Sharon's Research Portfolio

The following is a compilation of short research papers I wrote weekly as part of my LL.M program, each with a 500-word limit. They explore a variety of topics, including Cyber Law, Telecommunications Law, AI and Robotics Law, E-Commerce Law, Information Control Law, and E-Governance Law.

Semester 1

Table of Contents

Introduction & Reflectivity Statement

Abstract

This is a portfolio of research papers on Ghana's telecommunication regulation and transformation, the

country's cybersecurity laws, and internet governance in general. The selected papers cover a range of **interconnected themes**—digitalization policies, cyber law, telecom regulation, internet governance, and legal frameworks for emerging technologies—all of which are essential to Ghana's evolving digital economy. This compilation reflects both the challenges and opportunities in **Ghana's digital transformation journey** and offers policy recommendations on how laws and policies may be used to foster the budding digital transformation.

Why These Papers?

These papers were chosen for their relevance to the current space in IT Law. Each one discusses a critical part of digital governance. The papers on e-voting, leapfrogging, and drafting a Heads of Agreement reflect my interest in the practical application of the knowledge acquired in the real world. Additionally, these papers challenge Ghana's existing frameworks on telecommunication, e-governance, and cyber law, pushing for a stronger, forward-thinking approach to regulation.

What My Compilation Says About Me

My approach to learning is analytical. I am always looking to connect the dots, tie it all together, and understand the bigger picture. My communication style is structured and ensures that every essay logically builds a cohesive and well-supported argument. In this program, I found tech governance, cyber law, e-voting systems, and drafting agreements the most engaging. These topics allowed me to understand how law works to regulate technology and how these results inform policy making.

Despite this, I recognize that one major **shortcoming** I faced in my first semester was identifying loopholes in existing laws and recommending authentic, unique policy solutions to fill the gaps. I look forward to sharpening my skills in this area next semester.

The themes addressed in this portfolio reflect Ghana's digital future and my own academic and professional growth. Moving forward, my goal is to continue gaining research experience in these areas and contribute to policy making efforts that ensure sustainable technological progress in Ghana and beyond.

Section 1: E-Governance & Digitalization

Exploring policies and frameworks that drive Ghana's digital transformation

1.1 Enhancing Ghana's Digital Transformation Through the Implementation of 'Digital by Default' Policies

This paper examined policy-driven digitalization in Ghana and the role of government in fostering an enabling environment through laws and policies that accommodate digitalisation.

Introduction

The aim of the African Union (AU) **Digital Transformation Strategy**[1] goal is to have "A Digitally Transformed Continent for Prosperity and Inclusivity." The strategy includes foundation pillars, critical sectors, and cross-cutting themes, each with unique roles to play in Africa's digitisation journey. The foundation pillars are central to the strategy, one being "Enabling environment, Policy and Regulation." **This paper applies "digital by default" principles to design policy recommendations for Ghana, that create an enabling environment for digitalization through policies and regulations**

Understanding Digital by Default

Digitalization is a way of thinking where technology is used to carry out everyday tasks, while digitization is the process of using technology to optimize formerly analog processes."Digital by default" in public service delivery prioritises digital technologies and online platforms as the primary means for delivering services efficiently. **Multi-channel delivery**, is one of its principles which states that public services should be delivered through various digital and non-digital channels in a way that accommodates all users. It also envisages that trust in digital systemsstarts with **data protection and security**. Also, the principle of **'no one left behind'** ensures inclusivity of minority groups people in rural areas.

Challenges in Ghana and Policy Recommendations

Digitalization of basic services in Ghana incorporates the "digital by default" principle in services such as the new online passport application process, the e-justice platform, and the Ghana Post GPS addressing system. Efforts have also been made to regulate digitalization in Ghana, through policies

[1] African Union, The Digital Transformation Strategy for Africa (2020-2030) (2020)

such as the Ghana ICT for Accelerated Development (ICt4AD) Policy[2], the National Broadband Policy & Implementation Strategy[3], and the Ghana National Cyber Security Policy & Strategy[4].

From 2014 to 2020, Ghana's ICT sector grew by an average of 19% annually, making Ghana a digital leader in Sub-Saharan Africa. [5] Despite this growth, Ghana's digitalization efforts is still challenged.[6]

In Ghana, digital infrastructure is developed in urban areas, leaving many rural areas with limited internet access and creating significant connectivity gaps. By applying the **"no one left behind"** principle, internet infrastructure should be extended to said rural areas through public-private partnerships (PPPs) that incentivize private companies who extend fiber optic cables and broadband networks to underserved communities.

Ghana's cyber ecosystem also remains underdeveloped, with limited public awareness and a weak cybersecurity culture. The principles of **State-Space Reconstruction** can be applied to design policies that reform public sector operations to integrate cybersecurity measures. Legislation requiring software companies to implement security measures must also be enforced. Digital literacy seminars and cybersecurity education must be integrated into the national curriculum at all educational levels, as well as cybersecurity training and certification for professionals and small company proprietors.

Conclusion

Ghana has made significant progress in creating an enabling environment, policies and regulations for digitization. Advancing this progress requires policies that incentivize the extension of broadband networks into rural areas and policies that sensitize citizenry on cybersecurity awareness.

Critique

In his essay, "Strategies for Enhancing Cybersecurity in Ghanaian Digital Banking," **Nana Ayiwah** argues that "digital by default" principles should be embedded from the start, rather than be added later. I find this idea important because treating digital by default as an afterthought often leads to inefficiency in digital systems. By integrating these principles early, we can design systems that are

[2] Ministry of Communications, Ghana ICT for Accelerated Development (ICT4AD) Policy (2003).
[3] Ministry of Communications, National Broadband Policy and Implementation Strategy (October 2012).
[4] Cybersecurity Authority, National Cybersecurity Policy & Strategy (2023)
[5] World Bank Group, 'Ghana - Digital Acceleration Project' (Washington, DC, 2022) http://documents.worldbank.org/curated/en/938111649959522167/Ghana-Digital-Acceleration-Project accessed 9 November 2024.
[6] The World Bank, 'Ghana Digital Economy Diagnostic' (2020) https://pubdocs.worldbank.org/en/412821598381054828/Ghana-DE4A-LOW-Res.pdf accessed 9 November 2024.

more secure, user-friendly, inclusive and adaptable to future needs, reducing the risk of costly adjustments and security vulnerabilities down the line.

Moreover, I believe this integration, following the agile approach, should include continuous user feedback and iteration during the design phase. Gathering feedback early on could help identify loopholes and usability issues. This approach aligns with best practices in user-centered design, which is particularly important in a context like Ghana, where digital literacy levels vary widely.

Additionally, another colleague **(22260408)** highlighted the importance of designing digital education frameworks that accommodate students with disabilities. This aligns well with the inclusivity aspect of "digital by default." While I agree, I would extend this idea by noting that true inclusivity in digital frameworks must also address infrastructure challenges, particularly in rural areas where internet access is limited. Without considering these barriers, even the best-designed accessible features may not reach the intended users.

1.2 Leap, But Look First: A Thoughtful Approach to ICT Leapfrogging for Socio-Economic Development in Ghana

This paper analyzes the pros and cons of ICT leapfrogging in Ghana, and how the rapid digital transformation age can be approached sustainably for socio economic development.

Introduction

Frontier technologies are driving the world's technological progress. This presents developing countries like Ghana, a two-way road: the advantage of leapfrogging legacy technologies or risking being left behind.

According to "catch-up" theory[7], developing countries must follow the same development path as more developed countries in order to advance. With the emergence of frontier technologies, it has been counterargued that developing countries without legacy technologies have the opportunity to bypass traditional stages of technological development and directly adopt digitised solutions.[8] [Digitization is

[7] Calestous Juma and Norman Clark, 'Technological Catch-Up: Opportunities and Challenges for Developing Countries' (January 2002)
[8] African Union, The Digital Transformation Strategy for Africa (2020-2030) (2020)

converting information to digital form, while digitalization is the broader transformation of operational processes with digital technologies.[9]]

I argue that Ghana can leapfrog but must do so cautiously for sustainability.

Leapfrogging is

"... the adoption of advanced or state-of-the-art technology in an application area where immediate prior technology has not been adopted." [10]

A country's ability to adopt emerging technologies has been said to directly contribute to its competitive advantage. Countries that fail to adopt emerging technologies may eventually be excluded from the global economy.[11] For developing countries like Ghana, leapfrogging becomes a necessity rather than a luxury.

Advantages of Leapfrogging

In Ghana the adoption of mobile phones and mobile money services, without prior landline and banking infrastructure, have increased financial inclusion for rural folks.[12] This demonstrates how **leapfrogging can boost socio-economic development**.[13]

Leapfrogging also **enhances governance through e-governance**. E-governance is the broader use of technology to enhance decision-making in governance, while e-government focuses on delivering government services through digital platforms.[14]

Leapfrogging also offers **cost effective and user-friendly solutions**[15]

Factors to Consider Before Leapfrogging

[9] SAP, 'Digitization vs. Digitalization' https://www.sap.com/africa/products/erp/digitization-vs-digitalization.html accessed 21 November 2024.
[10] Michelle W L Fong, 'Technology Leapfrogging for Developing Countries' in Mehdi Khosrow-Pour (ed), Encyclopedia of Information Science and Technology (2nd edn, IGI Global 2008), pp 3707
[11] United Nations Conference on Trade and Development (UNCTAD), Trade Policies, Structural Adjustment and Economic Growth: Trade Policy Reforms in Developing Countries and the International Support Required (1993).
[12] United Nations Conference on Trade and Development, 'Look Before You Leap' (Policy Brief No. 71, December 2018), 1.
[13] Ibid. p.2
[14] Vephkhvia Grigalashvili, 'E-government and E-governance: Various or Multifarious Concepts' (2022) 5 International Journal of Scientific and Management Research 183.
[15] See note 4

Despite the advantages, certain factors must be considred when adopting frontier technologies because technology is an enabler not a panacea[16]. It only boosts development efforts but does not cure fundamental problems.

1. Research is needed to assess the current technological climate, including infrastructural gaps and varying digital literacy levels across demographics. Furthermore, evaluating successful and unsuccessful leapfrogging cases in other countries can help Ghana avoid certain pitfalls. Additionally, examining the potential impacts of adopting emerging technologies will help us anticipate and prepare for any disruptive effects on various socio-economic sectors.

2. Leapfrogging requires strategic innovation policies that support the adoption of emerging technologies[17] and foster competitive markets. The AU's Digital Transformation Strategy emphasizes the need for policy environments that ensure data protection, inclusivity, and the accommodation of frontier technologies.[18] Ghana can leverage advisory support from international bodies like UNCTAD and the Commission on Science and Technology for Development to design effective innovation policies.[19]
3. As outlined in the AU's Digital Transformation Strategy, **digital infrastructure** including telecommunication networks, broadband, and data centers, are essential for digitisation and leapfrogging [20].

