THE IMPACT OF INFORMATION TECHNOLOGY ON CIVIC PROTEST: A LEGAL OVERVIEW OF CIVIL RIGHTS AND CRIMINAL LIABILITY.

Adetola. A.O. Lawore-Akinyele, Michael Olusegun Eluyefa, Wilson Sakpere

ABSTRACT

The advent of information technology has fundamentally reshaped the dynamics of civic protests and democratic engagement in modem societies. In Nigeria, the widespread use of digital platforms such as social media, mobile communication tools, and online forums has facilitated mass mobilization, enabled real-time coordination, and amplified the voices of protesters beyond traditional geographic and political boundaries. While these technological advancements have enhanced citizen's ability to assert their constitutional rights-particularly the rights to freedom of expression, peaceful assembly, and association, they have also triggered a range of legal and regulatory challenges. By adopting a multidisciplinary approach, this article critically examines the dual impact of information technology on civil rights and criminal liability. It explores how state authorities have responded to digitally coordinated protests through legal sanctions including charges of cyber stalking, sedition, incitement, and breach of public peace. Drawing on relevant statutory provisions, Nigerian and comparative case law, and international human rights norms, the article analyses the adequacy of existing legal frameworks in protecting digital protest while maintaining public order. It argues for a more balanced, rights-based approach to regulation and calls for legislative and judicial reforms to prevent the misuse of criminal law in stifling legitimate dissent.

This article investigates the complex interplay between information technology and civil protests, with specific focus on the implications for civil rights and criminal liabilities. By adopting a multidisciplinary approach, this study investigates how Information technology has transformed the dynamics of civic protest, including the mobilization of protesters, the dissemination of information and the interaction with authorities. A critical analysis of existing literature, case studies, and empirical data is conducted to identify the opportunities and challenges presented by information technology in the context of civic protest. The findings of this study highlights the tension between the exercises of civic rights associated with the use of information technology in civic protest. Ultimately, this study aims to contribute to a deeper understanding of information technology in shaping the contours of civic protest and its implications for democratic participation, social justice and human rights,

Keywords: Information Technology, Civic protest, Civil rights, Criminal liabilities.

1.0 INTRODUCTION

The advent of Information technology has revolutionized the landscape of civic protests, enabling activists to mobilize, organize, and disseminate information with unprecedented ease and scale. However, this increased reliance on digital platforms has also exposed protesters to new and complex legal challenges, blurring the lines

BSC Psychology (Hons), LLB (Hons), LLM, PhD Candidate, Lead City University, Ibadan. Email:adetolalaworeakinyele@gmail.com

LLB, LLM, PhD Candidate, Lead City University, Ibadan

PhD, Lecturer and Head of Department, Computer Science, Lead City University, Ibadan. Email: sakpere.wilson@lcu.edu.ng

between civil rights and criminal liabilities. As government worldwide grapple with the implications of digital activism, it is imperative to investigate the intersection of information technology, civic protests, and the law. This study provides an in-depth examination of the impact of information technology on civic protests. Exploring the tensions between freedom of expression, assembly, and association, and the criminalization of online activism, explore the legal framework governing such activities and highlights the balance required between safeguarding civil liberties and addressing potential criminal liabilities.

In investigating this concept, relevant queries that croups up are; how does the use of information technology during civic protests affect the enforcement of protesters' civil rights? What legal liability arise for civil protesters as a result of IT usage during protests, and how are these liabilities accounted for; enforced? How can legal frameworks be adapted to address the challenge posed by IT in the context of civic protests while safeguarding civil rights liberties? Understanding these dynamics is crucial to safeguarding protesters' civil rights while ensuring accountability within the bounds of the law.

2.0 HISTORICAL CONTEXT

2.1. Civic Protests before the Prevalence oflnformation Technology:

Before the widespread adoption of Information Technology (IT) civic protests relied on traditional methods of communication and organization4.These methods, while effective in their time, were often slower and less scalable compared to the digital tools available today.

Communication and mobilization were mainly through words of mouth, distribution of printed materials and media broadcasting. Protesters relied on face-to-face communication to spread messages and recruit participants; for instance, gatherings in public spaces, religious institutions, or homes were common for planning activities. The use of Print Media included flyers, pamphlets, posters, and newsletters were essential for disseminating information. The civil rights movement in the United States during the 1960s used printed materials to inform communities and advocate for racial justice. Radio and Television provided an additional mean of broadcasting events after they occurred, these platforms helped spread awareness but were controlled by governments or large organizations, restricting their use for activist narratives.

For organization strategies, grassroots networks were relied on whereby activists depended heavily on localized, person-to-person networks. Leaders like Mahatma Gandhi in India and Martin Luther King Jr. in the U.S. orchestrated large movements through meticulous planning and regional coordination. There were Centralized Leadership with movements having clear hierarchies, with a few prominent leaders who coordinated actions and represented the cause.

Due to the above mentioned limitations, there were evident challenges such as, Limited Reach-Outs. Information dissemination was often localized, making it difficult to scale movements nationally or internationally. There was also the issue of Slow Response Time; coordinating responses to government crackdowns or emergencies required significant time, limiting the agility of protests. The protesters equally

---

Charles Tilly, Contentious Performances (Cambridge University Press 2008)

James J Jasper, 'The Art of Moral Protest: Culture, Biography, and Creativity in Social Movements' (1997) 61(3)AmericanJournal of Sociology 352

John Foran (ed), Theorizing Revolutions (Routledge 1997)

Sidney G Tarrow, 'Cycles of Collective Action: Between Moments of Madness and the Repertoire of Contention' (1995) 6(2) Social Science History 281

Gerbaudo, P. (2017). The Mask and the Flag; Populism, Citizenism and Global Protest. Oxford University Press. See also, Bakardjieva, M., Svensson,J., & Garden, J. (2018). Digital Citizenship and Digital Activism:A conceptual framework in Digital Activism in Asia (pp.21-28)

faced the challenge of facing the risk of isolation: Without global attention, governments could suppress protests with minimal accountability.

3.0 CIVIC PROTESTS IN THE DIGITAL ERA.

The incoming oflnformation technology and the availability of internet access has been claimed to have transformed civic protests, providing activists with tools to organize, amplify, and sustain movements with unprecedented speed and scale via the interjection of apt mediums of information communication technology. Social Media Platforms like Facebook, Twitter, and Instagram enabled real-time communication and mass mobilization. Hashtags such as #BlackLivesMatter and #MeToo turned localized concerns into global movements. Instant Messaging and Encrypted apps like Signal, WhatsApp, and Telegram allow secure and immediate communication among activists. IT allows for civic protest organizers to engage in crowdsourcing thus able to create virtual communities; this further enables collective decision-making and resource mobilization, from organizing rallies to fundraising.

