case a policy is made has to cover medical expenses exceeding the income from premiums? Which commercials will succeed persuading this person to buy the product or vote for the candidate? How many more users will push the button and provide valuable attention, if it is red? Which products and services will he desire later today? In two minutes? Ten seconds after this specific online marketing stimulus is provided through his smartphone? (Zuboff, 2016, para. 9).

The central theme of all these inquiries revolves around the generation and maximization of future profits. The core of the dominant surveillance capitalism business model lies in the data-driven anticipation of consumer behavior, aimed at boosting sales and profits. The practice of predicting future outcomes has evolved into a lucrative enterprise, where the ability to forecast events translates directly into financial gain.

The ability to forecast future events holds significant power, as it opens up the opportunity to not only foresee outcomes, but also to potentially alter them, thereby taking advantage from such changes. This concept -of predicting in order to manipulate -lies at the heart of targeted marketing strategies, where success is measured by the ability to modify individuals' actions in a way that benefits the client, whether commercially or politically. The key to achieving marketing success through prediction lies in the capacity to anticipate and subsequently influence behavior by providing specific stimuli at the right time. By accurately predicting consumer desires and timing, marketers can strategically guide individuals towards making purchases, thus maximizing their chances of success in influencing and controlling consumer behavior. Demographic profiling plays a crucial role in enabling such predictive power, as it allows for the generation of insights based on data related to factors such as home address, gender, ethnicity, employment status, income level, consumption habits, political leanings, and social connections. By leveraging this information, marketers can tailor their advertising efforts to target specific pain points and effectively influence consumer behavior, ultimately leading to a more successful marketing approach. (Hendricks & Vestergaard, 2019, p. 13).

The predictive capabilities of big data have the potential to reveal deeply personal information such as political affiliations, religious beliefs, and sexual orientation. This information, which is often considered private, can be exploited for purposes beyond targeted advertising, leading to aggressive and predatory marketing tactics. Cathy O'Neil in *Weapons of math destruction* (2016), highlights the potential misuse of demographic, behavioral, and consumer data to target vulnerable individuals with offers that exploit their social and economic circumstances. Individuals facing financial hardship may be inundated with offers for high-interest payday loans, while those in stagnant career positions may be targeted with expensive university courses. This exploitation of personal data can have detrimental effects on individuals who are already struggling, further exacerbating their challenges and

perpetuating social and economic inequalities, "… to localize the most vulnerable persons and use their private information against them. This involves figuring out where they hurt the most, their so-called pain point". (O'Neil, 2016, pp. 72–73)

2.3 Privacy and the Digital Infringement

On the one hand, following the destruction of the Twin Towers in 2001, an FBI agent articulated his dissatisfaction in a series of emails concerning the "radical, militant librarians" who declined to comply with requests for patron records from the Federal Bureau of Investigation. This criticism was directed at the FBI's use of secret warrants permitted by Section 215 of the USA PATRIOT Act to obtain library user data. The librarians' resistance was rooted in their advocacy for patrons' rights to read freely, shielded from governmental surveillance or examination. The concerted actions of numerous library personnel across the country subsequently contributed to influencing Congress to prolong its discussions regarding the renewal of the USA PATRIOT Act (American Library Association, January 17, 2006).

The term "radical, militant librarians" gained significant traction on the internet and continues to be a prominent part of online discourse. These librarians took pride in displaying this label on badges, coffee mugs, and tote bags. Their activism was primarily directed against the potential and actual threats of data profiling (Gellman & Dixman, 2011, p. 10), where inquiries into searches, checkouts, and interests in unconventional subjects could arouse governmental suspicion and lead to investigations, potentially suggesting involvement in illicit activities. Essentially, the agent highlighted a longstanding priority within the library community: the protection of patron privacy and the fundamental right to read freely without scrutiny or consequences. Librarians viewed themselves as pioneers in advocating for rights related to privacy, copyright, surveillance, data mining, and freedom—issues that remain critically important in the contemporary digital landscape, perhaps even more so than in previous decades.