Disadvantages of Leapfrogging

Despite the benefits, leapfrogging may also create a digital divide - an imbalance of access to digital technology in rural and urban areas. Consequently, the adoption of such technologies should focus more on inclusion of users than the technology. [21] To prevent a digital divide, public private partnerships can support initiatives that expand wireless communication access to rural areas.

Conclusion

While leapfrogging presents an opportunity to accelerate socio-economic development, without good planning, it can be an expensive failure and can exacerbate already existing developmental challenges. ICT leapfrogging in Ghana is necessary but must be done cautiously.

[16] See note 4
[17] ibid
[18] See note 2
[19] See note 5
[20] ibid
[21] See note 4

Critique

22260408 argues in favor of leapfrogging. While I don't disagree with this argument, one angle that was not considered is the factors and risks involved in leapfrogging. When adopting emerging technologies, factors such as the availability of sufficient local expertise and infrastructure should be taken into consideration. The absence of these can cause Ghana to become overly reliant on foreign aid and stifle innovation and digitalization efforts. The author could strengthen their argument by discussing how Ghana might mitigate such risks, for instance, through capacity-building initiatives or partnerships with local tech startups.

In their essay, **22256923** argues for a cautious leapfrogging approach and highlights the need to train human capital to manage emerging technologies. They argue that subjects like Mathematics, Science, and Technology should be taught to equip citizens with the right skills to operate digital technologies. While focusing on teaching STEM is important, this approach overlooks the immediate need for digital literacy programs at a basic level, especially in rural and underserved communities. Vocational training and reskilling programs, can quickly fill gaps in the labor market for emerging tech industries. For instance, short-term coding bootcamps or digital marketing courses could provide practical skills without the lengthy timeline of formal STEM education.

1.3 Legal and Technological Considerations for Implementing an E-Voting System in Ghana

This paper discusses the legal, technological, and policy factors that must be considered for digitising Ghana's electoral processes. The paper designs a sample e-voting system for Ghana called "The Secure National E-Voting System" (SNES)

Introduction

In an era where technology is reshaping governance and democratic participation, concepts like e-governance, e-government, and e-democracy have become increasingly relevant. These concepts represent different yet interconnected approaches to integrating Information and Communication Technologies (ICTs) into governance and public life. The purpose of this paper is to design a national e-voting system that promotes e-governance, e-government, and e-democracy. This design includes legal and non-legal tools, design specifications, implementation steps, and the legal instruments

required for effective implementation. This paper also discusses Ghana's current manual voting system and its flaws and suggests ways in which an e-voting system can fill up these gaps. We also examine countries that adopted e-voting and succeeded, and ones which did not.

E-Governance

E-governance is a broad framework that uses ICTs to enhance government processes, decision-making, and relationships with society.[22] It addresses not only service delivery but also how ICTs influence institutional structures and interactions between government and citizens.[23] E-governance aims to make governance systems more transparent, participatory, and efficient, ensuring that technology is an enabler of good governance rather than just a tool for automation.

E-Government

Within the broader scope of e-governance lies e-government, which focuses on using ICTs to deliver public services more efficiently.[24] Examples include platforms for e-tax filing, e-health services, and e-transportation systems. While e-government emphasizes transactional efficiency, it does not replace traditional government structures. Instead, it complements them, providing citizens with faster and more accessible service delivery mechanisms.

E-Democracy

E-democracy, often seen as a subset of e-governance, is concerned with the use of ICTs to enhance citizen participation in governance and decision-making.[25] It emphasizes empowering citizens to engage in the democratic process by fostering dialogue, accountability, and inclusiveness. Tools such as online petitions, social media platforms, and digital town halls illustrate how e-democracy creates spaces for interaction between citizens and their representatives, strengthening democratic systems. E-democracy builds on the infrastructure established by e-government but shifts the focus from service delivery to active citizen engagement.

Formative Principles & Objectives of E-Democracy

[22] F Bannister and R Connolly, 'Defining e-Governance' (2012) 8(2) E-Service Journal 3 https://doi.org/10.2979/eservicej.8.2.3 accessed 18 January 2025.
[23] ibid
[24] E Abu-Shanab, 'E-democracy: The Fruit of E-government' (2015) International Journal of Technology and Globalisation https://www.researchgate.net/publication/306167221 accessed 18 January 2025.
[25] R Kies, F Mendez, P Schmitter, and A Trechsel, Evaluation of the Use of New Technologies in Order to Facilitate Democracy in Europe (STOA 116 EN), European Parliament Report (2004) https://www.europarl.europa.eu/thinktank/en/document/IPOL-JOIN_ET(2003)471583 accessed 18 January 2025.

The objectives of e-democracy include strengthening public trust in government, enhancing transparency, and improving citizen-government relations. It aims to foster proactive citizen participation in policymaking, enable continuous interaction between citizens and representatives regardless of time or location, and empower citizens to propose policy options and shape policy dialogue effectively.[26]

The formative principles of e-democracy focus on democratic development by increasing transparency in political processes, enhancing citizen participation, and improving opinion formation through accessible, interactive, and user-friendly technology.

Fundamentally, the foundation of electronic democracy is characterized by effective communication systems dedicated to active and meaningful citizen participation, rather than being merely limited to the distribution of information.

E-Voting

E-voting is a critical intersection of e-governance and e-democracy. It applies technology to one of the most fundamental aspects of democracy—elections. By enabling citizens to cast and count votes electronically[27], e-voting systems aim to make the electoral process more secure, accessible, and efficient. Examples of e-voting systems include electronic voting machines, online voting platforms, and mobile voting applications.

E-voting, more broadly defined, refers to voting systems in which voters cast their ballots electronically, either through specialized kiosks, the internet, or other digital platforms.[28] It promises to make voting more accessible, speed up vote counting, and reduce logistical challenges. However, its adoption requires meticulous planning and policy considerations in the socio-political and legal context of Ghana. Addressing issues of technological readiness, legal frameworks, stakeholder involvement, physically challenged and illiterate inclusion, and public trust in the transition toward e-voting in Ghana is crucial. No one should be left behind in the e voting process.

Failed and Successful E-voting Case Studies from Around the World

[26] Matsuura K, 'Cyberspace, Democracy and Development: A Contribution to the Open Democracy Online Debate' (2003) https://www.opendemocracy.net accessed Friday 17th January, 2025
[27] Kumar S, Walia E and others, 'Analysis of Electronic Voting System in Various Countries' (2011) International Journal on Computer Science and Engineering <https://www.researchgate.net/profile/Ekta-Walia-3/publication/267235287> accessed [Friday, 17th January. 2025].
[28] ibid

All over the world, countries are adopting e-voting mechanisms to enhance the efficiency of elections, increase voter participation, and tighten voting processes, thereby increasing election integrity.[29] Some examples of such countries include Brazil, India, Belgium, Australia, Italy, and Argentina. Brazil adopted the use of electronic voting in 1996 and by 2000, had deployed over 400,00 kiosk-style machines, becoming the first country to have elections completely by an electronic voting system. [30]Currently, Brazil relies solely on e-voting as their main means of voting[31]. To maintain the integrity of the elections, The Brazilian Superior Electoral Court (TSE) hosts an event called Public Safety Test (PST) where voters attend lectures about the voting process and security measures that have been put in place.[32] Notwithstanding, there remain concerns about the reliability of the voting system. Concerns have been raised about the fact that the system does not produce a receipt for the voter[33], violations of the secrecy of votes, and voter identification, some of which has been addressed. Notwithstanding, Brazil has not recorded any cases of election fraud since its adoption of the e-voting system. In India, it has been found that the use of an e-voting system has "eliminated the occurrence of invalid votes during elections" and reduced time taken to tally votes.[34] Despite its convenience and promise of a more efficient election, e-voting is not without flaws and must be adopted with caution.

Ghana's Electoral Process

To design an effective e-voting system for Ghana, it is important to assess the country's current electoral process. Ghana's election process begins with voter registration, where eligible citizens (aged 18+, nationals, and residents) are enrolled into a provisional voter register using scannable forms, unique voter numbers, and indelible ink to prevent double registration. The provisional register is exhibited for public verification to ensure accuracy. On voting day, registered voters present their voter ID, receive a ballot, and cast their vote in a private booth. Voters' fingers are marked with indelible ink to prevent double voting. Ballots are manually counted, with results collated from polling stations to the national level. The Electoral Commission (EC) then publishes the results.[35]

---

[29]A D Kelly, 'Secure Oracle 91AS Gets Their E-Vote' (2003) Oracle Magazine (January-February) 45-50.
[30] G Lin and N Espinoza, 'Electronic Voting: A Survey of the Advantages and Disadvantages' (Stanford University, 2007) https://cs.stanford.edu/people/eroberts/cs201/projects/2006-07/electronic-voting/index.html accessed 17 January 2025.
[31] ibid
[32] Public Safety Tests (PSTs)' (Tribunal Superior Eleitoral) https://international.tse.jus.br/en/electronic-ballot-box/public-safety-tests-psts accessed 17 January 2025.
[33]J Gragnani and J Horton, 'Brazil Election: Do Voting Machines Lead to Fraud?' (BBC News, 3 October 2022) https://www.bbc.com/news/63061930 accessed 18 January 2025.
[34] G O Ofori-Dwumfuo and E Paatey, 'The Design of an Electronic Voting System' (2011) 3(2) Research Journal of Information Technology 91.
[35] ibid

Although Ghana has been praised for its peaceful elections, issues such as invalid votes, lengthy voting processes, delays in result publication, and the high cost of organizing manual elections highlight the need for more efficient and cost-effective solutions, such as adopting computerized or online voting systems.[36]

How can e-voting fill in the gaps in Ghana's current voting system?

The concept of e-voting has gained significant attention around the world as a means of increasing the efficiency, transparency, and inclusiveness of electoral processes. In Ghana, where the election process is still manual, the move toward e-voting could provide a transformative change.

An e-voting system will eliminate invalid votes through automated ballot validation and ensuring accurate vote capturing. It will significantly reduce voting time, minimizing long queues, and streamlining the process. Results can be instantly tallied, eliminating delays in publication. Additionally, e-voting reduces the high cost of elections by cutting expenses on materials like ballot papers, boxes, and indelible ink, making the process more efficient and cost-effective eventually.[37]

An efficient e-voting system must be secure, accurate, discrete, auditable, accessible, anonymous, trustworthy, and sustainable[38]. E-voting systems come in various forms including Direct-Recording Electronic (DRE) Systems, Optical Scan Voting Systems, Hybrid Systems, Internet Voting (i-Voting), Paper-Based Electronic Voting Systems[39]. The type of e-voting that will be adopted in this design will be **a Hybrid System.**

Design and Implementation Steps

The Secure National E-Voting System (SNES)

The Secure National E-Voting System (SNES) is an electronic voting platform designed to simplify and secure national elections in Ghana. SNES leverages innovative technologies to ensure **transparency**, **accuracy**, and **inclusivity** while safeguarding the integrity of the electoral process.