The advent of information technology promoted the organizational strategies of civic protests as there can now be Decentralized Leadership as digital tools allow leaderless movements to thrive, such as the Occupy Wall Street protests. Online platforms facilitate collective action without reliance on hierarchical structures. Digital connectivity empowers activists to collaborate across borders, building solidarity and sharing strategies in real-time thereby enabling Global Alliance. Equally the concept of amplification and awareness is promoted. Real-Time Broadcasting through Live-streaming protests on platforms like YouTube and Instagram brings global attention, documenting events as they unfold, by so doing the truth of the civic protests is communicated at the same time thereby gathering global momentum. Citizen Journalism is enabled by Protesters using smartphones to record and share evidence of abuses, challenging state narratives and traditional media gatekeeping. To create virtual communities; this further enables collective decision-making and resource mobilization, from organizing rallies to fundraising. It is advocated that the transition from traditional to IT-driven protests marks a significant evolution in civic activism. While IT has democratized access to tools for organization and amplification, it has also introduced new challenges, such as surveillance and misinformation. This dual-edged impact continues to shape the dynamics of modem civic protests, offering activists powerful opportunities while necessitating greater awareness of associated risks.

3.1 The role of some specific information technology platforms in civic protests

Organization and Mobilization:

Information technology platforms like Twitter, Facebook, WhatsApp, and Signal have revolutionized the way civic protests are organized, mobilized, and amplified. These IT platforms have gone a long way in providing modem day civic protest activists with accessible, powerful, and scalable means to challenge authority, raise awareness, and build solidarity.

Twitter commonly referred to as the Catalyst for Real-Time Awareness; serves as a real-time information hub for civic protests. Its' concise format and use of hashtags have proven instrumental in rallying supporters, sharing updates, and drawing global attention to issues. Twitter plays a role in protest organization by enabling activists to coordinate events and disseminate information quickly. During the Arab Spring, hashtags like

"Defending the Rights toProtest" by ICNL2022 Published;October 2022.hrtps://www.icnl.org/post/analysis/defending-the-right-to-protest

[10] Manuel Castells, Networks ofOutrage and Hope: Social Movements intheInternetAge (2ndedn,Polity Press2015)

[11] Amnesty International,Toxic Twitter: AToxic Place for Women (Amnesty International 2018)

[12] Emiliano Tren::, 'The Dark Side ofDigital Politics: Understanding the Algorithmic Manufacturing of Consent and the Hindering of Online Dissidence' (2019) 22(7) Communication Theory 67

[13] Tarleton Gillespie, 'Platfonns are Not Intermediaries' (2018) 22(3) Social Media+ Society

#Jan25 (referring to Egypt's January 25 revolution) were used to organize protests and infonn participants of meeting points. Awareness and Global Solidarity is created during protests such as The Black Lives Matter movement used hashtags like #BLM to spread awareness about racial injustice, engage international audiences, and attract media coverage.

However, there are challenges associated to the use ofTwitter; it has faced criticism for being used to spread misinfonnation or by authoritarian governments to counter movements through propaganda and bot attacks.

Facebook commonly referred to as aPlatfonn for Community Building; provides aspace for protesters to create groups, share resources, and build asense of community. Its visual and textual capabilities allow for in-depth storytelling and advocacy. Activists use Facebook to organize events, recruit and mobilize participants.During the 2019 Hong Kong protest, Facebook groups were crucial for disseminating protest locations and strategies. Visual content, such as videos and images, shared on Facebook often goes viral, increasing the visibility of movements. For example, the Standing Rock protests against the Akota access Pipeline gained significant traction through Facebook live streams. Challenges commonly faced in the use ofFacebook in this regard is that Governments have used Facebook to monitor activists and censor content,and the platfonn's algorithms sometimes suppress activist posts.

WhatsApp is considered an Encrypted Coordination for Grassroots Movements. WhatsApp is a popular tool for private and encrypted communication,enabling activists to coordinate actions without fear of interception. During the 2019 Indian protests against the Citizenship Amendment Act, activists used WhatsApp to mobilize participants and coordinate on-the-ground logistics. Protesters use WhatsApp groups to share real-time live updates, such as police movements or safe routes, ensuring agility and safety during demonstrations.

Challenges associated with the use of this ITplatfonn includes it's closed nature which makes it difficult to reach a broader audience, and it has been criticized for the rapid spread of misinformation within closed groups.

Signal is noted as the Ultimate Tool for Privacy-Conscious Activists. Signal has emerged as a go-to platfonn for activists who prioritize security and privacy. Its open-source encryption and minimal data retention policies make it especially valuable for protests in authoritarian regimes.

Enhanced privacy features on the Signal app includes disappearing messages, encrypted calls, and anonymous registration protect activists from government surveillance. This has been vital for protesters in regions like Belarus, where the government uses extensive digital monitoring.

Hashtags and Viral Content have become central to the impact of Infonnation Technology on civic protests. These tools amplify messages, mobilize participants, and attract global attention, making them indispensable in modem activism.

Hashtags serve as a unifying symbol, allowing users to connect with specific movements and track discussions in real time. Their simplicity and accessibility make them powerful tools for building momentum. The key features of hashtags in protests includes organizing and mobilizing, raising awareness,and creating virality.

In organizing and mobilizing, hashtags provide a central point for coordinating efforts. For instance, #Jan25 was used during the Egyptian revolution to rally support and share updates, also #UmbrellaRevolution became a symbol of the Hong Kong democracy protests in 2014; just as #EndSARS in the Nigeria's national protest in 2020.Hashtags allow activists to reach global audiences instantly thus raising awareness for example, #MeToo turned personal stories of sexual harassment into a worldwide movement, sparking debates and policy changes across industries. The viral nature of hashtags ensures that movements can quickly gain attraction; in 2020,

[14] https://en.m.wikipedia.org/wiki/WhatsApp

[15] Leah A Lievrouw (ed), Alternative and Activist New Media (Polity Press 2011).

#EndSARS mobilized millions against police brutality in Nigeria, with celebrities and global organizations joining the conversation.

Challenges in this realm includes dilution of message. As hashtags trend, unrelated content can flood the discussion, diluting the core message. In addition, there comes in to play governrnent and opponent manipulation whereby some governrnents or counter-groups use bot accounts to flood hashtags with disinformation ordistract from the protest's agenda.

On the other hand, Viral content, including videos, images, and memes, has become a cornerstone of modem protests. These elements evoke emotional responses, making movements relatable and shareable, this generally amplifies the cause of the civic protest. Viral Content in Protests provides probable visual documentation of injustice, Videos and images provide undeniable evidence of misconduct, often sparking outrage and calls to action.For example: the video of George Floyd's death in 2020 spread rapidly on social media, galvanizing global protests under the #BlackLivesMatter banner. Viral footage of protesters being attacked during the 2019 Hong Kong demonstrationsdrew international condemnation of police brutality. Empathy and Engagement generated by means of Memes and short impactful clips distil complex issues into relatable formats, engaging younger audiences. For example, satirical memes during the #FridaysForFuture movement helped engage the youth in climate activism. Viral content creates a ripple effect, encouraging solidarity across borders. The protests in Iran following Mahsa Amini's death in 2022 gained international support through videos shared with #WomanLifeFreedom.

Like every other enabling IT application used by civic protesters in their cause, the Challenges encountered includes manipulation of content wherein Governrnents or adversaries can manipulate or fabricate viral content to discredit movements. In addition to this is the challenge of oversaturation whereby viral content risks becoming ephemeral, as platforms inundate users with new information daily, potentially reducing long-term impact.

Indeed, it has now become apparent that hashtags and viral content have redefined the dynamics of civic protests, transforming local grievances into global movements. They democratize activism by lowering barriers to participation, allowing anyone with an internet connection to contribute. However, to maintain momentum and credibility, activists must navigate challenges such as misinformation and content saturation strategically. These tools highlight the transformative power of IT in empowering modem civic protests.