One of the most notable threats to the privacy of library patrons in recent history is the USA PATRIOT Act, formally known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism. Enacted in the aftermath of the September 11 attacks in 2001, this legislation, particularly Sections 215 and 505, conferred significant authority upon federal agents to request and obtain personal information about library users, including their reading habits and borrowing records. The implications of this expanded governmental authority raised immediate concerns among librarians, as it contravened the ethical principles that underpin the profession. These principles encompass intellectual freedom, information literacy, equitable access, and the fundamental right to free expression, all of which are integral to the American Library Association's (ALA) Code of Ethics (1994) and the Library Bill of Rights (originally adopted in 1939 and revised in 2019) (American Library Association, August 19, 2021)

The PATRIOT Act introduced a nondisclosure clause that restricted library personnel from revealing whether the FBI had sought information from them. Although many states had established laws safeguarding the confidentiality of library users, these state regulations are effectively superseded by federal statutes that permit federal entities to access library records. As noted by Lambert et. al. (2015), "No federal or case law protects the privacy of library records" (p.3). Under the provisions of the PATRIOT Act, federal agents were no longer required to present a subpoena to acquire library patron records; a Foreign Intelligence Surveillance Act (FISA) court order was deemed sufficient, allowing access to any record for any purpose, even in the absence of a direct link to ongoing terrorism investigations. It is important to acknowledge that the PATRIOT Act was, from a centralized viewpoint, designed

to safeguard the American populace from terrorist threats, although this interpretation has been the subject of ongoing scholarly debate (Whitehead et al., 2002, pp. 110-115)

The transformation of libraries into environments of scrutiny, where the research activities of patrons could be monitored and potentially weaponized against them, significantly undermined the foundational principles of privacy and intellectual freedom that are integral to the library profession. By the twentieth century, the American Library Association (ALA) had established a strong presence, yet even in the nineteenth century, the public perception of librarianship was increasingly recognized as a scientific discipline (Lugya, 2014, pp. 140-145). By the onset of the twentieth century, librarians began to incorporate social science methodologies to guide their collection practices, analyse user demographics, and evaluate the informational requirements of various patron groups. This approach remains relevant today, shaping the ways in which librarians engage with and serve their communities, as well as influencing the resources they advocate for and uphold. The contemporary field of library studies is deeply rooted in social science principles, while also embracing the application and advancement of technology. Modern libraries prioritize the use of data sets, statistical analysis, and evidence-based arguments that are substantiated by measurable outcomes. The approach of librarians towards technology is characterized by a commitment to freedom and openness, rather than a stance of skepticism. As Jesse Shera (1973) articulates, “Librarians and book collectors are custodians of the transcript, the ‘keepers of the Word’ …,” indicating that they serve not as gatekeepers but as advocates for unrestricted access to materials, both in print and digital formats. Shera further describes the library as “the memory of society,” referring to it as the social cortex (Shera, 1973, p. 91). This defense of access to such a vital societal resource is central to the identity of librarians. Libraries function as both repositories and champions of information, ensuring that individuals have free access to knowledge. The implications of restricted access to these knowledge bases pose significant social risks. Given this perspective, it is understandable why librarians expressed concern regarding the intrusive measures of the PATRIOT Act. In retrospect, these concerns appear minor when juxtaposed with the current operations of US Immigration and Customs Enforcement (ICE)

On the other hand, the ruling party in China, benefiting from the nation's economic output, is increasingly focusing on the development and application of information technologies as instruments for comprehensive surveillance of its populace. The initiative known as the "Golden Shield" has already been employed to restrict citizens' access to the "external network," achieving a degree of success. However, the continuous advancement of new information technologies has been always directed towards the eradication of the "privacy" notion and the establishment of complete transparency regarding citizen data for governmental authorities. This entails a centralized system to collect information on individuals that extends beyond the digital realm, where every action is assessed by computer algorithms in real-time, leading to modifications in the “social credit score”. While this scenario may resemble a narrative from dystopian literature, it is, in fact, the current reality for more than a billion citizens in China (Mosher, 2019).

The “Sovereign Internet” project by the Russian government was another model for active online surveillance which was meant to increase the level of the national security. Roskomnadzor, the Russian regulatory body overseeing information channels worked to ban the messaging application Telegram, developed by Pavel Durov. The agency's decision to block IP addresses associated with Amazon Web Services, inadvertently, restricted access to numerous significant online resources. However, Telegram remained accessible. Later on, Roskomnadzor was compelled to retrieve its restrictive measures. Consequently, while Telegram is officially prohibited, it continues to be utilized by millions of users in Russia.