---

[36] ibid

[37] European Commission, 'Study on the Benefits and Drawbacks of Remote Voting Solutions to Support the Preparation of a Best Practice Guide for the Use of Digital Tools to Facilitate the Exercise of EU Citizens' Political Rights' (2019) https://commission.europa.eu/system/files/2019-11/remote_voting_main_findings.pdf accessed 17 January 2025.

[38] A Mugica, 'The Case for Election Technology' (2015) 14(1) European View 111 https://doi.org/10.1007/s12290-015-0355-5 accessed 18 January 2025.

[39] See note 13

Goals of SNES

The primary objectives of SNES are to:

1. Ensure transparent and tamper-proof elections.
2. Guarantee inclusivity and accessibility for all eligible voters, including persons with disabilities and the illiterate.
3. Prevent fraud, such as multiple voting or impersonation.
4. Facilitate quick and accurate vote counting and result transmission.
5. Build trust in the electoral process by using verifiable and immutable data.

Design Specifications

Core Components

SNES consists of the following subsystems:

Voter Registration System (VRS)

- Centralized and encrypted voter registration database.
- Biometric verification using fingerprints, facial recognition, and retina scans.
- Automatic generation of unique Voter Identification Numbers (VIN).

E-Voting Platform (EVP)

- User-friendly interface with multilingual support.
- Accessible features for visually impaired voters.
- Offline voting capabilities for areas with limited connectivity.
  Real-time turnout tracking via IoT integration.

Vote Management System (VMS)

- Blockchain technology to provide immutable vote records.
- End-to-end encryption for vote confidentiality.
- Intrusion prevention systems to block unauthorized access.
- Machine learning algorithms to detect and flag anomalies.

Election Monitoring System (EMS)

- Real-time dashboards for election officials.

- Logging mechanisms for audit trails.
- Secure channels for complaint submissions and resolution.

Data Recovery and Backup System (DRBS)

- Cloud-based and on-premises backup to ensure data resilience.

Technical Requirements

Functional Requirements

System Security

- Implement perimeter and web application firewalls to filter inbound and outbound traffic.
- File integrity monitors to detect unauthorized changes.
- Just-in-Time (JIT) access for privileged users.
- IP whitelisting to restrict system access.
- Integrate security in all software development lifecycle through Secure requirements, Secure Coding standards, Threat modelling, secure code practices, secure code review, vulnerability assessment, penetration testing, secure deployment, security patch updates etc.

Vote Transmission

- AES encryption for secure data transmission.
- Digital signatures to validate vote integrity.

Fraud Prevention

- Legislation against SIM card swapping near election dates.
- Biometric authentication for voter verification.

Infrastructure Resilience

- Distributed servers to ensure system availability.
- IoT devices to monitor operational efficiency.

Non-Functional Requirements

Usability

- Intuitive interfaces with support for local languages.
- Accessibility features for voters with disabilities.

Reliability

- System uptime guarantee of 99.99% during elections.

- Robust mechanisms for disaster recovery.

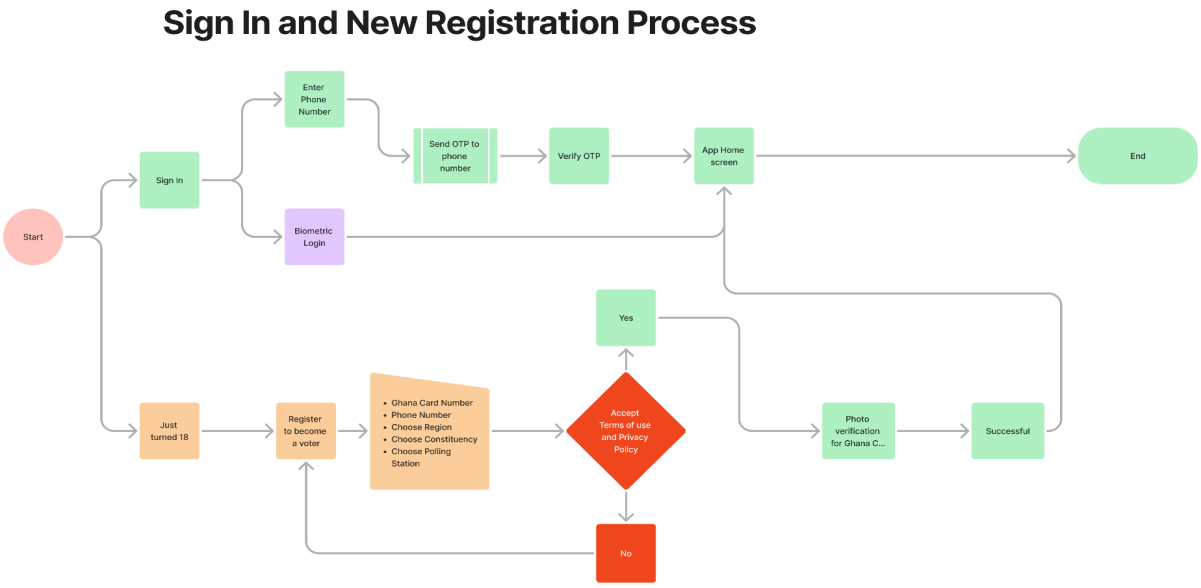
Transparency

- Blockchain-based ledger for vote storage and audits.

Implementation Steps

Pre-Election Phase

- Conduct public awareness campaigns on the SNES system.
- Train election officials and technical personnel.
- Deploy biometric voter registration kits nationwide.



Election Day

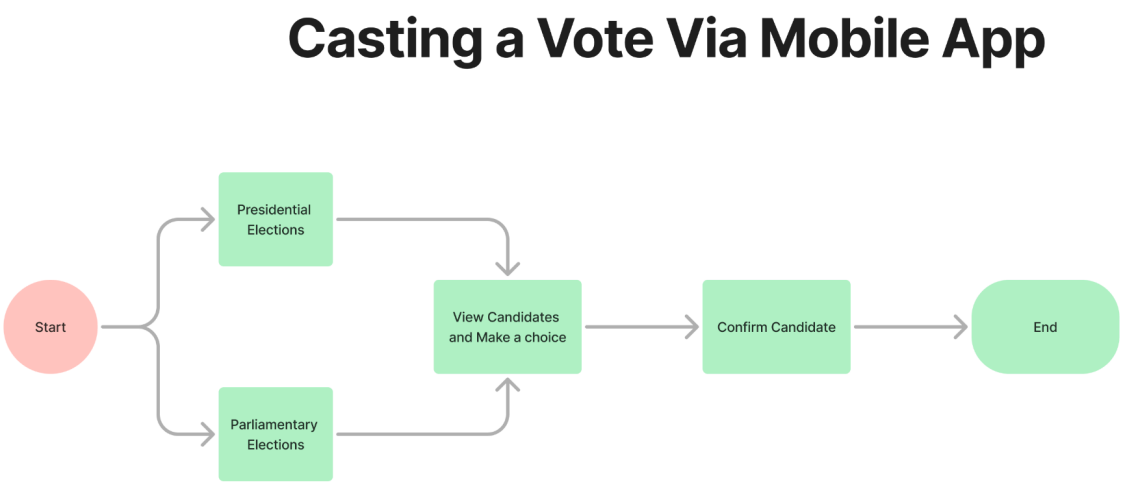
- Set up e-voting kiosks with offline functionality.
- Allow remote voting through secure portals for eligible voters.
- Provide real-time election monitoring via EMS dashboards.

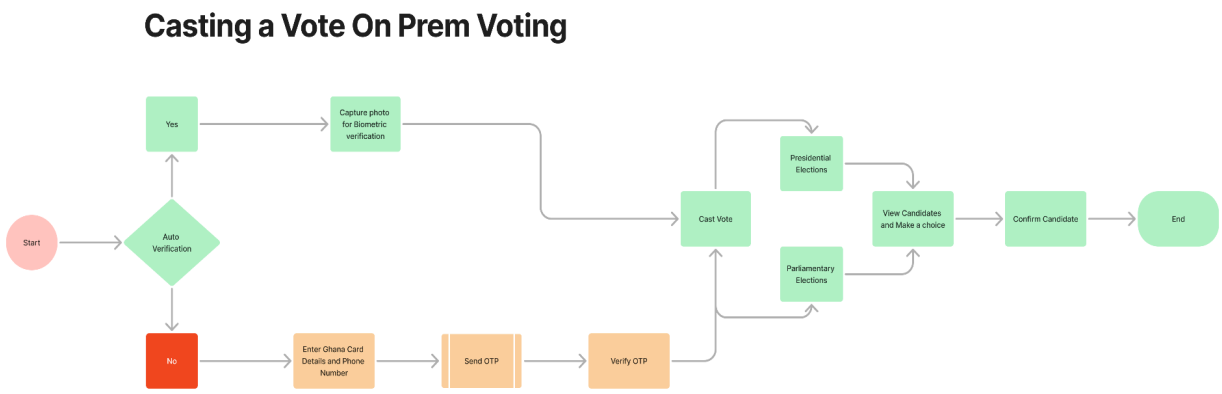
Post-Election Phase

- Automatic tallying of votes using blockchain verification.
- Publish cryptographic proofs of election results for public validation.

- Generate audit reports for independent review.

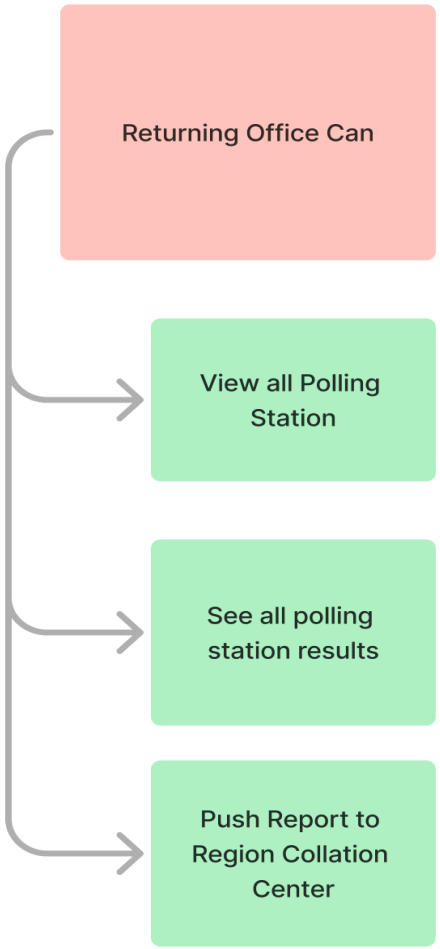
How SNES Works





1. **Voter Authentication**
    a. Voters who are unable to use the web application or internet to vote will have to be physically present at a Polling Station to access the e-voting system using a secure method such as biometric verification, facial recognition, or a One-Time Password (OTP) to cast their vote.
    b. Authentication ensures that only eligible voters can proceed.
2. **Vote Casting**
    a. Once authenticated, voters are directed to an electronic ballot interface.
    b. They select their preferred candidates and submit their vote through a secure, user-friendly interface.
3. **Encryption and Anonymization**
    a. The submitted vote is encrypted to ensure it cannot be tampered with.
    b. The system anonymizes the vote to maintain secrecy.
4. **Vote Storage**
    a. Encrypted votes are securely stored in a tamper-proof digital ledger, such as a blockchain, or on secure servers.
    b. Backup systems ensure data resilience in case of system failure.
5. **Real-Time Monitoring and Audits**
    a. The system is monitored in real-time by election officials and independent auditors.
    b. Transparent audit trails are maintained for accountability.