3.2. Instances of Protest MovementsAmplified by Digital Platforms.

i) **George Floyd Protests (Black Lives Matter):** The murder of George Floyd in Minneapolis, Minnesota, in May 2020 became a focal point for protests against police brutality and systemic racism in the United States. Aviral video captured the police officer's knee on Floyd's neck, which sparked outrage globally. The video, initially shared by a bystander on Facebook, was rapidly disseminated across Twitter, Instagram, and otherplatforms, leading to widespread calls for justice and reform.

The Black Lives Matter (BLM) movement, which had already been active for several years, saw an unprecedented global wave of protests and online activism following Floyd's death. Digital platforms played a central role in organizing protests, creating petitions, sharing information about systemic racism, and raising funds for legal efforts. Hashtags like #BlackLivesMatter, #BLM and #JusticeForGeorgeFloyd gained massive traction, helping amplify the message ofracial equality and police accountabilityworldwide. The useoflive-streamingduring the George Floyd protests, particularly on platforms likeFacebookLiveandlnstagram,

---

[16] EndSARS: How Nigeria's youth found its voice with the protest movement, CNN https://www.cnn.com/2020/10/25/africa/ nigeria-end-sars-protests-analysis-intl

[17] Viral Content: Viral Impact: The Ripple Effect of Sharedable Content https://fastercapital.com/contentNiral-content--Viral-Impact--Viral-Impact--The-Ripple-Effect-of-Shareable-Content.html

References for the impact of George Floyd's death video on calls for justice and reform

allowed protestors to document clashes with law enforcement, police violence, and the overall atmosphere of unrest. This created immediate global awareness and empathy, putting pressure on authorities and leading to significant political and social discussions on systemic racism worldwide.

ii) **Hong Kong Protests (2019-2020):** The Hong Kong pro-democracy protests erupted in response to a proposed extradition bill in 2019. Protesters used digital tools, particularly live-streaming, to document their actions, especially as authorities were known to crack down on public protests. Pro-democracy activists employed Telegram, WhatsApp, and other encrypted messaging platforms to organize and communicate while bypassing government surveillance.

The protests were widely covered on social media, with images and videos of clashes between protesters and the police quickly spreading across the globe. Live-streaming platforms like Facebook Live and YouTube played a crucial role in broadcasting the events, allowing the world to witness the extent of the protests and the government's violent response. The hashtag #StandWithHongKong became a symbol of international solidarity, spreading across Twitter and Instagram as people worldwide voiced support for the Hong Kong protesters' struggle for democracy and autonomy. The movement also utilized crowdfunding campaigns to support legal defenses, medical supplies, and other resources needed for the protests.

iii) Arab Spring (2010-2012): Although earlier than the George Floyd and Hong Kong examples, the Arab Spring in countries like Egypt, Tunisia, and Libya showed the power of digital platforms in mobilizing protest movements. Social media platforms like Facebook and Twitter allowed activists to organize protests, share real-time updates, and document police violence during uprisings. YouTube became a significant platform for broadcasting violent confrontations between protesters and authorities, garnering international attention. All these brought international attention to grassroots uprisings in Tunisia, Egypt and Lybia, accelerating regime changes. The Facebook page "We Are All Khaled Said," which was created to honour a young Egyptian man beaten to death by police, played a central role in organizing protests in Egypt. The hashtag #Jan25 referred to the day protests began in Egypt, and it trended globally, demonstrating how digital platforms were integral to sparking the revolution.

iv) Nigeria #EndSARS (2020) wherein protesters in Nigeria used viral images of police violence to sustain momentum for the movement, while hashtags allowed activists to unify and coordinate globally but the lack of structured leadership limited post-protest policy impact. Platforms like Twitter provided a space for collective identity formation and ensured the documentation of state violence, but also highlighted the vulnerability of movements to state suppression through misinformation and censorship.

In summary, Information Technology has impacted real time protests worldwide, it can be rightly stated that Live-streaming and digital platforms have become essential tools for modem-day protests, amplifying the voices of those fighting for justice, freedom, and human rights. They allow for real-time documentation, global solidarity, and widespread awareness of injustices, making it possible for local movements to attract international support. The EndSARs, George Floyd protests and Hong Kong demonstrations exemplify how digital media can fuel widespread movements, enabling people around the world to mobilize and advocate for change. In an increasingly interconnected world, digital platforms will continue to be instrumental in shaping the dynamics of social and political movements.

4.0 SURVEILLANCE AND COUNTER MEASURES.

[19] Ibid, 18

[20] UNDP, Civic Space in the Digital Era(UNDPReport2021

[21] Philip N Howard and Muzammil M Hussain, 'The Role ofDigital Media' (2013) 22(2) Journal of Democracy 35

[22] Olumide Abimbola and Tobi Oshodi, 'The #EndSARS Protests and the Prospects for Youth-Led Digital Activism in Nigeria' (2021) 58(2)Africa Spectrum 121

[23] Ebenezer Babatunde Obadare, 'Digital Media and the Trajectory of the #EndSARS Movement in Nigeria' (2021) 39(4) Media, Culture & Society621

Surveillance in the digital age is increasingly pervasive, driven by both state security imperatives and corporate profit motives. Counter measures range from individual practices (for example encryption. Anonymity tools) to broader societal strategies (for example regulation, activism). Surveillance and countermeasures represent the ongoing technological arms race between authorities and protestors. Governments and institutions increasingly use advanced IT tools to monitor and control protests, while activists and protest groups employ counter-surveillance methods to protect their privacy and evade detection.
Governments increasingly rely on IT to collect vast amounts of data during protests. This data can be used for a variety of purposes, ranging from public safety to the suppression of dissent. Governments often justify the collection of data during protests in the name of public safety and national security. Surveillance tools like CCTV cameras, drones, and facial recognition systems are often deployed to monitor large crowds, track movements, and identify potential threats18

4.1. Authorities Usage ofIT for Surveillance.

This can be traced generally to tracking of digital footprints and Surveillance; during protests, participants often use mobile phones, social media, and other online platforms to communicate, organize, and document events. While these tools are essential for modem activism, they also generate digital footprints that can be tracked by authorities or other entities

i) **Facial Recognition Technology (FRT):** Facial recognition is one of the most controversial surveillance technologies used by authorities to monitor and identify individuals in crowds. By matching faces captured by surveillance cameras to databases ofknown individuals, governments can track and identify protesters. This technology is often deployed in urban areas, public spaces, and transportation hubs to monitor the movements of protestors. During the Black Lives Matter protests in the United States, there were concerns that facial recognition tools were being used by law enforcement agencies to identify protestors, especially in high-profile cities like New York where the New York Police Department [NYPD] employed facial recognition technology to identify Derrick Ingram, a protester accused ofcausing hearing damage to an officer with a megaphone.
ii) **Geolocation Tracking:** Geolocation tracking allows authorities to track the movement of individuals through their mobile phones or other GPS-enabled devices. Many protesters carry smartphones that constantly transmit location data via GPS. This data can be used to track the movements of individuals, especially in crowded environments like protests. Governments or private actors can track where protests occur, identify key organizers, and followprotestors inreal-time.
Apps and social media platforms may also collect location data, often without users fully understanding the extent to which their whereabouts are being monitored. Geolocation data can be harvested via apps, SMS, or location-sharing features on social media platforms.
During the 2019-2020 pro-democracy protests in Hong Kong, authorities reportedly used mobile phone location data to track activists and identify protest organizers. The government in Hong Kong also implement a real time mandatory SIM card registration program to help trace protestors. In Egypt during the Arab Spring, mobile phone services and internet access were shut down to prevent the organization of protests. CNET and the CNN