The application of John Stuart Mill's Harm Principle to the situation involving Telegram illustrates the intricate challenge of reconciling the right to free speech with the necessity of harm prevention. On one side, Telegram's dedication to free expression resonates with Mill's principles of personal freedom and opposition to censorship. The platform's encryption capabilities create a secure environment for users to articulate their opinions without the apprehension of governmental oversight, a factor that holds significant relevance in authoritarian regimes (Parida, 2021). However, the lack of regulation on Telegram facilitates the proliferation of detrimental content. For example, extremist organizations have exploited this platform to organize their operations and spread propaganda (Looney et al., 2022). The Harm Principle suggests that such content warrants intervention due to its potential to inflict harm on others. Mill's principle reinforces the notion that, although free speech holds significant value, it should not encompass actions or expressions that directly harm individuals or society. The primary challenge facing Telegram is to balance its dedication to free speech with the imperative of harm prevention. From the standpoint of the Harm Principle, the platform bears an ethical responsibility to adopt content moderation strategies that reduce the dangers linked to harmful content, even if this necessitates the restriction of certain expressions.

Content moderation on digital platforms such as Telegram can be viewed as a pragmatic implementation of the Harm Principle. Although Durov has consistently prioritized privacy and free speech, the increasing prevalence of harmful content on Telegram underscores the necessity for a more nuanced strategy. The Harm Principle justifies content moderation as an essential measure to avert potential harm. Nevertheless, the difficulty resides in executing moderation in a manner that does not violate users' rightful entitlements to free expression (Etzioni, 1993, pp. 95-100). The discord between Telegram and numerous governments, especially that of Russia, exemplifies the friction between governmental authority and the independence of digital platforms. Authorities frequently cite national security issues as a rationale for their requests for data access and content regulation, whereas platforms such as Telegram oppose these requests on the grounds of protecting free expression and privacy (Wijermars & Lokot, 2022, pp. 267-270). The Harm Principle provides a useful lens through which to assess these disputes, positing that governmental intervention is warranted solely when it aims to avert harm, rather than to stifle dissent.

Nisbet (2012) argued that financial resources have the potential to secure the interest of voters and provide the necessary knowledge to sway their actions in a specific manner. This strategy was effectively employed by Barack Obama's campaign back in 2008, during the rise of digital micro-marketing in American political campaigns. The campaign sent out over a billion personalized emails, with a focus on reaching out to young individuals and minority groups, aiming to encourage them to participate in the electoral process and cast their votes in favor of Obama. Hendricks and Vestergaard (2019) argued that the utilization of precise political micro-marketing achieved an advanced stage and underwent a negative transformation during the Brexit referendum in the United Kingdom and the 2016 Presidential Election in the United States. Both Leave.EU and Trump's campaign enlisted the services of the company Cambridge Analytica, which promoted itself as a firm that "utilizes data to influence audience behavior" in both commercial and political promotional activities. (Hendricks & Vestergaard, 2019, p.15)

Furthermore, social media platforms' utilization of AI-powered algorithms for content moderation can inadvertently stifle the spread of truth and information by flagging and deleting content that may challenge dominant narratives or reveal inconvenient truths. Despite the purported goal of these algorithms to uphold a secure online environment by targeting harmful content, their implementation results in the suppression of crucial information. For

example, following the 7th of October 2023, when social media platforms implemented stricter content moderation policies, posts related to the ongoing genocide in Palestine were frequently taken down for violating community guidelines. This censorship also encompassed content portraying the suffering of innocent victims, effectively muting their voices and concealing the realities of the situation from global audiences. Consequently, essential information regarding human rights abuses has become unattainable.

2.3 The Ethical Implications of Digital Practices

The challenges posed by the pervasive use of the internet and digital platforms underscore the need for proactive measures to navigate the intricate landscape of social interactions and information sharing. As we grapple with the implications of our interconnected world, it becomes imperative to cultivate a critical awareness of the potential risks and consequences associated with our online activities. By fostering a culture of digital literacy and responsible engagement, we can strive towards mitigating the negative impacts of the "social dilemma" and fostering a more informed and resilient society.

The ongoing collection and examination of personal information without explicit permission give rise to substantial ethical queries concerning transparency and responsibility. A study conducted by The Pew Research Center revealed that 79% of Americans express concerns about how their personal data is managed (Duggan & Smith, 2016). Particularly, younger individuals and those who engage in social media or online shopping exhibit heightened apprehension. Furthermore, the challenges extend beyond mere data aggregation. The digital realm is rife with manipulation and distortion, where algorithms and customized content have the potential to sway public opinion, impact behaviors, and even influence democratic processes. For instance, during the 2016 US presidential election, Russian operatives leveraged social media platforms to support Trump's campaign, disseminating misinformation and fostering discord among American voters (Nicas & Rosenberg, 2018).