6. **Vote Counting and Results Declaration**



a. After the election period, the encrypted votes are decrypted and counted automatically by the system.
b. Results are verified and published to the public.

Current Voting Laws in Ghana

The legal framework for Ghana's elections is primarily anchored in the 1992 Constitution. The key provisions are as follows:

Constitutional Provisions

Article 42: Guarantees the right of every Ghanaian of 18 years and above, and of sound mind, to vote.

Article 45: Grants the Electoral Commission (EC) the mandate to conduct and supervise public elections and referenda.

Article 51: Empowers the EC to make regulations for the effective conduct of elections.[40]

Representation of the People Law, 1992 (PNDC Law 284)

Establishes substantive offenses related to elections, such as voter fraud and election malpractices, and prescribes penalties for such offenses.

Data Protection Act, 2012 (Act 843)

Regulates the protection of personal data, including voter information collected during elections.

Electronic Transactions Act, 2008 (Act 772)

Includes provisions for securing electronic systems and prescribes penalties for breaches of protected systems.

Cybersecurity Act, 2020 (Act 1038)

Provides for the protection of critical information infrastructure and creates obligations for securing electronic systems against cyber threats.

Public Elections Regulations, 2020 (C.I. 127)

This Constitutional Instrument provides the regulatory framework governing public elections in Ghana and was the law used in the most recent election in December 2024. It details processes like voter registration, voting procedures, and mechanisms for dispute resolution.

Proposed Legal Framework for E-Voting in Ghana

To implement e-voting in Ghana, the following legal framework is proposed:

Constitutional Basis:

[40] The Constitution of the Republic of Ghana, 1992, art 42 and 51

The 1992 Constitution already provides the Electoral Commission with the authority to adopt any form of voting, including electronic voting, without requiring constitutional amendments. **Articles 42, 45, and 51** will serve as the foundation for the legal framework.

Cybersecurity and Data Protection Laws:

The Cybersecurity Act, 2020 (Act 1038), can guide the development of strict security measures for the e-voting system, including encryption standards, incident response protocols, and penalties for breaches. **The Data Protection Act, 2012 (Act 843)**, should be expanded to include specific regulations for voter data protection in e-voting systems.

Policy Framework

The new CI proposed in this paper shall accommodate e-voting systems as we have, including but not limited to voter authentication, electronic ballot secrecy, and mechanisms for dispute resolution [41]. The document will cover the rights of citizens, system transparency, security measures, and post-election management. Principles such as transparency, inclusivity, accountability, and resilience must guide the policy.

New Constitutional Instrument (C.I.) for E-Voting

The EC can consider enacting a new C.I. to govern e-voting. Key provisions should include:

- Definitions for the e-voting system, transparency mechanisms (e.g., blockchain), and authentication methods.
- Regulations for system design, including encryption, verification systems (e.g., biometrics, OTP), and standards for hardware and software.
- Provisions for independent audits and periodic system updates.
- Rules for data storage, backup systems, and tamper-proof mechanisms, with oversight by the Cyber Security Authority.
- Enhanced penalties for election offenses involving digital systems under **Act 772** and **PNDC Law 284**.

Alignment with International Standards

Ghana's e-voting framework should align with international democratic principles, such as those in the Universal Declaration of Human Rights **(Article 21)** and the African Charter on Democracy, Elections,

[41] Public Elections Regulations (C.I. 127)

and Governance which encourage values of inclusiveness, transparency and fairness—benchmark requirements against which e-voting platforms must be measured.[42]

Identified Potential Flaws

1. Lack of a stable power supply system may have an impact on the system that will be implemented. To combat this, the EC must ensure that its devices will have stable backups or solar powered that will enable the system to remain active during any power outage.

2. Another potential flaw will be the penetration of the telecommunications networks themselves. Both reliance on the internet and basic telecommunications such as texting all rely on the Telcos having sufficient penetration as well as stable networks to ensure that the objective of inclusivity is met. In the alternative, the State should have its own telecommunication network as it will not be entirely safe to rely on private profit-making entities if the objective is to make sure that challenges to the declared results will fail. Private Telcos will be a loophole that can be tampered with.

Conclusion

Ghana's current voting system is inefficient and lacks security. As such, an e-voting system is a step in the right direction. The voting system must leverage technologies such as biometric authentication, blockchain, and encryption. The system must also comply with Ghana's voting laws. Although Ghana does not currently have a law on e-voting, this paper proposes a comprehensive policy direction for e-voting. This design presents a transformative solution to address the shortcomings of the current manual voting system.

Policy Recommendations

1. Ghana should launch a nationwide awareness campaign to sensitize citizens on the importance of e-voting.
2. Ghana must also consider expanding telecommunication services to the most remote parts of the country to aid in the deployment and ensure wider coverage for citizens after the implementation of an e-voting system.
3. Ghana can benchmark countries that have successfully implemented e-voting and adopt the strategies that led to their success.

[42] Universal Declaration of Human Rights, art 21

Critique

We read group five's submission on the above topic. They gave detailed submissions on their proposal with their supporting flow charts, diagrams and pictorials that gave a clear meaning and understanding to their proposal. They equally supported their proposal with all the appropriate laws including the Electoral Commission Act, 1993(Act 451). They also included countries that tried implementing e-voting but failed. They also made recommendations as well.

However, their submission on the existing voting processes in Ghana was not exhaustive enough in exposing the challenges with the existing voting system. [references]. Additionally, the group did not mention the use of Web Application Firewall to detect malicious traffic from the internet since perimeter firewalls cannot detect malicious traffic passing through the two internet ports 80 and 443. Finally, the group did not make mention of the use of File Integrity Monitoring solution to identify changes made to the source code whilst the system is live in production or voting is in process.

Section 2: Communications Law & Regulation

(Assessing governance, competition, and executive influence in Ghana's telecom sector)

2.1 Executive Control of the Telecommunications Sector: A Necessary Evil or a Barrier to Innovation and Competition?

This paper analyzes government influence in telecommunications, balancing regulation, innovation, and market competition.

Introduction

In 1881, the first telegraph line in Gold Coast was built to facilitate communication among the British. The colonial government heavily protected their telecommunications infrastructure - a legacy of centralized control that has persisted post-indepoendce.[43] Following independence, Ghana's regulatory framework for telecommunications began with NRCD 311[44] heavily emphasizing state control over infrastructure.[45] Poor service quality and limited infrastructure[46] influnced the formation of the National Communications Authority (NCA).[47] Established under Act 524 , in 1996 (repealed by Act 769 [48]), the NCA grants the president authority to appoint its Director and staff.

This paper examines the rationale for executive control, its implications for national security and its impact on competition in the telecommunications industry.

Historical Roots

The president's authority over NCA appointments [49] reflects the colonial-era centralized control, which was justified on grounds of national security. Post-independence, Act 769, [50] preserved this system, empowering the President to appoint and revoke appointments in line with Article 70 of the

[43] Peter Tobbin, 'Understanding the Ghanaian Telecom Reform: An Institutional Theory Perspective' (Centre for Multimedia and Information Technologies, Aalborg University, Denmark)
[44] Posts and Telecommunications Corporation Decree of 1975
[45] Alexander Osei-Owusu, The Analysis of the Ghana Telecom Industry, 26th European Regional Conference of the International Telecommunications Society (ITS): "What Next for European Telecommunications?", Madrid, Spain, 24-27 June 2015 https://hdl.handle.net/10419/127172 accessed 20th November 2024.
[46] ibid
[47] Godfred Frempong, Telecommunications Reforms – Ghana's Experience (IWIM - Institut für Weltwirtschaft und Internationales Management, University of Bremen 2002) Berichte aus dem Weltwirtschaftlichen Colloquium der Universität Bremen, vol 78 https://doi.org/10.26092/elib/2880 accessed 24th November, 2024.
[48] National Communications Authority Act, 2008 (Act 769), ss. 16 - 19
[49] See note 5
[50] See note 5

Constitution. The NCA's indepedence is further undermined by the minister of communications Minister of Communications also appointed by the President. This governance framework clashes with the needs of a competitive telecommunications market.

Executive Control Necessary for National Security?

Telecommunications is important for national security, hence state oversight is arugued to protect sensitive information, mitigating security risks.[51]

While this is true, a politicized regulator prioritizes executive interests over industry growth, promoting inefficiency, corruption, and stagnation. A competitive market however, promotes transparency and fosters innovation.

Impact on Industry Growth

Executive control undermines regulatory independce, leading to politically driven policies that stifle sector growth. Over-centralization breeds bureaucratic delays ill-suited to the fast-paced demands of telecommunications. A competitive regulatory environment encourages private sector participation, leading to competitiveness and innovation.

My Stance

Concentration of regulatory power within the executive branch stifles the growth of Ghana's telecommunications sector. While secure communication and surveillance is important, excessive executive involvement risks politicizing the sector. Ghana needs a more liberalized regulatory framework that balances national security with competitiveness and innovation.

Policy Recommendations

Legislative reforms must strengthen the NCA's independence.[52] Ghana can learn from the US Federal Communications Commission (FCC) which operates independently despite its presidentially appointed head or the the UK's Office of Communications (OFCOM) Chairperson who is selected through

[51] Carsten Fink, Aaditya Mattoo, and Randeep Rathindran, An Assessment of Telecommunications Reform in Developing Countries, Policy Research Working Paper 2909 (World Bank 2002)
[52] See note 4

competitive processes with paliamentary oversight. Both bodies operate independetly by reporting to the legislature.

Critique

While Kekeli's work identifies the issues of executive overreach and the need for reform, the arguement can be extended by showing how a liberalized and independent NCA will attract investors to Ghana's telecommunications sector and promote innovation.

Wilson Amfo also mentions the potential for political interference due to the President's appointment power. However, the discussion can explore real-world examples where political appointments have influenced regulatory decisions in Ghana's telecommunications sector.

2.2 A Guide to Ghana's Telecommunication Laws and Regulations - Key Considerations for Foreign Investors

This paper compiles all the key regulations and laws a foreign investor will need to know about before

LEGAL OPINION ON LEGAL REGIME FOR GHANA'S TELECOMMUNICATIONS SECTOR

Introduction

Per your instructions, you are a telecommunications company seeking to operate in Ghana. You have requested that we advise you on the relevant Ghanaian legal provisions to ensure your compliance with the relevant legal framework, protect the company's interests, and identify potential regulatory challenges. This document sets out the laws including the Constitution, Acts of Parliament, case law, regulations and other relevant provisions.