[24] Zeynep Tufekci, Twitterand Tear Gas:The Power and Fragility ofNetworkedProtest(Yale University Press 2017)
[25] Protesting in an Age of Government Surveillance- ICNL https://www.icnl.org/post/analysis/protesting-in-an-age-of-government-surveillance
[26] Ibid,25
[27] Cops across the U.S. are using facial recognition tech to arrest protestors https://www.inverse.com/culture/cops-across-the-us-using-facial-recognition-tech-to-arrest-protestors
[28] Ibid,25
[29] International Supreme Card l Real-name Registration Programme for SIM Cards https://web.three.com.hk/prepaid/realnameregistration/index.html

has been one of the coW1tries to impose frequent internet shutdowns during protests, particularly in Kashmir and during the farmers' protests of 2020-2021. This limits protestors' ability to organize and communicate, but also increases therisk that any remaining digital traces can bemonitored byauthorities.

viii). Data Collection by Third Parties: Aside from governments, third-party companies often collect and sell data on individuals, including those participating in protests. Social media platforms, advertisers, and even tech companies track user behaviour for commercial purposes. This data can include personal preferences, geolocation, browsing habits, and even interactions with specific posts or events. During protests, this data may be used by companies to target ads or influence public opinion.In some cases, third-party data can be accessed by governments through legal or extrajudicial means. Data brokers, for example, sell consumer data, which might be used to target protestors or monitor their activities.

ix). **Facial Recognition and Biometric Data:** Many companies use biometric data, such as facial recognition technology or fingerprints, to improve security or customer experience. However, this data can also be harvested without consent, and if these companies do not sufficiently protect the data, it can be accessed by governments or other entities for surveillance purposes. In protest settings, facial recognition software can be used to identify individuals in public spaces without their knowledge or consent. For instance, Clear View AI, a company that scrapes images from social media to build a massive facial recognition database, has faced legal challenges for scraping publicly available images. In protest contexts, .such companies might be used by governments or private organizations to track activists.

5.0. COUNTER SURVEILLANCE TOOLS

I) **VPNs (Virtual Private Networks):** VPNs are commonly used by activists to mask their location and encrypt their internet traffic, preventing authorities from tracking their online activities. The VPN creates a private, encrypted connection between the user's device and the internet, effectively hiding the user's IP address and physical location from surveillance tools.

Activists use VPNs to access social media platforms and communication channels in coW1tries where access is restricted or under surveillance. They also use VPNs to safely access the internet from public networks, such as those in cafes or libraries, which might otherwise expose them to eavesdropping.

ii) **Encrypted MessagingApps:**

Encrypted messaging apps like Signal, WhatsApp, and Telegram are widely used by protest groups to commW1icate securely without fear of interception. These apps use end-to-end encryption, ensuring that only the intended recipient can read the messages, and preventing third parties (such as law enforcement for hackers) from accessing the content ofcommunications.

Privacy International, 'Big Tech and Protest: How Companies Are Facilitating the Surveillance of Protesters' (2020) https://privacyinternational.org/report/4375/big-tech-and-protestaccessed 3August 2025.

[36] Julia Angwin, Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance (Times Books 2014)

[37] Amnesty International, 'Ban the Scan: Facial Recognition Technology Endangers the Right to Protest' (2021) https://www.amnesty.org/en/latest/research/202 l /06/ban-the-scan-new-york-city/

[38] Bruce Schneier, Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World (WWNorton2015)

[39] The 13 High-Tech Used by Protestors and Cops In Their Escalating Battlehttps://observer.com/ 2020/06/surveillance -technology-fueling-cops-vs-pratestor-battle/?

[40] JuliaAngwin See note 36

iii) **Anti-Surveillance Software:**
Anti-surveillance software is designed to block or mask various forms of surveillance. The use oflaser pointers, mirrors and face masking such as face paint, infrared LEDs, adversarial fashion disrupt surveillance drones or facial recognition Some tools protect users from facial recognition by blurring faces in photos or videos (for example CV Dazzle and adversarial makeup resist biometric surveillance), while others protect against tracking via cookies, geolocation or even ad networks. The "Privacy Badger" extension blocks spying advertisements, and "Tracker Blocker" prevents websites from tracking online behaviour. Some protesters also use software that disables or limits location-tracking on their devices.

iv). Burner Phones and Anonymous Communication:
Activists often use burner phones (temporary, prepaid phones) to avoid linking their real identities to protest activities. These phones are discarded after use, making it difficult for authorities to trace individuals involved in organizing protests.

v). Anonymous and Pseudonymous Means:
In addition, anonymous email services and pseudonymous accounts on social media help protestors maintain privacy and evade surveillance by avoiding the use of personal identifiers. Metadata Obfuscation with tools like CoverMe and ScrambleSuite obscure metadata to prevent profiling. Privacy-by-design tools like pseudonymization and differential privacy offer protection while ensuring compliance with data protection laws.

vi). Decentralized Communication Networks:
Some activists tum to decentralized communication methods, such as mesh networks (peer-to-peer networks that don't rely on centralized infrastructure) to bypass government-controlled communication channels. These networks can allow communication between protestors even when internet or phone service is shut down by authorities. In response to internet shutdowns during protests, some groups use Fire Chat, an app that uses Bluetooth and Wi-Fi connections to allow people to communicate without relying on mobile networks.

vii). PublicAdvocacy:
Legal frameworks and public awareness amplify the effectiveness of technological tools so as to counter invasive surveillance practise.

---

41 Computer Vision Dazzle https://en.m.wikipedia.org/wiki/Computer_vision_dazzle?, Ibid 39

42 Christopher Parsons, 'Beyond Privacy: Tools and Tactics for Resisting Surveillance' (2020) 12(1) Surveillance & Society 74; see also David Lyon, Surveillance Studies: An Overview (Polity Press 2007)

43 Tips for protesting oppressive regimes safely https://www.reddit.com/r/Preppi ng4Democracy /com men ts/1ikaver/ti ps_for_protesting_oppressi ve_regi mes_safely/?, Ibid 39

44 Ibid, 43; Ibid 39

45 Ian Brown and Dou we Korff, 'Tensions between Data Protection, Freedom of Expression and Government Surveillance' (2018) 16(2) International Data Privacy Law

46 Ibid, 43; Ibid, 39

5.1. The Concept oftheArms Race: Surveillance vs. Countermeasure.

The balance between surveillance and countermeasures creates a technological "arms race." As authorities develop more sophisticated surveillance tools, activists and protesters continue to innovate new ways to counteract these methods. While surveillance technologies, such as facial recognition and geolocation tracking, are increasingly being used to monitor public protests, counter-surveillance tools, including VPNs, encrypted messaging apps, and burner phones, are helping to preserve activists' privacy and security. This technological battle highlights the ongoing tensions between government control and individual freedoms, with digital tools playing a central role in both enabling protest movements and attempting to suppress them. As both authorities and activists continue to develop new techniques, the debate over privacy, surveillance, and freedom of expression remains a critical issue in the digital age.