Another important question about the ethical implications of these digital tools is their potential to exacerbate existing biases and inequalities. Adding to the complexity are concerns about bias, fairness, and accountability in AI technologies.

The ethical implications of digital tools have come under scrutiny due to concerns about exacerbating existing biases and inequalities. In particular, the discussion around bias, fairness, and accountability in artificial intelligence (AI) technologies has gained prominence. Buolamwini and Gebru's (2018) research shed light on the troubling biases present in facial recognition algorithms, especially in their mis-identification of individuals from marginalized groups such as people of color and women. These biases pose a significant threat as they have the potential to perpetuate systemic inequalities and undermine the credibility of AI systems. The research revealed a notable disparity in error rates for gender classification based on skin tone, with darker-skinned individuals experiencing higher error rates compared to their lighter-skinned counterparts. For instance, women of color had error rates as high as 34.7%, while lighter-skinned men had error rates as low as 0.8%. This disparity in error rates across different gender and racial groups underscores the presence of clear biases within the algorithms. The findings highlight the urgent need for addressing these biases to ensure that AI technologies are developed and deployed in a fair and equitable manner, free from perpetuating existing inequalities. (Buolamwini & Gebru, 2018, pp. 6-10)

The proliferation of unethical behaviors within the digital realm has sparked apprehension regarding the consolidation of authority among a select few individuals. This small cohort of influential figures exerts an overwhelming amount of control over information dissemination, communication channels, and technological frameworks. These affluent denizens of the digital sphere, who possess exclusive entry to vast reservoirs of data and

intricate algorithms, amplify concerns surrounding the widening power gap within society. Often situated in prominent positions within technology enterprises or governmental entities, they mold narratives, sway public sentiment, and set cultural benchmarks. This centralization of power not only hampers competition and creativity but also perpetuates existing power structures, constraining opportunities for smaller businesses and marginalized voices. Furthermore, the unbridled sway wielded by these elites fosters a climate of impunity wherein transgressions like exploiting data for financial gain under the guise of upholding order or preserving market dominance are normalized. The unchecked influence of a select group of individuals not only distorts the digital landscape but also poses a significant threat to the democratic ideals of transparency, accountability, and inclusivity. As such, it is imperative to address these power imbalances and promote a more equitable distribution of authority within the digital domain to safeguard the interests of all stakeholders.

2.4 Digital Platforms: The Commodification of Pleasure

Digital platforms have a crucial impact on the commercialization of pleasure, converting personal encounters into products that can be bought, sold, and utilized. They exploit human desire, feelings, and choices, converting them into measurable data that can be studied and controlled. According to Zuboff (2016), this process entails utilizing these platforms to gather personal interactions, repackaging them as information for financial gain rather than for reciprocal transactions.

Surveillance capitalism is a system that capitalizes on individuals by utilizing their personal data to develop predictive products and services, underscoring the unbalanced dynamic in which users are treated as sources of data rather than as customers, perpetuating a cycle of consumerism and surveillance. This concept, as described by Zuboff (2019), sheds light on how human experiences and emotions are commodified in the digital era. In the realm of surveillance capitalism, the process involves the collection and exploitation of individuals' online activities as a form of valuable data, all without their explicit consent or awareness. This approach views human experiences, such as browsing habits and interactions, as data points that can be scrutinized and transformed into behavioral predictions. These predictions are then leveraged to influence and forecast human conduct for commercial objectives, like personalized advertising and content delivery. The unilateral acquisition and utilization of personal data in surveillance capitalism give rise to significant ethical concerns regarding privacy, autonomy, and the power dynamics between individuals and corporations in the digital landscape. This practice raises questions about the extent to which individuals are aware of and consent to the use of their data, as well as the implications for their rights and freedom in an increasingly data-driven world. (Zuboff, 2019, pp.73-80)

Furthermore, digital platforms are intricately designed to captivate users and prompt specific actions, fostering a continuous state of connectivity and digital consumption. The primary goal is to optimize user engagement, cultivate enduring connections, and gather valuable data for targeted advertising and personalized content delivery. Despite the potential for digital spaces to be inclusive and expressive, they often perpetuate and intensify societal disparities and power differentials, revealing the manipulative influence of digital platforms in shaping user behaviors and preferences. Additionally, digital platforms leverage sophisticated algorithms and data analysis to curate personalized content and recommendations based on individual browsing history, preferences, and interactions. This tailored approach to content distribution creates a filter bubble, reinforcing existing beliefs, preferences, and interests while limiting exposure to alternative perspectives and competing viewpoints. The algorithmic screening techniques employed by major digital entities may inadvertently contribute to the formation of ideological bubbles and the propagation of extreme viewpoints.