By examining the relevant laws and regulations to enable its operations inside the Ghanaian legal framework, this paper investigates the regulatory requirements for a foreign business looking to invest in or participate in the country's telecom industry. General Requirements of the law for setting up a company, Exit/Departure Regulatory Requirements, Telecommunication Industry Specific Legal Requirements, and Operational Legal Requirements in the Telecommunication Industry are the four (4) structure approach requirements in the sector that will be provided by a comb through the regulatory architecture of the laws pertinent to the telecom sector. Thus, these four (4) structured approach criteria

will serve as the foundation for the presentation, along with the rationale and applicability of these regulations in the telecommunications sector.

The Constitution

All laws in Ghana are derived from or authorized by the 1992 Constitution[53]. A foreign investor in the Ghanaian telecommunications sector must thus adhere to and establish its commercial activities in accordance with it. The 1992 Constitution also stipulates the kind of interest non-citizens i.e, "No interest in, or right over, any land in Ghana shall be created that vests in a person who is not a citizen of Ghana a freehold interest in any land in Ghana and any agreement, deed or conveyance of whatever nature to that effect is void"[54]. The maximum leasehold term that the Constitution allows foreigners is fifty (50) and hence it is important to take note of this when purchasing land in Ghana for operations.

INCORPORATION OF THE COMPANY AND RELATED MATTERS

Companies Act, 2019 (Act 992)

A foreign investor seeking to participate in Ghana's telecom sector must first of all incorporate a company in accordance with the Companies Act, 2019 (Act 992). In the case of **Attorney General vs. Balkan Energy & 2 Ors[55]**, the Supreme Court defined a foreign company as one which is wholly owned by a foreign entity or one with the control and management in foreign hands.[56]

Though there are different types of companies under this Act, it would be advisable to incorporate a private company limited by shares[57]. **The company must at all times have at least two directors[58] (one of whom must be ordinarily resident in Ghana), one company secretary[59], one shareholder, and an auditor**. The company is required to file its annual returns every year and report to the Registrar-General every change in company officers, shareholding, amendment of constitution, and address, among others.

Ghana Investment Promotion Centre Act, 2013 (Act 865)

Pursuant to incorporation, all foreign companies are by law required to register with the Ghana Investment Promotion Centre (GIPC)[60]. Act 865 governs the promotion of investments in Ghana and

[53] Article 11 of the 1992 Constitution
[54] Ibid, Article 266
[55] [2012] GHASC 35 (16 May 2012)
[56] Attorney General vs. Balkan Energy & 2 Others, unreported Civil Appeal No. J6/1/2012
[57] Section 7 of Act 992
[58] Section 171 of Act 992
[59] Section 211 of Act 929
[60] Sections 24 and 25 of Act 865

provides guidelines for foreign businesses wishing to invest in the country in terms of minimum capital requirements[61], foreign ownership restrictions[62] and local employment requirements[63]. The Act also sets out incentives for investors including tax holidays and exemptions as well as guarantees against expropriation. The company is required to have a minimum capital of USD 200,000.00 (for joint venture with a local partner) or USD 500,000 (wholly foreign owned) in cash or goods and equipment related to the business.

National Identification Authority Act, 2006 (Act 707)

This Act requires any foreign director or shareholder of the company to register with the National Identification Authority for the issuance of (non-citizen) national identity cards[64].

Taxpayers Identification Numbering System Act, 2002 (Act 632)

During incorporation the company and its directors will receive unique tax identification numbers (TIN) under Act 632 for tax registration purposes.

ADMINISTRATION, TAXATION, AND ACQUISITION OF PROPERTY

The Local Governance Act, 2016 (Act 936), Land Use and Spatial Planning Act, 2016 (Act 925)

These laws govern the issuance of permits and licences namely business operating permits, building permits including permits for the erection of telecommunication masts and towers in areas of operation of the business or company. Without them the company cannot operate its business.

Ghana Revenue Authority (Taxation) Laws

The Company after incorporation is required to meet tax obligations which are codified in the **Income Tax Act, 2015 (Act 896)**, the **Value Added Tax Act, 2013 (Act 870), Electronic Transfer Levy (Amendment) Act 2022 (Act 1089)** and others. These Acts require the payment of corporate tax, VAT on telecom services, withholding tax on certain payments, and e-levy on money transfers. The company will also be required to pay industry-specific taxes in addition to general taxes. The Class I **Communications Regulations 2003 (L.I. 1719)"** [65]levies the Communication Service Tax "on all communications service usage charged by communication service providers". The current rate under

[61] Section 28 of Act 865
[62] Section 27 of Act 865
[63] Section 34 of Act 865
[64] s. 2 of Act 707
[65] Communication Service Tax Act, 2008 Act 754 2008 1.

L.I 1719 is 5%. Interconnected services between operators were added when the L.I was upgraded. Breaking the terms of the aforementioned acts can result in fines and penalties.

Non-compliance with VAT obligations can lead to severe penalties, as illustrated in the case of **Ghana Revenue Authority v. West African Shipping Ltd. (2017).** The court ruled that the GRA had the right to impose penalties on the company for failing to register despite meeting the threshold. This judgment underscores the importance of timely VAT registration to avoid legal and financial repercussions.

Foreign Exchange Act, 2006 (Act 723)

Should the company deal in foreign exchange, it needs to to apply for a license from the Bank of Ghana under this Act[66]. The license is renewable yearly. Dealing in foreign exchange means buying and selling; receipt or payment; importation and exportation; and lending and borrowing of foreign currency. It also prohibits the pricing, advertising, ad receipt or payment for goods and services in foreign currency in Ghana.

Land Act, 2020 (Act 1030) and Lands Commission Act 2008 (Act 767)

Act 1030 seeks to "to revise, harmonise, and consolidate the laws on land to ensure sustainable land administration and management, effective and efficient land tenure"[67] hence knowing its provisions will aid the company. It is also important to be familiar with the operations of the Lands Commission[68] as the institution mandated inter alia to "register deeds and instruments that affect land throughout the country"[69].

Criminal Offences Act, 1960 (Act 29) and Criminal and Other Offences (Procedure) Act, 1960 (Act 30)

The principal laws governing the definition and sentencing of crime in Ghana are Act 29 and Act 30 although other laws prescribe offences and penalties. It is important to be aware of the provisions of these Acts including offences such as bribery and corruption, stealing, fraud, and embezzlement which could be committed by the company or its employees .

[66] Section 3 of Act 723
[67] Preamble of Act 1030
[68] A government institution established under Act 767 in accordance with Article 258 of the Constitution, 1992
[69] Section 3 of Act 767

INTELLECTUAL PROPERTY AND OTHER RIGHTS IN CYBERSPACE

Protection Against Unfair Competition Act, 2000 (Act 589)

Act 589 protects against acts or practices in the course of commercial activities that damage or are likely to damage the reputation or goodwill of another's business, mislead the public, and discredit another person's business. Act 589 equally protects registered/unregistered trademarks used in commercial activities, protects against disclosure, acquisition or use of trade secrets and activities likely to result in breach of Ghanaian law or international or regional obligations. As such a duly incorporated company in Ghana will enjoy such benefits in its business operations under Act 589.

Copyright Act, 2005 (Act 690)

The telecommunications sector in Ghana relies significantly on software, data systems, and other forms of intellectual property, making the Copyright Act essential for foreign investors. The Act explicitly protects computer programs and other creative works, ensuring that technology or software developed or imported by companies is safeguarded under Ghanaian law[70]. This provision is particularly relevant for foreign companies entering the market, as it offers legal security for proprietary technologies.

Additionally, foreign companies are required to secure appropriate licenses from the holders of the rights for any copyrighted works they intend to use, such as telecom software or databases[71]. Compliance with these requirements ensures smooth operations and prevents intellectual property disputes. A landmark case highlighting the consequences of non-compliance is **Ghana Music Rights Organization (GHAMRO) v. Ghana Broadcasting Corporation (GBC).** Here, GBC was found guilty of copyright infringement for broadcasting music on its platforms without proper licensing agreements. The High Court in Accra ordered GBC to obtain user licenses from GHAMRO within 90 days and awarded the plaintiff GHS 100,000.00 in damages for the copyright breach.

Furthermore, this Act emphasizes the public performance and use of copyrighted works, stipulating that authorized producers and performers are entitled to royalties for such usage[72]. It also warns against infringement, making it imperative for foreign companies to ensure their proprietary technologies,

[70] S. 5(1) of Act 690
[71] S. 42 of Act 690
[72] S. 37 of Act 690

software, or media comply with Ghanaian intellectual property laws. This is particularly critical in the telecommunications sector, where software and proprietary systems are integral to operations

Trade Marks Act 2004 (Act 664) amended by Trade Marks Act, 2014 (Act 876)

This Act defines trademark as "any sign or combination of signs capable of distinguishing between the goods or services of one undertaking from the goods and services of other undertakings including words such as personal names, letters, numerals and figurative elements[73]". The Act protects such marks by allowing registration which lasts for ten years and is renewable. As a telecommunications company which seeks to stand out in the industry, protecting your trade mark will save you from much economic loss.

EMPLOYEES AND LABOUR LAWS

Labour Act, 2003 (Act 651), Workmen Compensation Act, 1987 (PNDCL 187). National Pensions Act, 2008 (Act 766)

These laws govern employer-employee relations in Ghana and a foreign investor must acquaint itself with the same.

Act 651 among other things, requires the provision of satisfactory, safe and healthy conditions for employees, the right to form form unions[74] if they wish, at least fifteen days of paid leave[75], and maternity leave of at least twelve weeks of maternity leave for women[76].

The **Workmen Compensation Act, 1987**[77] allows employees who sustain injuries arising out of and in the course of work to receive payment. The **National Pensions Act, 2008**[78] mandates employers to register with the Social Security & National Insurance Trust (SSNIT) which receives pension contribution from employers on behalf of employees. Failure by an employer to pay the pension attracts sanctions including penalties and fines.

Immigration Act, 2000 (Act 573)

[73] Section 1 of Act 664
[74] Section 14 of Act 651
[75] Section 20 of Act 651
[76] Section 57 of Act 651
[77] PNDL 187
[78] National Pensions Act, 2008 (Act 766) *amended by the* National Pensions Amendment Act, 2014 (Act 883)

To bring expatriates into Ghana for work, the Company must be conversant with this Act since it provides for the "admission, residence, employment and removal of foreign nationals in the country"[79].

TELECOMMUNICATION INDUSTRY SPECIFIC LAWS

The National Communications Authority Act, 2008 (Act 769)

Act 769 is the regulatory backbone of the telecommunications sector. It establishes the National Communications Authority as the primary regulator for Ghana's telecommunications sector. It mandates the NCA to issue licenses, allocate frequencies, and ensure fair competition among telecom operators. It further provides the legal framework for regulating communication services, including mobile networks, Internet Service Providers (ISPs), and broadcasting. Act 769 is designed to ensure the orderly development of Ghana's telecommunications sector by promoting fair competition, protecting consumer rights, and maintaining industry standards.