6.0. LEGAL FRAMEWORKS ON CIVIL RIGHTS IMPLICATIONS

The freedom of speech and assembly are fundamental human rights, often protected by both international frameworks and domestic laws. These rights allow individuals to express their opinions and assemble in groups without fear of government retaliation. However, the advent of modem information technology (IT), especially in the context of social media and digital communication, has introduced new challenges in balancing freedom with control. Governments and private companies increasingly face legal battles regarding these rights, particularly when they intersect with the regulation of online platforms. Eric Barendt highlights the tension between free speech protections and state interests, arguing that legal systems must carefully balance these rights to prevent repression during civic protests.

There are in existence legal statutes that provides protection for Protester's Civil Rights Protections under International Frameworks; one of the key international framework safeguarding freedom of speech and assembly is the Universal Declaration of Human Rights (UDHR). The Universal Declaration of Human Rights, adopted by the United Nations in 1948, by its' Article 19 of the UDHR specifically addresses freedom of speech, stating that:

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regardless of frontiers. "

Article 20 of the UDHR addresses freedom of peaceful assembly and association, asserting:

"Everyone has the right to freedom of peaceful assembly and association. "

These articles highlight that the freedom to express oneself and gather peacefully is a universal right, with protection under international law. They emphasize the right to seek, receive, and impart information through

---

47 Wade K, Brubaker JR and Fiesler C, 'Protest Privacy Recommendations: An Analysis of Digital Surveillance Circumvention Advice During Black Lives Matter Protests' (2021) CHI Conference Extended Abstracts. dlnext.acm.org (https://dlnext.acm.org/doi/fullHtml/10.1145/3411763.3451749?)
Tufekci Z, 'Hong Kong protests become digital arms race against authorities' (Privacy International, 22 October 2019) Privacy International. Privacy International+ 1Privacy International+ 1 (https://privacyintemational.org/examples/4568/hong-kong-protests-become-digital-arms-race-against-authorities?)
Privacy International, 'Hong Kong protesters and police engage in digital arms race' (26 July 2020) Privacy International. Privacy International (https://privacyinternational.org/examples/4564/hong-kong-protesters-and-police-engage-digital-arms-race?)

48 Eric Brendt, Freedom of Speech (2nd edn, OUP 2007)

49 United Nations General Assembly. (1948). Universal Declaration of Human Rights. Retrieved from https://www.un.org/en/about-us/universal-declaration-of-human-rights.

any medium, which is especially relevant in the digital age where communication and assembly increasingly happen online

In addition, there is the International Covenant on Civil and Political Rights (ICCPR); the ICCPR, adopted by the United Nations in 1966, further protects freedom of speech and assembly. Article 19 of the ICCPR echoes the protections in the UDHR but also notes that restrictions on freedom of expression may be imposed in certain circumstances, such as protecting national security, public order, or public health. However, such restrictions must meet a high threshold of necessity and legality. Article 21 of the ICCPR protects the right of peaceful assembly, allowing individuals to assemble freely, provided the assembly is peaceful and does not disrupt public order. The ICCPR thus enshrines the idea that any restrictions on speech or assembly must be necessary and proportional, a principle that is often debated in the context of digital censorship or state-led crackdowns on online protests. The issue oflegal protections for protesters under the ICCPRArticle 21 have been explored, and it has been noted that while the international legal framework is comprehensive enforcement mechanism are often weak thus leaving protesters vulnerable to state abuses.

Examining the regulatory framework for peaceful protests under the United Kingdom Human Rights Act 199828, Meads finds that while the legal framework provides robust protections for peaceful protesters, police powers to impose restrictions can disproportionately limit civil rights. In the same vein it is opined that there is the need for greater accountability when policing protests in the UK particularly in the light of the challenges posed by broad discretionary powers given to law enforcement agencies.

There are equally legal statutes which provide protection to Protester's Civil Rights under domestic framework; for instance, in the United States, the First Amendment of the U.S Constitution provides robust protections for freedom of speech and assembly. It provides that congress shall make no law that tends to abridge the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances" - this protection covers both physical and digital spaces. The First Amendment has been the foundation for numerous landmark legal cases that define the limits of government control over speech and assembly in the U.S., including debates about free speech online.

For the purpose of impacting the civil right of Freedom of Assembly in some other Countries, they have incorporated the protection of speech and assembly into their constitutions and legal frameworks. For example, the European Convention on Human Rights (ECHR), under Article 11, protects the right to freedom of peaceful assembly and association, although this right can be restricted in cases of public safety or national security. Countries like Germany, India, and Brazil also have constitutional protections for freedom of speech and assembly, although they vary in scope and specific limitations. The situation in the United States, United Kingdom and Nigeria are as extensively discussed below in this article.

---

[50] United Nations General Assembly. (1966). International Covenant on Civil and Political Rights. Retrieved from h ttps://www.ohchr.org/en/instru ments-mechan isms/instru ments/in ternationa1-covenan t-c i vi1-and-political-rights

Jeremie Gilbert, 'Protesters' Rights in International Human Rights Law' (2020) 23(2) International Journal on Minority and Group Rights 156

[52] United Kingdom Human Rights Act 1998 - Legislation.gov.uk (https://www.legislation.gov.uk/ukpga/1998/42/contents)

[53] Aileen McColgan, 'The Right to Protest and the Police in the UK' (2015) 74(1) Cambridge Law Journal 1

First Amrnendment of the U.S Constitution https://constitution.congress.gov/constitution/amendment-1/

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) 4 November 1950, ETS No 5.

6.1. Statutory Provisions Enabling Protesters' Civic Rights.

In this section consideration shall be given to legal statutory provisions in the United Kingdom, United States of America and in Nigeria which enables individuals to exercise their civic rights of assembly, rights of protesting and right against unsolicited digital surveillance and recording. There are key legal statutes and constitutional provisions in the United Kingdom, United States, and Nigeria that protect individuals' civic rights to assembly, protest, and privacy against unsolicited digital surveillance. These statutes offer legal grounds for exercising and safeguarding these rights, although interpretations and enforcement can vary across jurisdictions. Protesters in these three jurisdictions in general, benefit from statutory legal frame works that supports the freedom of expression, freedom to peaceful assemble, right to private and family life, access to information and protection of personal data. Under the United Kingdom legislation there are the Human Rights Act I 998, Data Protection Act 2018, and Freedom of Information Act 2000 together forming a crucial trio of protective laws enabling civic protest, democratic engagement, and accountability of public authorities. The UK framework not only enables lawful protest but also regulates hoe authorities respond, fostering transparency, accountability and proportionality-all core principles of a democratic society.

On the other hand with regards to the United States of America, there are the four major legal provisions governing the realm of enabling the protester's civil rights; these includes the First Amendment, the Fourth Amendment, the Electronic Communications Privacy Act [ECPA] 1986 and the Privacy Act of 1974.Together these constitutional and statutory provisions for freedom of expression assemble, privacy, and control over personal data particularly relevant during civic protests. Key protection for protesters includes freedom of speech, freedom ofassemble, and right to petition.