The commercialization of pleasure on digital platforms goes beyond targeted advertising and individualized content distribution, to include the "gaming" of engagement by users and the monetization of social connections. Gamification tactics, prizes, and rewards are used on digital platforms to increase user interaction, develop community engagement, and promote regular use. These gamified experiences establish a sense of accomplishment, satisfaction, and enjoyment, encouraging repeat participation and reinforcing platform loyalty.

These digital platforms enable the commercialization of social interactions through influencer marketing, sponsored content, and affiliate programs, transforming people's connections and interactions into valuable assets that can be utilized for commercial advantage. The blurring of personal and professional boundaries on digital platforms commodifies social interactions and relationships, reducing real ties to transactional transactions. Likewise, it influences people's interactions with technology by encouraging dependency, addiction, and reliance on digital gadgets and online services. Digital platforms' continual connectedness, notifications, and rapid pleasure set off a cycle of reliance and obsessive involvement that interrupts offline contacts, face-to-face conversation, and real-world experiences. The culture of digital consumption prioritizes immediate gratification over long-term well-being and societal values, indicating the negative influence of digital technology on individuals' well- being and relationships. It also undermines privacy, autonomy, and individual agency by controlling users' data, choices, and actions. Digital platforms' ubiquitous monitoring and data gathering methods harm people's capacity to make educated decisions, govern their personal data, and safeguard their privacy.

Besides, encouraging hedonistic purchasing habits adds to the commercialization of desires and identities, transforming personal preferences and goals into marketable commodities. This commodification promotes capitalist accumulation by promoting continual consuming and reinforcing consumerist ideals that emphasize material acquisition over social justice and equitable resource allocation.

2.5 The Road to Artificial Super Intelligence: a Utopia or a Dystopia?

It is important to recognize that although emerging technologies such as artificial general intelligence (AGI), synthetic biology, geo-engineering, and distributed manufacturing offer significant advantages for humanity, they simultaneously present existential threats to human societies. Knight (2015) posits that the year 2015 was marked by significant discussions surrounding self-driving vehicles, robotics, deep learning, and advanced AI. The swift advancements in these fields, particularly in machine learning and artificial neural networks inspired by biological systems, have sparked concerns regarding the existential threats posed by future AI developments. Among these threats are the potential for "the creation of new weapons of mass destruction, or catastrophe through accidental misuse." Furthermore, AGI is said to underpin human capabilities in areas such as strategic planning, social manipulation, cyber-security, technological innovation, and economic efficiency. Given the unpredictable nature of technological advancements, there is an imperative to implement proactive policy measures and establish a regulatory framework aimed at mitigating these risks, even in the absence of immediate breakthroughs. Bostrom's exploration of "existential risk" (Future of Humanity Institute 2013, Knight ibid.) suggests that AI could represent the most catastrophic technology imaginable. He argues that self-improving AI systems, possessing intellectual capabilities beyond human understanding, could potentially enslave or annihilate humanity if they so desired. While Bostrom expresses doubt regarding the controllability of such machines, he asserts that programming them with appropriate "human-friendly" values could ensure that they adhere to these principles, regardless of their power. Additionally, Knight comments on the discourse surrounding deep learning, highlighting that the fundamental limitation of artificial neural networks lies in their inability to match the

speed and accuracy of human cognitive processes. Consequently, one of the most challenging obstacles in machine learning is the creation of artificial neurons capable of operating at an enhanced rate.

In his analysis of Bostrom's research on existential risk, Geist (2015) acknowledges the limitations inherent in super-intelligent machines. However, he argues that AI-enhanced technologies could pose significant dangers due to their capacity to exacerbate human folly. Regarding existential risk, he suggests that future AIs, by merely improving upon established twentieth-century technologies, could threaten the survival of current societal frameworks by destabilizing their fragile strategic equilibria. This could occur through the acceleration, cost reduction, and increased lethality of existing technologies. Geist further posits that machines capable of devising and executing complex plans, yet devoid of self-awareness, may present a greater threat than mechanical counterparts that mimic human cognition.