All companies must also acquire licenses before commencing operations[80] and obtain the proper authorization for spectrum allocation[81]. The Authority is also responsible for ensuring compliance and monitoring of industry players and enforces penalties for violations. Your company as a telecommunication sector player is further required to meet equipment certification standards[82] under the Act.

Note that if the NCA deems you to be a significant market player, it has the right to take any action it deems appropriate in dealing with the situation as happened with Scancom PLC in the case of Republic v. NCA Ex Parte Scancom PLC[83].

Data Protection Act, 2012 (Act 843)

This Act regulates the way personal information is processed in Ghana. It mandates data processors and controllers to apply for a licence from the Data Protection Authority (the Regulator) which must be renewed every two years. Processing personal data is required to be done only when necessary and with the consent of the data subject. It must be done in a way that is lawful, reasonable, and does not

[79] Preamble to the Act
[80] S. 3(c) of Act 769
[81] S. 3(j)
[82] Section s(n)
[83] Unreported case.Suit No, CM/MISC/0844/2020

infringe on the privacy rights of the data subjects. Consent of data subjects must also be sought prior to processing and should there be an objection, data processing must stop[84].

Data privacy concerns are taken seriously in Ghana, as envisaged by the case of **Francis Kwarteng Arthur v. Ghana Telecom Ltd. and 4 Others[85]** where the High Court held that the Emergency Communications System Instrument 2020 (E1 63) which directed network operators to provide customer data including called numbers and mobile money merchant codes was unconstitutional and a violation of customer privacy.

Act 843 must therefore be taken seriously in processing customer data.

Cyber Security Act, 2020 (Act 1038)

Act 1038 was passed to promote and regulate cybersecurity activities in Ghana[86]. It is relevant to your company as the telecommunication services are often used to perpetrate cybercrimes and an awareness of the relevant provisions will help to curb it. In policing the cybersecurity space, one of the laws the Cybersecurity Authority will rely upon is the provisions of the Electronic Transactions Act, 2008, (Act 772)[87] which provides that any existing offence will be considered a cyber crime once a computing system is used to commit the crime[88].

EXIT/DEPARTURE REQUIREMENTS

Corporate Restructuring and Insolvency Act, 2000 (Act 1015)

In order to safeguard the interests of creditors, employees, and shareholders, this law controls insolvency, bankruptcy, and restructuring. It also seeks to guarantee a secure transition for private enterprises. Additionally, it permits companies to go into administration or reorganize instead of being restricted to formal liquidation.

Electronic Communications Act, 2008 (Act 775)

[84] section 20
[85] [2023] GHACA 72 (16 February 2023)
[86] Preamble to Act 1038
[87] Section 1, *supra*
[88] Section 123 of Act 772.

Since the NCA regulates the telecom sector and grants licenses to operators, the organization has the authority to cancel or suspend licenses for specific telecom operations when the operator disregards the terms and conditions for obtaining those licenses. Accordingly, section 13 (1) of the Electronics Communications Act states among others that;

"The Authority may suspend or revoke a licence or a frequency authorisation where

(a) the licence or the authorisation holder has failed to comply materially with any of the provisions of this Act, Regulations or the terms and conditions of its licence or frequency authorisation

(b) the licensee or the authorisation holder has failed to comply materially with a lawful direction of the Authority,

(c) the licensee or the authorisation holder is in default of payment of a fee or other money, charged or imposed in furtherance of this Act, the National Communications Authority Act, 2008 (Act 769) or Regulations

(d) the licensee ceases to (i) operate the public communications network, (ii) provide the public electronic communications service, or (iii) use the frequency band".

Similarly, when a company which is registered as a legal entity and operating in the telecom industry is wound up in accordance with Section 274 of Act 992, such company ceases to exist and will accordingly not carry out the business of its operation.

Accordingly, when a telecom company's license is withdrawn or the company is wound up or liquidated, all of its operations, including its involvement in the telecom sector, stop, and the company ceases to exist as such.

CRITIQUE

Group 11 has accurately given a comprehensive overview of the telecommunication sector in Ghana. They have also given a general regulatory framework and specific regulatory framework for an investor who wants to invest in the telecommunications sector in Ghana.

The cases listed (10 in all) gives a comprehensive overview of the types of issues likely to be faced by an investor.

Our major critique is that even though group 11 gives a comprehensive list of the acts and case laws and briefs the cases, they do not justify why they selected the cases and how the cases would impact the potential investor.

Section 3: Internet Governance

(Assessing governances of internet usage)

3.1. Deliberate Ambiguity or Not?: Assessing the Governing Structure and Dispute Resolution Mechanisms of ICANN

This paper explores ICANN's governance and dispute resolution frameworks and critically assess its effectiveness and fairness.

Introduction

The Internet Corporation for Assigned Names and Numbers (ICANN) manages the Domain Name System (DNS)[89], which identifies Internet Protocol (IP) addresses. The Governmental Advisory Committee (GAC), an ICANN advisory board, represents governments and advises on public policy, particularly national laws and international agreements[90]. This paper assesses ICANN's decision-making and conflict resolution procedure, focusing on the DCA v ICANN[91] case.

DCA vs ICANN

The DCA v ICANN[92] dispute involved the .africa TLD, contested by DotConnectAfrica (DCA) and ZA Central Registry (ZA). ICANN awarded .africa to ZA after disqualifying DCA, following GAC's unexplained objection, **described by Dryden as "creative ambiguity" to avoid conflict**. DCA alleged irregularities, appealed to ICANN's Independent Review Panel, and gained procedural advantages, but the panel only recommended reconsidering DCA's application. ICANN upheld ZA's award, and DCA's subsequent lawsuit was dismissed under judicial estoppel.

ICANN Modus Operandi & Dryden's Statement

Dryden's "creative ambiguity" connotes the deliberate use of vagueness to avoid conflict and leave terms open to interpretation. This does not fully respresnt ICANN's bylaws, which emphasize **transparency**, **accountability**, and **clear**, **documented** decision-making.[93] ICANN's bottom-up,

[89] ICANN, 'What Does ICANN Do?' (ICANN, 25 February 2012) https://www.icann.org/resources/pages/what-2012-02-25-en accessed 3 January 2025

[90] GAC ICANN, 'Governmental Advisory Committee' (ICANN) https://gac.icann.org/ accessed 3 January 2025

[91] DotConnectAfrica Trust v Internet Corporation for Assigned Names and Numbers (American Arbitration Association International Centre for Dispute Resolution, 2013).

[92] ibid

[93] ICANN Bylaws (as amended, 28 July 2022) art 3.1 https://www.icann.org/resources/pages/governance/bylaws-en accessed 3 January 2025.

multistakeholder model relies on consensus to ensure informed stakeholder participation[94]. Additionally, ICANN's core values[95] require decisions to follow documented policies applied consistently, neutrally, and fairly, **further invalidating Dryden's statement**. Thus, soft laws and consensus are employed with the above principles.

My Opinion

ICANN's bylaws are designed to minimize ambiguity, making the philosophy of "creative ambiguity" inconsistent with its operational frame work.

Advice for AU Commission

The African Union Commission's (AUC) withdrawal of support for DCA and endorsement of ZA lacked transparency, appearing politically motivated. A clearer, objective process with published guidelines would have provided better justification for the decision.

Internet governance in:

AFRICA

African Union

- Provides continent-wide policies and strategies for internet governance.[96]

Africa Internet Governance Forum

- Facilitates discussions on policies of the internet [97]

African Network Information Centre

- Manages and allocates IP addresses and internet resources.[98]

African Telecommunications Union

- Develops strategies for improving internet and telecommunication infrastructure.[99]

[94] See note 6 s 1.2(a)(iv)
[95] See note 6 s 1.21.2(a)(v)
[96]African Union, https://au.int/ accessed 3 January 2025.
[97]African IGF, https://igf.africa/ accessed 3 January 2025.
[98]AFRINIC, https://afrinic.net/about accessed 3 January 2025.
[99] African Telecommunications Union, https://atuuat.africa/about/ accessed 3 January 2025.

African Forum of Computer Emergency Response Teams

- Promotes internet health[100]

GHANA

National Communications Authority

- Regulates internet services, telecommunication licensing, and spectrum management.[101]

Ministry of Communications and Digitalisation

- Oversees digital transformation initiatives.[102]

Ghana Internet Governance Forum

- Promotes awareness of Internet governance issues.[103]

Internet Society – Ghana Chapter

- Facilitates discussions on key internet governance issues.[104]

Cyber Security Authority

- Oversees the country's cybersecurity framework.[105]

Critique

My colleague Osiarfo rightly points out that ICANN employs creative ambiguity to balance stakeholder interests. While this promotes flexibility, it often results in conflicts, as seen in DCA v ICANN. The case highlights how ambiguous policies fosters conflict. While creative ambiguity facilitates participation, it must be tempered with robust accountability measures to avoid perpetuating inequities, particularly for weaker stakeholders like DotConnect.

[100] AfricaCERT, 'About Us' https://www.africacert.org/about-us/ accessed 4 January 2025.
[101] National Communications Authority (NCA), https://nca.org.gh/ accessed 4 January 2025.
[102] Ministry of Communications (Ghana), 'Home' https://moc.gov.gh/ accessed 4 January 2025.
[103] Ghana IGF, 'Home' https://igf.org.gh/ accessed 4 January 2025.
[104]ISOC Ghana, 'Home' https://isoc.gh/ accessed 4 January 2025.
[105] Cybersecurity Agency https://www.csa.gov.gh/ accessed 4 January 2025.

Furthermore, my colleague Julian in his recommendations for AU suggested that "The AU Commission must ensure that they are well represented at the board level of ICANN and in its subcommittees," and I completely agree. Doing so will ensure that Africa's interests are effectively advocated for in global internet governance, preventing the marginalization of weaker stakeholders and promoting a more equitable multi-stakeholder model.

3.2 Cybersquatting or Legitimate Use?: Evaluating Ghana Government's Claim Over Ghana.com Under the UDRP

This paper investigates the Ghana.com domain dispute through the lens of cybersquatting laws and international domain name governance.

Introduction

The Uniform Domain-Name Dispute Resolution Policy (UDRP) was created by the Internet Corporation for Assigned Names and Numbers (ICANN) to settle matters over domain name registrations for generic top-level domains and some country-code domains.[106]

In this dispute, Ghana's government (the complainant) and Ghana.com Limited (the respondent)'s arguments are as follows:

Parties' Arguements

Ghana.com Ltd argues it has used the domain for 30 years to promote tourism, thus demonstrating legitimate interest. The company claims that the domain name has acquired distinctiveness and is synonymous with its brand. It has used the domain transparently and without intention to mislead users. It also asserts that "Ghana" lacks inherent distinctiveness under UDRP.