Likewise, the Constitution, Cybercrime Act, Nigeria Data Protection Regulations Act [NDPR] and the Freedom oflnformation Act [FOIA] collectively provide the legal basis for civic protest, digital privacy and access to government information in Nigeria. While Cybercrime Act is considered a double edged sword potentially empowering of threating protest rights depending on its application, generally all these statutory provisions safeguard rights such as peaceful assembly and expression, data privacy, right to private family life/surveillance protection, freedom of thought/conscience and religion also access to government information and transparency.

All these above reviewed provisions collectively support individuals' rights to assembly, protest, and privacy in each country. A proper application of these legal provisions would indeed have gone a long way in positively shifting the paradigm of the impact of Information Technology on protesters civil rights. However, judging by real world occurrences the extent of protections and the effectiveness of enforcement vary, often requiring citizens to challenge infringements through legal means or advocacy.

---

56 HumanRightAct 1982, C.42 United Kingdom
57 Data Protection Act 2018,C.12 (Replaced the Data Protection Act, 1928)
58 Freedom oflnformation Act, 2000
59 First Amendment of the United States Constitution
60 Fourth Amendment of the United States Constitution
61 Electronic Communications Privacy Act of 1986 (ECPA)18U.S C S2510 et seq
62 Privacy Act of 174 (US), 5 USC S 552a
63 The Constitution of the Federal Republic of Nigeria, 1999 (as amended)
64 The Cybercrime (Prohibition, Prevention, etc) Act 2015, Laws of the Federation of Nigeria (LFN).
65 Nigeria Data Protection Regulations Act (NDPR), 2019
66 Freedom oflnformation Act (FOIA), 2011
67 Federal Republic of Nigeria SS 37, 38, 39, & 40.
68 Nigeria Data Protection Regulations Act (NDPR), 2019 & The Cybercrime Act, 2015
69 S.37, The Constitution of the Federal Republic of Nigeria, 1999 (as amended)
70 S.38, The Constitution of the Federal Republic of Nigeria, 1999 (as amended)
71 Ibid, 65

6.2.Legal Statutory Provisions Enabling the Use of Digital Surveillance Civic In Protests.

Just as there are legal statutes protecting the civil rights of protesters, so also are there statutes which provide a legal basis for the use of digital surveillance in relation to civic participation and protests but also include certain protections for individual rights. Using the same jurisdiction as above;

The three United Kingdom statutory provisions that provide legal foundation for state surveillance during civic protests are the Regulation oflnvestigatory Powers Act 2000, Investigatory Powers Act 2016 **[IPA],** Police, Crime, Sentencing and Courts Act 2022. These laws collectively enable UK authorities to conduct overt and covert surveillance, intercept communication and impose control measures on public protests, while also outlining procedural safeguards and oversight.

In respect ofUnited States of America, the covered legal instruments for government surveillance at civic protests are the USA Patriot Act [2000], USA Freedom Act [2015], Executive Order 12333 [1981], and the First Amendment to the United State Constitution. Key provisions of these statues is the permission to involve roving wiretaps, allowing the FBI to obtain any tangible things for investigations tied to terrorism or national security, enables surveillance of individuals not directly linked to terrorism, potentially including protesters deemed disruptive.

Coming down to Nigeria, the Constitution of the Federal Republic ofNigeria 1999 [as Amended], the Cybercrimes [Prohibition, Prevention, etc.] Act 2015, Nigerian Communications Act 2003 and the Official Secrets Act are relevant instruments applicable in this realm. Even though these instruments were not expressly drafted with civil protests in mind they have been interpreted, applied or enforced to justify, regulate, or limit government surveillance practices, particularly in the interest of national security, public order and crime prevention. The laws allow for limit to rights to privacy, expression and assembly; allow for inception of electronic communication, retention of individual's information, facilitate access to communications infrastructure for national security purposes. There is also provision for legal grounds for secrecy and surveillance operations by public officers especially in matters of state security. While these legal instruments are intended to serve public interest, they have often raised concerns of overreach especially where surveillance is done without court orders as statutorily prescribed for, or where technologies are used without transparency. Such acts infringes on the constitutional rights to privacy, assembly and expression. Therefore while surveillance powers exist, their exercise is meant to be judicially supervised, proportionate, and necessary, a standard that is inconsistently met in practise.

Findings from the legal frameworks herein reviewed reveal that each of these statutes and legal provisions reflects the tension between the right to protest and the state's use of surveillance, with varying degrees of safeguards across these countries .The legal frameworks in the United Kingdom and United State tend to include more oversight mechanisms compared to Nigeria, though concerns about proportionality and necessity in surveillance remain prevalent in all three nations. Human rights instruments like the ICCPR, ECHR, and national constitutions provide robust legal protections for protesters; however laws restricting protests (for example public order laws) and excessive police powers often undermine these rights. International law mandates proportionality and necessity in the use of force, but these principles are frequently violated. Protesters

[72] Regulation oflnvestigatory Powers Act 2000 (UK), c 23.
[73] Investigatory Powers Act 2016 (UK), c 25.
[74] Police, Crime, Sentencing and Courts Act 2022 (UK), c 32.
[75] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act 2001, Pub L No 107-56, 115 Stat 272 (US).
[76] USA Freedom Act 2015, Pub LNo 114-23, 129 Stat268 (US).
[77] Executive Order 12333-United States Intelligence Activities, 46 Fed Reg 59941 (4 December 1981) (US).
[78] United States Constitution amend I
[79] Nigerian Communications Act 2003, Cap N97,Laws of the Federation of Nigeria (LFN), 2004
[80] Official Secrets Act, Cap 03, Laws of the Federation of Nigeria (LFN) 2004, Section 1 - 3

face significant threats from state surveillance which infringes on privacy and create a psychological deterrent 'chilling effect' that discourages public participation in protests.

7.0 PROTESTER'S CRIMINAL LIABILITY AND LEGAL CHALLENGES

The use of information technology (IT) in protests has created new legal challenges for protesters, especially as authorities seek to regulate and control online activities related to activism. While technology enables faster mobilization, greater visibility, and broader participation in protests, it also increases the risk of legal consequences for those who use digital tools to organize, communicate, or participate in dissent. Protesters can face a variety of charges, ranging from incitement to cybercrimes, depending on the nature of their actions and the legal frameworks of the countries in which they operate. This section discusses the potential legal ramifications for protesters using IT during demonstrations, drawing on examples like the prosecution of individuals who use social media to organize or promote protests.

i). **Incitement to Violence or Unlawful Acts:** One of the most common legal issues protesters face when using IT tools is incitement to violence or incitement to illegal acts. Authorities often argue that using platforms like Facebook, Twitter, or Telegram to organize or encourage protests can lead to public disorder, violence, or civil disobedience, particularly if the protest involves acts those authorities considerunlawful, such as vandalism or property damage38. Incitement laws vary by country, but they generally criminalize the act of encouraging or urging others to engage in unlawful conduct. In some cases, individuals involved in organizing protests or sharing provocative content can be charged with incitement, even if they are not directly involved in violent actions.

ii). **Cybercrimes:** Protesters who use IT platforms to disrupt normal digital activities, such as denial of service attacks (DoS), hacking, or distributing illegal content, can be charged with cybercrimes which is enforced whereby cybercrime divisions employ advanced analytics and subpoena service providers to identify perpetrators. Many countries have cybercrime laws that criminalize the use of digital technologies to commit offenses like data breaches, hacking, or the disruption of websites and networks. For instance, hacktivist groups such as Anonymous have been involved in various protests, often using cyberattacks as a form of protest. In many jurisdiction, social media posts, tweets, or other online communications that encourage digital disruption can lead to cybercrime charges.