Baum et al. (2015) discuss the risks posed by advanced AI, highlighting the potential emergence of a global governance structure, referred to as a "singleton," and the intriguing notion that humanity might exist within a computer-generated simulation. While the pursuit of generalized computational solutions to existential risks may attract proponents of machine learning, the concept of human existence within simulations remains largely speculative. It is crucial to recognize the varying trajectories of technological advancement, which may favor the development of safe AI technologies over those that pose significant dangers.

Baum et al (2015) offer a pragmatic viewpoint on the ethics surrounding catastrophic risks, arguing that the conventional ethical rationale for addressing such threats is rooted in the long-term advantages of doing so. They suggest that individuals who are not yet convinced of the existential risk argument can still contribute to long-term research by emphasizing the immediate benefits of addressing near-future threats and integrating these actions into current initiatives. Their analysis indicates that a substantial portion of the overall threat can be mitigated through actions that resonate with existing public interests, and that these measures are likely to yield the most significant reductions in Global Catastrophic Risk (GCR) relative to the effort invested.

Naughton (2015), in a recent opinion piece, discusses the implications and potential of big data, particularly in relation to the privacy and security concerns associated with the rapidly evolving Internet of Things (IoT). He argues that for the technology sector, IoT represents the Next Big Thing, closely linked to the concept of big data, as both phenomena are fundamentally interconnected. Naughton emphasizes that advancements in computing technology, characterized by smaller and more affordable devices, coupled with the widespread availability of wireless networks, will soon enable the integration of trillions of miniature, interconnected computers into everyday objects. These devices will possess the capability to detect environmental changes, control various functions, and autonomously make decisions—such as opening doors, regulating valves, or reordering essential items like milk—while continuously exchanging information with one another and transmitting data to remote server farms.

The discussions surrounding AI and Big Data highlight several critical issues relevant to the development of super intelligent systems. Notably, while AI technology and Big Data hold significant promise, they also impose a professional, ethical, and moral obligation to ensure the safety of individuals in our environment. The Responsible Data Forum (2015) asserts that responsible data management transcends mere technical security and encryption; it necessitates a commitment to upholding the dignity, respect, and privacy of the individuals involved. It is essential that those represented in the data we utilize are acknowledged and empowered to make informed choices regarding their lives. A significant concern arises from

the fact that users often encounter algorithmic biases, particularly when algorithmic solutions are applied to human-centric areas such as social risks and disasters. Regulatory frameworks aimed at providing global solutions frequently overlook personal, local, and community contexts, as well as regional and national considerations, which can result in the marginalization of the very individuals who are most vulnerable. Thus, the challenge identified by this Forum is to navigate the risks while achieving substantial successes and benefits, all the while remaining attuned to existing disparities.

Boyd (2015) posits that the predominant concern of the twenty-first century regarding AI is not the fear of machines usurping human roles, but rather the challenge of finding an appropriate equilibrium between human capabilities and automation to enhance outcomes. He emphasizes that human intelligence, characterized by skill, creativity, and ingenuity, is our most precious asset. In contrast, machine intelligence is defined by its ability to process information and analyze data. Achieving optimal solutions to critical issues facing humanity necessitates a harmonious integration of human and machine intelligence. Boyd uses the transition from propeller-driven aircraft to jets as an illustrative example, noting that the success of jet aviation hinges on understanding what functions to delegate to automated systems and which aspects should remain under human control. Furthermore, he highlights the F35 aircraft, where the pilot's helmet integrates with the aircraft's sensors, enabling the pilot to perceive the environment as if they were "seeing through" the aircraft. This experience fosters a sense of unity between the pilot and the machine, exemplifying a genuine symbiotic relationship. Boyd argues that this fusion, characterized by a "fluid interface" of collaborative interaction between humans and machines, allows for the development of new capabilities that neither humans nor machines could achieve independently.

3. Conclusion

The emergence of new social issues, which are not solely related to computation, can lead to various critical speculative discussions. These discussions have the potential to influence the ethical, legal, and imaginative boundaries of the environments in which our information architectures and infrastructures operate. Algorithmic implementations often reflect a desire for pure knowledge, devoid of uncertainty and human guesswork, and productive debates can play a role in altering these parameters. Rather than violating established societal norms, contemporary algorithms are establishing new standards of what is considered good or bad, normal or abnormal, against which actions are evaluated.