The government counterargues that "ghana.com" is identical to the country's name, implying an official association with the state. It claims that "Ghana" represents a national identity and should not be commercially exploited.

[106] Hornle J, 'The Uniform Domain Name Dispute Resolution Procedure: Is Too Much of a Good Thing a Bad Thing' (2008) 11 SMU Science and Technology Law Review 253 https://scholar.smu.edu/scitech/vol11/iss3/3 accessed Friday, 6th December, 2024

Analysis & Determination

In a claim of cybersquatting, the complainant must satisfy the three-tier test:[107]

a) **The domain is confusingly similar to their trademark**

The UDRP does not automatically recognize geographic names as trademarks, unless they acquired distinctiveness or trademark registration exists.[108] In the *Barcelona.com Case,*[109] The U.S. Court of Appeals ruled that a geographic name could not be a trademark unless it had acquired a secondary meaning. The court sided with the domain name registrant, as the complainant could not prove trademark rights over the geographical term. Since "Ghana" is inherently geographical and lacks acquired distinctiveness, or trademark registration, the domain is not confusingly similar to a trademark the complainant owns.

b) **They own legitimate rights in the domain**

Under UDRP[110] a respondent can demonstrate legitimate interest by using the domain for a bona fide offering of goods and services or by being commonly known by the domain. Ghana.com Ltd has been using the domain name for commercial tourism purposes for decades, establishing a clear legitimate interest. This aligns with the *Andalucia case*[111] where the panel upheld a respondent's use of a descriptive domain for bona fide commercial purpose. Ghana.com Ltd has demonstrated a legitimate interest in the domain "ghana.com," based on its long-standing use of the domain for tourism services.

c) **The domain was registered in bad faith**

Bad faith requires intent to exploit the complainant.[112] In the *Barcelona Case,* [113] the court emphasized the necessity of bad faith in deciding such disputes. Ghana.com Ltd's consistent use of the domain for tourism promotion demonstrates no deceptive intent, weakening the complainant's claim.

---

[107] Uniform Domain Name Dispute Resolution Policy (adopted 24 October 1999, last updated 21 February 2024) ICANN. Accessible from https://www.icann.org/resources/pages/policy-2024-02-21-en accessed Friday, 6th December 2024.
[108] Excelentisimo Ayuntamiento de Barcelona v Barcelona.com, Case No D2000-0505 (WIPO 2000)
[109] ibid
[110] See note 2, Paragraph 4(c)
[111] Junta de Andalucia Consejeria de Turismo, Comercio y Deporte, Turismo Andaluz, S.A v. Andalucia.Com Limited (Case No: D2006-0749| WIPO Administrative Panel Decision of 13th October 2006) Accessible from https://www.wipo.int/amc/en/domains/decisions/html/2006/d2006-0749.html Accessed 5th December 2024
[112] See note 4
[113] See note 5

The complainant failed to satisfy all three UDRP elements required to prove cybersquatting. Therefore, the request to transfer "ghana.com" to the complainant is denied.

Critique

My colleague Osiarfo's arguments made in his work are convincing. I agree that the lack of evidence for bad faith weakens the complainant's case. However, an elaboration on why Ghana's national identity claim cannot override lawful registration under the UDRP would enrich his arguments.

My colleague Kekeli also makes valid points I agree with. To strengthen his case, he can consider addressing whether a broader interpretation of "bad faith" could include the respondent's potential monopolization of a term central to Ghana's sovereign identity.

I have also read my colleague Johnny (**22258203)**'s work and I disagree with his stance that the Ghana government's case for cybersquatting is strong. In his arguments, he did not establish clear evidence of bad faith such as an intent to harm Ghana's digital presence or obstruct its sovereign interests. Additionally, an engagement with UDRP precedents like the *Barcelona Case*[114] will provide a more balanced perspective on geographic names and their treatment under the policy.

Section 4: Digital Security

(Examining Ghana's cybersecurity legal framework and how it measures up to global cyber law frameworks.)

[114] See note 3

4.1 Cyber Offences Under Ghana's Cybersecurity Act, 2020 (Act 1038) and Electronic Transactions Act, 2008 (Act 772)

This paper breaks down key cyber offenses, legal provisions, and enforcement mechanisms in Ghana's two main cyber laws.

Cybercrime refers to the use of cyberspace or electronic systems to commit crime[115]. A crime is any act punishable by death, imprisonment, or fine[116]. With Ghana's growing reliance on technology, the Cybersecurity Act, 2020 (Act 1038)[117] and the Electronic Transactions Act, 2008 (Act 772)[118] codify cyber offences to address unlawful digital activities. This paper discusses the offences created by these Acts, identifies potential gaps, and proposes solutions to enforcement and regulatory challenges.

The Acts' Interconnectedness

Before Act 1038, Act 772 was the primary law governing cyberspace in Ghana. Subsequently, Act 1038 provided a more comprehensive approach to regulating cyberspace, adding to offences not covered in Act 772 and repealing certain sections. **Section 98** of Act 1038 repeals **Section 118** and **Section 136**.

Act 772, Section 136 and **Act 1038, Section 62** both address offenses relating to **child pornography**. However, Act 1038 includes additional provisions about online exploitation and luring.

Act 772, Ss124, 125 and **Act 1038, Section 94** criminalize **unauthorized access** to and interference with electronic records, though Act 1038 specifically focuses on subscriber data and interception.

Act 772

Ss107-115 extend specific sections in Act 29 to cover traditional crimes committed through electronic means. For example, **Section 107** extends stealing to include crimes using electronic systems; **Section 108** expands appropriation to cover electronic property and intangible assets and **Section 110** extends charlatanic advertisements to online platforms, among others.

Act 772 also criminalizes false representations to obtain an electronic payment medium **(Section 119),**

[115] Cybersecurity Act 2020 (Act 1038), s 97.
[116] Criminal Offences Act 1960 (Act 29), s 1.
[117] See note 1
[118] Electronic Transactions Act 2008 (Act 772)

possessing electronic payment mediums unlawfully **(Section 120)**, the unauthorized use of another's records **(Section 122)**, actions intended to interfere with access to an information system, such as a Denial of Service (DoS) or Distributed Denial of Service (DDoS) attack **(Section 128)**, unauthorized access and misuse of computers containing sensitive information critical to national security or financial institutions **(Section 133)**, among others. **Ss124, 125, 126, 127** also provide for other cyber offences.

Act 1038

Act 1038 criminalizes the sharing of intimate images without consent (**Section 67)**; mandates service providers to install interception capabilities on their networks (**Section 76)**; prescribes a retention period for subscriber information and traffic content (**Section 77);** and empowers tthe removal of illegal content, particularly in cases related to national security or public safety.

Section 123, Act 772 & Section 95, Act 1038

Section 123 extends Act 29[119] and other laws to cyberspace, allowing traditional criminal laws to apply to cybercrimes. Consequently, it bridges the gap between Act 29 and Act 772, ensuring that all criminal provisions are adaptable to online offences. S**ection 95 of Act 1038** sets a general penalty for violations where the Act doesn't specify a punishment. Together with section 123, they address potential loopholes, leaving room for the ever-changing nature of technology.

Recommendations

Ghana's cybersecurity law is evolving and doesn't address emerging cyber offences like cyberterrorism. It also lacks clear frameworks for international cooperation on cybercrime, as recommended by the **Malabo**[120] and **Budapest**[121] Conventions. Additionally, Ghana should consider criminalizing offences such as the dissemination of racist and xenophobic material, cyberbullying, and AI-powered cyberattacks.

Critique

In her essay, my colleague Pacey asserts that "The Cybersecurity Act of 2020 (Act 1038) amends the Electronic Transactions Act of 2008 (Act 772) to create a stronger cybersecurity framework for

[119] See note 2
[120] Convention on Cybercrime (Budapest, 23 November 2001).
[121] African Union Convention on Cyber Security and Personal Data Protection (2014).

Ghana." I disagree with this claim. While the Cybersecurity Act introduces additional cyber offences to complement those in the Electronic Transactions Act, it does not amend the latter. Instead, Section 98 of Act 1038 specifically repeals Section 118 of Act 772, rather than amending the entire Act. My colleague should have made this distinction clearer.

I read my colleague Baffour's work and believe he should have elaborated more on the provisions of Act 123 and addressed the overlaps between the provisions of both Acts. Additionally, he did not provide recommendations on how Ghana's cybersecurity laws could be strengthened nor discuss gaps in our laws compared to international conventions like the Budapest Convention.

4.2 Comparative Analysis: Ghana's Cybersecurity Laws & International Cybercrime Conventions

(Examining and juxtaposing the Budapest Convention, Malabo Convention, UN Cybercrime Convention, and Ghana's cybersecurity laws.)

1. Introduction

Ghana's Cybersecurity Act, 2020 (Act 1038) defines cybercrime as "the use of cyberspace, information technology or electronic facilities to commit a crime"[122]. The pervasiveness of information technology - social media, e-commerce, remote work, and artificial intelligence - has increased the rate of cybercrime worldwide, creating a global need for enhanced cybersecurity. Ghana's position on cybercrime is shown by the enactment of laws such as the Cybersecurity Act, Electronic Transactions Act[123] and by being a party to international conventions. It was also a member of the GLACY+ project[124]. By being a party to these conventions, it binds itself to implementing them locally. It is our position however that Ghana's legal framework remains inadequate for addressing emerging cyber threats.

This paper assesses Ghana's cybersecurity legal framework which includes the Budapest Convention and its protocols, the Malabo Convention[125], the United Nations Convention against Cybercrime[126], and

[122]Cybersecurity Act 2020 (Act 1038), s 97
[123] Electronic Transactions Act 2008 (Act 772)
[124] Global Action on Cybercrime Extended, Council of Europe <https://www.coe.int/en/web/cybercrime/glacyplus>
[125] African Union Convention on Cybersecurity and Personal Data Protection
[126]United Nations General Assembly, 'United Nations Convention against Cybercrime' (24 December 2024) UNGA Res 79/243.

Ghana's Cybersecurity Act[127] and evaluates how effectively Ghana's local laws combat cyber offenses that affect national and individual interests.

2. INTERNATIONAL AND REGIONAL CYBERCRIME FRAMEWORKS

2.1 Budapest Convention

The Budapest Convention on Cybercrime[128], drafted by the Council of Europe in 2001, is the first international treaty that addresses cybercrime. It is a model for the development of cybercrime legal frameworks.

Its provisions cover both substantive criminal law and procedural law. Its objective is to harmonize member states' laws for effective international cooperation in combating cybercrime, while covering both substantive and procedural law. Its **First Additional Protocol** came into force in 2003, targeting child pornography. It criminalized the production, possession, and dissemination of child pornography physically and online. The protocol also established measures to prevent the use of the internet for trafficking, sexual exploitation, and related offenses.

In 2021, The **Second Additional Protocol** was adopted, focusing on electronic evidence and cross-border access to data. It addressed the challenges of cross-border data flow, cloud storage, encryption, and access to electronic evidence across jurisdictions.