iii). **Spreading Misinformation orFake News:** Another legal risk for protesters using IT is being accused of spreading misinformation or fake news, especially in politically sensitive contexts. Governments often regulate online speech and content to prevent what they view as false information that could destabilize the state, inflame public opinion, or undermine public order. Government monitors digital communications and online activity in order to identify and charge individuals for violating speech related laws. Content shared online may also be used as evidence in court.

iv). Unauthorized Use ofEncrypted Communication: The useof encrypted communication tools, such as Signal, Telegram, or WhatsApp, is increasingly common among protesters who seek to protect their privacy from government surveillance. However, depending on the legal environment, some governments may interpret the use of encryption or other privacy tools as suspicious or even illegal. Some countries, the use of encrypted messaging services has led to legal action. For instance, in China, where authorities maintain strict control over internet and communication,individuals using encrypted tools to organize protests or avoid government

---

81 David Mead, The New Law of Peaceful Protest (Hart Publishing 2010); see also R v Gui [2013] UK.SC 64

82 C O Adebanjo, 'Misinformation, Fake News and the Digital Public Sphere: Legal Risks for Protest Movements in Nigeria' (2021) 5(2) Nigerian Journal of Cyber Law and Digital Rights 78.

83 Cybercrime (Prohibition, Prevention, etc) Act 2015, Laws of the Federation of Nigeria (LFN) Section 24, See also, Protection from Online Falsehood and Manipulation Act 2019 (Singapore), No 18 of2019

84 Onuorah v Kaduna State Government (2020) Unreported; see SERAP Commentary on Civic Space and Digital Rights (2021)

surveillance can face serious charges. The government's increasing use of surveillance technologies, including deep packet inspection to monitor encrypted communications, means that protestors could face criminal liability even if they are simply using encrypted messaging services to avoid state monitoring.

v). Data Privacy Violations: In some cases, protesters can be held accountable for data privacy violations, particularly if they share or leak personal data ofindividuals involved in protests. This could involve doxxing, the practice of publicly revealing private information (such as names, addresses, or phone numbers) about individuals, including law enforcement officers, public officials, or other protesters. Doxxing can lead to harassment, violence, or retaliation. In some jurisdictions, activists or protestors who engage in doxxing can face criminal charges related to the unlawful release of private data. For example, in Germany, laws are in place to protect individuals' personal information, and activists who share or release personal data without consent could face charges under the German Federal Data Protection Act (Bundesdatenschutzgesetz-BDSG).

8.0 THE LEGAL RESPONSIBILITY OF INFORMATION TECHNOLOGY COMPANIES IN ENABLING OR RESTRICTING CIVIC ACTIVISM:

IT companies play a key role in either enabling or restricting civic activism, and their actions can directly affect the success or failure of protest movements. As these companies have become the primary platforms for organizing protests, they face significant legal and ethical questions about their role in fostering or hindering public expression.

On the one hand, IT companies including social media giants like Facebook, Twitter, YouTube, and Telegram can enable protest and activism by providing platforms for people to share information, organize, and express dissent. These platforms often become digital town squares, where individuals can amplify their messages and mobilize others in a way that would be difficult through traditional media. Many activists argue that social media companies should provide stronger protection for users engaged in activism, preventing censorship and promoting freedom of expression. Going by a review of the trend locally and internationally, it is opined and rightly so that IT companies must navigate a complex landscape of legal pressures, corporate responsibility, and ethical concerns when it comes to protest movements.

On the other hand, IT companies are often pressured by governments to restrict content, block accounts, or censor posts related to protests. In many cases, these companies comply with government requests to avoid legal repercussions, fines, or the loss of access to the local market. Twitter, Facebook, and Google (through YouTube) have been repeatedly criticized for complying with government demands to censor protest-related content. Critics argue that large platforms prioritize profit and access to lucrative markets over the protection of free speech and activism.

IT companies are increasingly faced with questions about their legal responsibilities when it comes to protecting free speech and enabling civic activism. Many countries have laws that require IT companies to cooperate with law enforcement on issues such as terrorism, illegal content, and hate speech. However, the extent to which

---

85 Nigeria Data Protection Act 2023, Laws of the Federation of Nigeria; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation) [2016] OJ Lll9/l; Privacy Act of 1974 (US), 5 USC§ 552a; See also AO Olowu, 'Data Privacy, Surveillance, and Protest Rights in Africa: Legal Gaps and Emerging Norms' (2022) 14(1) African Journal of Human Rights Law and Practice 113.

86 Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG), Act to Adapt Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680, BGBI I 2017, 2097 (Germany).

87 Paradigm Initiative for Digital Rights v Nigeria [2022] ACHPR/COMM/7 47/21

88 United Nations Human Rights Council, Report of the Special Rap rteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression (A/HRC/38/35,6Apnl 2018). See also, SVaidhyanathan,Antisocial Media: How Facebook Disconnects Us and Undermines Democracy (Oxford University Press 2018).

companies should cooperate in restricting civic activism is a point of contention. One of the key ethical dilemmas faced by IT companies is whether to protect users' rights to free speech and privacy or to comply with government regulations that may infringe on those rights

As these issues have become more prominent, many civil rights organizations have called for stronger global standards that would hold IT companies accountable for their role in activism suppression. Proposals include creating international regulations that protect freedom of expression and privacy online while ensuring that companies cannot be easily coerced into suppressing protest activities.

Governments and IT companies both play central roles in how technology is used during protests, and both are capable of misusing or abusing IT to undermine protest movements and limit civic activism. Governments use internet shutdowns, censorship, and surveillance technologies to control and suppress dissent, while IT companies are often caught between providing platforms for activism and complying with government demands for content moderation and surveillance. The challenge lies in holding both parties accountable for their actions, ensuring that digital activism can thrive without fear of repression, and protecting the fundamental rights of individuals to freely express their views online.

In Nigeria, social media companies have been asked to remove protest-related content, block accounts, or deactivate services that could facilitate dissent. Facebook and Twitter have faced requests from the Nigerian government to take down protest-related content, especially during the #EndSARS protests. Social media platforms have had to balance local compliance with the global standards of free expression. However, the government has also used legal threats to force compliance, and many activists argue that companies prioritize access to the Nigerian market over the protection of free speech. The suspension of Twitter in Nigeria, although temporary, highlighted the tension between corporate responsibility and government control. While Twitter claimed the ban was a free speech violation, the government argued that the platform had been used to incite violence and disorder. In response to the ban, Nigerian activists called for greater support from tech companies in standing up for human rights and free speech.

Generally, IT companies face significant ethical dilemmas regarding their role in enabling or restricting protests. On the one hand, they are obligated to comply with local laws, but on the other hand, they must also respect global human rights standards. Many international organizations, such as Human Rights Watch and Amnesty International, have urged tech companies to take a stronger stance against government actions that infringe on freedom of expression and the right to protest. They argue that corporations must be accountable for how they handle requests to censor content or limit access to communication tools that facilitate protest.