The potential disruptions caused by digitalization extend beyond the realms of democracy and self-determination in politics. The digital revolution poses a risk of eroding individual autonomy and free will, as an excess of information could prove to be a more significant threat to freedom than misinformation. A society that is overly factual and excessively informed due to digitalization may pave the way for a new type of digital totalitarianism. In such a scenario, the absence of trust, which currently fuels post-factual trends, might pale in comparison to the challenges posed by a data-driven society where trust is eradicated and control takes its place.

With the pace and acceleration, new digital technology is developed and integrated with behavioral science and design, and we may be heading toward—but hopefully never reach— the total elimination of autonomy and self-determination by data-driven behavioral control. Achieving totalitarian outcomes does not necessarily require a state with totalitarian aspirations. The tech industry's pursuit of complete surveillance and control over our lives mirrors the ambitions of a totalitarian regime, aiming to exploit, dominate, commercialize, and capitalize on every aspect of our existence and actions in order to maximize financial gains. By monitoring user behavior through applications, developers will be able to

distinguish between positive and negative behaviors, subsequently devising strategies to incentivize the former and discourage the latter. Through experimentation, they can evaluate the effectiveness of the prompts in prompting desired actions from users, as well as their impact on the overall success of those corporations. (Hendricks, 2019, p. 124).

References

American Library Association (17 January 2006). https://www.ala.org

American Library Association (19 August 2021). https://www.ala.org

Arendt, H. (1951). *The origins of totalitarianism*. Harcourt Brace & Company.

Barkun, M. (Ed.). (2013). *A culture of conspiracy*. University of California Press.

Barnes, J. (1994). *A pack of lies: Towards a sociology of lying*. Cambridge University Press.

Bartlett, J. (2018). *The people vs tech: How the internet is killing democracy (and how we save it)*. Penguin Random House UK.

Baudrillard, J. (1994). *Simulacra and simulation*. University of Michigan Press.

Baum, S. D., & Tonn, B. E. (2015). Confronting future catastrophic threats to humanity. *Futures, 72*, 1–3.

Berger, J., & Milkman, K. L. (2012). What makes online content go viral? *Journal of Marketing Research, 49*(2), 192–205.

Berridge, K. C., & Kringelbach, M. L. (2015). Pleasure systems in the brain. *Neuron, 86*(3), 646–664.

Boyd, D., & Crawford, K. (2012). Critical questions for Big Data. *Information, Communication & Society, 15*(5), 662–679.

Boyd, R. (2015, June 11). Man vs. machine: How humans are driving the next age of machine learning. *CRUNCH Network*. http://techcrunch.com/2015/06/11/man-vs-machine-how-humans-are-driving-the-next-age-of-machine-learning/#.frrlobk:gSSP

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 1–15.

Duggan, M., & Smith, A. (2016, October 25). The political environment on social media. *PEW Research Center*. https://assets.pewresearch.org/wp-content/uploads/sites/14/2016/10/24160747/PI_2016.10.25_Politics-and-Social-Media_FINAL.pdf

Etzioni, A. (1993). *The spirit of community: Rights, responsibilities, and the communitarian agenda*. Crown Publishers.

Flint, T., & Turner, P. (2016). Enactive appropriation. *AI & Society, 31*(1), 41–49.

Gellman, R., & Dixman, P. (2011). *Online privacy: A reference handbook*. ABC-CLIO.

Geist, E. (2015, March 3). Is artificial intelligence really an existential threat to humanity? *The Bulletin of the Atomic Scientists*. http://thebulletin.org/artificial-intelligence-really-existential-threat-humanity8577

Gerlitz, C. (2016). Interface methods: Renegotiating relations between digital social research, STS and sociology. *The Sociological Review, 64*(1), 21–46.

Hayles, K. N. (2017). *Unthought: The power of the cognitive nonconscious*. University of Chicago Press.

Hendricks, V. F., & Hansen, P. G. (2014/2016). *Infostorms: Why do we "like"? Explaining individual behavior on the social net* (2nd Rev. and expanded ed.). Copernicus Books/Springer Nature.

Hendricks, V. F., & Vestergaard, M. (2019). *Reality lost: Markets of attention, misinformation, and manipulation*. Springer Nature.

Kahneman, D. (1999). Objective happiness. In D. Kahneman, E. Diener, & N. Schwartz (Eds.), *Well-being: The foundation of hedonic psychology* (pp. 3–25). Russell Sage Foundation.

Kane, R. (Ed.). (2002). *The Oxford handbook of free will*. Oxford University Press.

Knight, W. (2015, December 29). What robots and AI learned in 2015. *MIT Technology Review*. http://www.technologyreview.com/news/544901/what-robots-and-ai-learned-in-2015/

Kringelbach, M. L., Stein, A., & van Hartevelt, T. J. (2012). The functional human neuroanatomy of food pleasure cycles. *Physiology & Behavior, 106*(3), 307–316.

Kringelbach, M. L., & Berridge, K. C. (2010). The neuroscience of happiness and pleasure. *Social Research, 77*(2), 659–678.

Lambert, A. D., Parker, M., & Bashir, M. (2015). Library patron privacy in jeopardy: An analysis of the privacy policies of digital content vendors. *Proceedings of the Association for Information Science and Technology, 52*(1), 1–9.

Looney, S., Conway, M., & Watkin, A. L. (2022). Violent extremism and terrorism online in 2021: The year in review. *Plymouth Research Commons*. https://plymouth.researchcommons.org/cgi/viewcontent.cgi?article=1235&context=scresearch

Lugya, F. K. (2014). What counts as a science and discipline in library and information science? *Library Review, 63*, 138–155.

Marr, B. (2015, December 17). Barbie wants to chat with your child – but is Big Data listening in? *Forbes*. https://www.forbes.com/sites/bernardmarr/2015/12/17/barbie-wants-to-chat-with-your-child-but-is-big-data-listening-in/#:~:text=Hello%20Barbie%20has%20a%20microphone,all%20in%20under%20a%20second.

Mosher, S. (2019). China's new 'social credit system' is a dystopian nightmare. *New York Post*. https://nypost.com/2019/05/18/chinas-new-social-credit-system-turns-orwells-1984-into-reality/

Mill, J. S. (1859). *On liberty*. J.W. Parker and Son.

Naughton, J. (2015, December 6). Should we be worried if our homes are soon smarter than we are? *The Guardian*. http://www.theguardian.com/commentisfree/2015/dec/06/smart-homes-security-risk-internet-of-things

Nicas, J., & Rosenberg, M. (2018, November 15). A look inside the tactics of Definers, Facebook's attack dog. *The New York Times*. https://www.nytimes.com/2018/11/15/technology/facebook-definers-opposition-research.html

Nisbet, M. (2012, April 30). Obama 2012: The most micro-targeted campaign in history? *Big Think*. http://bigthink.com/age-of-engagement/obama-2012-the-most-micro-targeted-campaign-in-history

O'Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.

Palmas, K. (2011). Predicting what you'll do tomorrow: Panspectric surveillance and the contemporary corporation. *Surveillance & Society, 8*(3), 338–354.

Parida, S. K. (2021). Telegram revolution: An analysis of political instability of Belarus in 2020. *Vital Library*. https://vital.lib.tsu.ru/vital/access/services/Download/koha:000723248/SOURCE1

Shera, J. H. (1973). For whom do we conserve, or what can you do with a Gutenberg Bible. In J. H. Shera (Ed.), *Knowing books and men: Knowing computers, too* (pp. 79–92). Libraries Unlimited.

Simon, H. A. (1971). Designing organizations for an information-rich world. In M. Greenberger (Ed.), *Computers, communications, and the public interest* (pp. 38–52). John Hopkins Press.

The Responsible Data Forum. (2015, April 10). Ways to practice responsible development data. https://responsibledata.io/ways-to-practice-responsible-development-data/

Zuboff, S. (2016, March 5). The secrets of surveillance capitalism. *Frankfurter Allgemeine Zeitung*. http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html?printPagedArticle=true

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.

Weltevrede, E., Helmond, A., & Gerlitz, C. (2014). Search engines: The politics of real-time: A device perspective on social media platforms. *Theory, Culture & Society, 31*(6), 125–150.

Whitehead, J. W., et al. (2002). Forfeiting 'enduring freedom' for 'homeland security:' A constitutional analysis of the USA Patriot Act and the justice department's anti-terrorism initiatives. *American University Law Review, 51*(6), 1081–1133.

Wijermars, M., & Lokot, T. (2022). Is Telegram a "harbinger of freedom"? The performance, practices, and perception of platforms as political actors in authoritarian states. *Post-Soviet Affairs*, *38*(4), pp. 267-287.

Wolfson, H [chair]. (2016, 19-21st Feb). Technological Displacement of White-collar Employment: Political and Social Implications. [Symposium]. Churchill College, Cambridge.