A growing movement is calling for tech companies to adopt transparency and accountability measures, such as publishing detailed reports about content removal requests and their compliance with government demands. These measures are crucial in holding companies accountable for their role in restricting or enabling civic activism.

9.0. CONCLUSION:

Withoutaniotaofdoubttheriseofinformationtechnology(IT)hassignificantlyreshapedthenatureofprotests and activism worldwide. While digital tools have become vital for organizing and amplifying protest

89 Okediran v Nigerian Communications Commission [2020] NGHC 84

90 Amnesty International, 'Nigeria: EndSARS Protests and the Role of Social Media Companies' (2021)

91 Paradigm Initiative, 'Digital Rights in Africa Report 2022: Nigeria Chapter' (2022) . See also Privacy International, 'Nigeria's Surveillance State and IT Companies' Accountability' (2021) (https://privacyinternational.org/) also Global Network Initiative, 'Corporate Responsibility and Free Expression: Lessons from Nigeria' (2020) (https://www.globalnetworkinitiative.org/)

movements, they have also introduced complex ethical, legal, and social challenges. Governments, corporations, and civil society must navigate a delicate balance between ensuring security, protecting privacy, and upholding freedom of expression Digital activism has proven to be a crucial tool for mobilization, awareness, and solidarity. However, these technologies are also vulnerable to manipulation, such as disinformation campaigns, state-sponsored surveillance, and government-imposed internet shutdowns as governments around the world have increasingly used IT tools to monitor, control, and suppress protests. Technologies like facial recognition, geolocation tracking, and internet shutdowns have been employed to track protestors,stifle dissent, and maintain order.The useof surveillance technologies during protests raises critical ethical questions about the balance between security and civil liberties. Surveillance technologies are employed differently across political systems, with authoritarian regimes typically using them to suppress dissent more directly, while democratic nations such as Nigeria faces complex and ethical debates over surveillance. In many cases, government surveillance is justified as necessary for public safety or order, but it often comes at the expense of personal privacy, freedom of assembly, and the right to protest. The legal consequences for protestors using IT to organize and mobilize can be severe, including charges of incitement, cybercrimes, or terrorism. The role ofIT companies in facilitating or restricting protest movements is crucial in the global digital landscape.. Companies must remain accountable for how their platforms are used and ensure that they donot become tools for state repression.

Legal framework struggles to keeppace with the evolving role ofIT in protests; often where there are in existence protective legislations, the appropriate mode of implementation are not explicitly stated out thus making avenues for such legislations to be interpreted and boycotted to the detriment of the protesters civil rights. Although legal provisions in some of the developed nations stipulates that surveillance must meet a test of proportionality and necessity even though law enforcement is allowed to usedigital surveillance tools to monitor potential orongoingprotestsundernational security orpublic safety grounds, however there are few robust privacy protection under these laws which should provide a check and balance on excessive usage; to achieve this there must beprovisions requiring oversight by investigatory powers for example obtaining of approval from the Commissioner of Police or surveillance warrants approval from Secretary of State and a Judicial Commissioner

By implementing stronger legal protections, establishing limits on surveillance technologies, ensuring corporate accountability, and promoting digital literacy, we can help ensure that IT continues to serve as a tool for empowerment and democracy, not as a means of oppression. Policymakers, tech companies, and civil society must work together to safeguard the right to protest and protect fundamental freedoms in the face ofdigital surveillance.

10.0.RECOMMENDATIONS:

In order to adapt frameworks that will address the challenges posed by Information Technology (IT) in the context of civic protests while safeguarding civil liberties; it would require a balanced approach that gives due consideration to technological advancements, the rights of individuals and the need for public order. Adetailed explanation ofhow this can be achieved is hereby outlined below:

i).**Strengthen Legal Protections forCivil Rights:**

National laws must be reformed to safeguard digital activism and ensure that protesters are not subject to disproportionate penalties for using IT platforms to organize peaceful demonstrations. There should be clear protections against incitement charges for peaceful protests conducted via social media and other digital platforms. Cybercrime Laws must be updated; these laws must strike a balance between addressing genuine threats (e.g., hacking or disinformation campaigns) and avoiding overly broad provisions that criminalise legitimate protest activities. There must be clarity in legal definitions of offences to prevent misuse of laws to target activists, provisions of the law must stipulate a differentiation between acts of civil disobedience and malicious cyber activities to ensure that peaceful protesters are notunfairly penalized.

ii). **Establish Clear Limits Guidelines on Surveillance** Technologies: Governments should be transparent about their use of surveillance technologies, such as facial recognition, geolocation tracking,and datacollection,

during protests. These tools should only be used under strict legal safeguards and in a manner that does not violate civil liberties.

There should be clear limits on how long surveillance data can be retained and who has access to it. Independent oversight mechanisms should be established to ensure that these technologies are not misused or abused for purposes of political repression.

Define specific conditions under which surveillance can be authorised, such as credible evidence of threats to public safety. Mandate judicial or independent oversight to approve and monitor surveillance activities.

iii).Ensure Greater Accountability for IT Companies: It is recommended that there should be put in place regulation of the private sector's involvement by imposing accountability measures on private technology companies providing surveillance tools to governments. Transparency about partnership between government and private entities in surveillance programs should be mandated. Companies should be required to provide detailed transparency reports on content removal and data sharing requests from governments, and refuse requests that infringe on free speech.

Global human rights standards should guide the practices of tech companies, ensuring that they respect user rights and democratic freedoms even in repressive regimes.

iv).Promote Digital Literacy and Data Privacy Education:

Awareness campaigns on digital rights and privacy protection should be prioritized to empower individuals to navigate the challenges posed by digital surveillance and to protect their fundamental rights.

v).International Collaboration for Digital Rights: International collaboration is essential for establishing global standards that protect the right to protest in the digital realm. Governments, tech companies, and civil society should work together to create international agreements that limit the use of surveillance technologies and ensure the protection of freedom of expression online. Align national policies with international conventions, such as the Universal Declaration of Human Rights and the ICCPR.

vi). Combat Transnational Surveillance Abuse: There should be put in place establishment of concensors to prevent the export of surveillance tools to regimes with poor human right records. The government should create international mechanisms to investigate and penalize cross-border surveillance abuses.

vii). Technology Innovation and Safeguards: Consideration should be given to fostering privacy respecting innovation; incentivize research of technologies that enhance security without infringing on privacy.

viii). Legal framework: There should be in place legal framework that provide robust privacy protection, ones that do not just allow for broad discretion in surveillance activities; bur rather ones that puts in place clearly defined and stringent oversights which provides adequate checks and balances on the excessive usage of surveillance under the guise of state security.

ix). Crisis Specific Measures: It is recommended that there should be specific guidelines for usage of surveillance during crises. This can be done by limiting the scope of surveillance during emergencies (such as protests) to a temporary measure with clear expiration dates. Inclusion of the "*sun set clauses*" in emergency law so as to ensure they expire once the crisis is resolved thereby preventing long-term encroachment on rights.

x).Judicial Recourse, Remedies and Legal Protections: Consideration should be given to putting in place accessible legal avenues for individuals to challenge unlawful surveillance so as to create a means of strengthening legal recourse must be put in place and properly implemented.

By adopting these policy recommendations, governments can protect civil rights while maintaining public safety, fostering trust, and ensuring that the right to protest is preserved in the digital age also limiting the undue generation of criminal liabilities for protesters.