Further, **Chapter Two of the Convention** mandates countries to criminalize cyber offenses like system and data interference, and child exploitation when committed intentionally without authorization**.**

The convention encourages parties to extend criminal liability to those who aid cybercrimes, including corporate entities.

The convention further mandates signatories to empower authorities to search and seize stored data when there are reasonable grounds to suspect illegal use.

2.2 African Union Malabo Convention

This convention strengthens regional cybersecurity, facilitates digital integration, protects personal data, and promotes cross-border cooperation against cybercrime. It also criminalizes offenses like hacking, fraud, identity theft, and illegal content distribution, advocating for a regional cybersecurity center.

2.3 United Nations Convention against Cybercrime

[127]See note 1

[128] Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185.

The convention, initially drafted in 2023 was adopted by the UN General Assembly on December 24, 2024, although negotiations are still ongoing to refine its provisions. It promotes international cooperation, standardizes legal frameworks and definitions, promotes cyber crime prevention and addresses emerging threats like AI-driven cyberattacks and cross-border data sharing. Despite the pros, human right safeguards remain weak, relying on domestic laws and loose proportionality principles, leaving privacy and free expression vulnerable.[129]

2.4 Cybersecurity Act, 2020 (Act 1038)

Passed in 2020, Act 1038 establishes Ghana's Cyber Security Authority and regulates cybersecurity activities. By recognising that cybercrime affects both individuals and the state, it creates national and sectoral computer emergency response teams and proscribes crimes that are national and individual in nature. It designates computer systems deemed important to national security or public safety as critical information infrastructure[130]. It thus regulates ownership and cybersecurity incidents regulating such information infrastructure to protect banking, health and other critical national interests[131]. For individual protection, it mostly targets sexual offenses and a few cybercrimes. **Sections 62–65** address child protection in cyberspace, outlawing child pornography, online solicitation, cyberstalking, and sexual extortion, with penalties ranging from fines to 25 years in prison. Section 67 also prohibits non-consensual sharing of intimate images. Offenders face a fine of 2,500–5,000 penalty units, imprisonment of 5–10 years, or both upon summary conviction. **Section 63** criminalizes using digital services to solicit, lure, or groom a child for unlawful sexual conduct or its depiction. It also prohibits aiding, abetting, and cyberstalking a child. **Section 66** also criminalizes sexual extortion, including threats to share explicit images to harass, coerce, extort, or force unwanted sexual activity. Offenders face 10 to 25 years' imprisonment upon summary conviction. **Section 67** prohibits the non-consensual sharing of intimate images. In line with the Budapest Convention, **Act 1038** allows an investigative officer to seek a high court production order for subscriber information. Under Section 69, the officer must show reasonable grounds that the information is necessary for a criminal investigation.

3. Strengths of Act 1038

[129] Karine Bannelier and Eugenia Lostri, 'Is Anyone Happy With the UN Cybercrime Convention?' (Lawfare, 2 December 2024) <https://www.lawfaremedia.org/article/is-anyone-happy-with-the-un-cybercrime-convention#:~:text=However%2C%20the%20cybercrime%20convention%20has,fundamental%20freedoms%2C%20and%20facilitate%20censorship > accessed 8th February, 2025..
[130] Section 35 of Act 1038
[131] Sections 36(4), 39, 40, and 47 of Act 1038

Act 1038 is commendable in protecting both national and individual interests. By designating certain computer systems as critical information infrastructure, it protects banking, security, health and other information whose breach can bring the nation to its knees.

By creating the Cyber Security Agency and national and sectoral emergency response teams, it centralizes the fight against cybercrime and provides individuals and organisations with resources to fight cybercrime. It also empowers the investigation and prosecution of cybercrime.

By creating stiff offences for child pornography and distribution of inappropriate personal images, it protects children and society's vulnerable ones.

Finally, it promotes international cooperation.

4. Shortfalls of Act 1038

One shortcoming of Act 1038 in comparison with the **Budapest convention** is that Act 1038 does not make sufficient provision for international collaboration, assistance and sharing evidence.

Ghana's Cybersecurity Act, while comprehensive within our jurisdiction, does not engage in the same level of global legal alignment as the UN Convention. It focuses on fewer offences such as child protection offences. This in a way makes its scope limiting. Ghana could potentially benefit from the guidance offered by the UN Convention in expanding its scope to include other offences for example identity theft and other measures in its fight against cybercrime.

In comparison with **Act 1038**, one shortcoming of Ghana's law is that it tends to focus more on a national approach when it comes to dealing with cyber crimes instead of an inclusion of an African integration Approach where there's an efficient collaboration between authorities across Africa. Although the Act makes provision for international cooperation under **Section 83**, it fails to give a detailed guideline to facilitate it.

A further addition to the shortfall of **Act 1038** is that while the Malabo convention emphasizes the need to protect personal data of citizens which happens to be one of the core mandates of the convention, Ghana's law is underdeveloped when it comes to providing an efficient framework required to safeguard personal data of citizens.

5. Similarities Between The Laws:

All frameworks share a common goal to fight cybercrime, emphasizing on cooperation among states or organizations and criminalizing common cyber offenses like illegal access, data interference, and

system misuse. They propose procedural measures for the investigation and prosecution of cybercrimes.

6. Differences Between The Laws:

However, they differ by:

Scope and Focus: The Budapest Convention primarily serves the European Union and other signatory states with a focus on international cooperation. The Malabo Convention targets African Union members and includes data protection. The UN Convention aims for a global standard, while Act 1038 focuses on national cybersecurity management.

Data Protection: The Malabo Convention uniquely integrates data protection significantly. The Budapest Convention, while not specifically focused on data protection, is complemented by other European conventions that cover these aspects.

Legal Provisions: The Budapest Convention is detailed in harmonizing laws for cross-border cooperation, while the Malabo Convention also addresses e-commerce and data protection. The UN is expected to be comprehensively global, whereas Ghana's Act emphasizes creating a robust national cybersecurity framework.

7. Additional Laws

While Act 1038 appears inadequate to deal with the volume of cybercrime, it is not the only weapon in Ghana's legal arsenal. Ghana has implemented other relevant laws including the following:

7.1 Electronic Transactions Act, 2008 (Act 772)

In 2008, Ghana passed the Electronic Transactions Act, 2008 (Act 772) "to provide for the regulation of electronic communications and related transactions and to provide for connected purposes". **Sections 107 to 117 of Act 772** criminalises offences whose main ingredients have already been created and defined by **Ghana's Criminal Offences Act, 1960 (Act 29)** but with modifications necessary to deal with ICT/cyber aspects. **Section 123** of Act 772 also creates a general provision which makes a person who uses any electronic medium to commit an offence which has been created by another law to be liable under that law. It addresses some of the requirements of the Budapest convention for parties to adopt legislation which extend criminal liability to persons who aid and abet cybercrimes. When combined with Act 1038, Ghana appears to have made significant headway towards meeting the goals for the Budapest Convention, the Malabo Convention and the United Nations Convention against cybercrime. However, with the increasing advancement in IT/Cyber

technologies, especially AI technologies, it is imperative that **Act 772** be reviewed and updated to keep up with the modern advancement in cyber technologies.

7.2 Data Protection Act.

Data Protection Act, 2012 (Act 843)

This Act regulates the way personal information is processed in Ghana. It mandates data processors and controllers to apply for a licence from the Data Protection Authority (the Regulator) which must be renewed every two years. It requires that personal data is only processed when necessary, with the consent of the data subject and must be done lawfully, reasonably, and not infringe on data subjects' privacy rights. Should data subjects object, data processing must stop[132].

Ghana's **Electronic Communications Act** and **Cyber Security Act** provide positive legislative headway in light of combating cybercrime. Ghana's primary national laws on cybersecurity such as the Data Protection Act, the Electronic Communications Act, and the Cybersecurity Act, compared to international standards like the Malabo Convention, the Budapest Convention, and the UN Convention on Cybercrime, show gaps:

In terms of scope, national laws are often less comprehensive, lacking the broader coverage of cybercrime activities found in international conventions with international cooperation**.** Ghana's laws have more limited provisions for international collaboration, which is extensively covered in international frameworks. While in effect**,** inconsistencies in enforcement, especially for cross-border issues, are more pronounced in Ghana's legislation compared to the robust mechanisms in international conventions.

7.3 Position of Ghanaian Courts on Cybercrime

In the case of **Ecobank Nigeria Plc v. Hiss Hands Housing Agency**[133], where money was moved electronically from plaintiff's account to 1st Defendant's bank account, the Supreme Court held that while the plaintiff could not prove how the theft occurred, it would not allow the defendant to unjustly benefit from the theft.

[132] Data Protection Act 2012, s 20.
[133] [2017-2018] 1 SCGLR 355

The High Court in the case of **Francis Kwarteng Arthur v. Ghana Telecom Ltd. and 4 Others**[134] where the High Court held that the Emergency Communications System Instrument 2020 (E1 63) which directed network operators to provide customer data including called numbers and mobile money merchant codes was unconstitutional and a violation of customer privacy.

8. Recommendations

Ghana's Cybersecurity Act is a step in the right direction. However, to align the legislation with international standards, we recommend:

a. A unified law to introduce a comprehensive cybercrime law that covers a broad spectrum of cyber offenses, enhancing Cooperation to Strengthen international cooperation mechanisms for effective cross-border crime management.
b. Robust enforcement to implement strong enforcement and compliance monitoring to uphold international standards and Future-proof Legislation to ensure the law adapts to technological changes to remain effective against emerging threats.
c. Upon Ghana signing the UN Convention, a decision can be made to amend Act 1038 to better incorporate the definitions and cybercrimes therein.

CRITIQUE

We have read the work of Group one and it's obvious an extensive reading and research on the various conventions was made. The writing was satisfactory but they failed to demonstrate their understanding of the question in the introduction and so rushed into answering the question. Secondly we again realized their paper still referred to the United Nations Conventions as a draft yet the General Assembly adopted it 24th December 2024. It also appears they did not appreciate the conflict of Ghanaian laws. Furthermore, their introduction lacked a clear thesis statement outlining whether Ghana's legal framework is adequate or not, making their argument unclear.

[134] [2023] GHACA 72 (16 February 2023)

Section 5: Practical Application of IT Law Knowledge

5.1 Heads of Agreement for IT Services for Kanewu Financial Services Ltd

A legal document outlining a Heads of Agreement for IT services for a company.

Introduction

This paper contains a Heads of Agreement for a company's procurement of managed IT services. The document outlines the scope, operational provisions, fees and payment terms, client responsibilities, service provider responsibilities, terms for termination, force majeure, and other relevant provisions as listed below. The Heads of Agreement serves as a high-level framework for the proposed contract and provides a concise yet comprehensive outline from which the final, detailed agreement will be created.

MANAGED IT SUPPORT SERVICE AGREEMENT:

This Heads of Agreement ("HoA") is made this 15th day of January 2025 between **Group 4 Consulting International Limited**, a Company incorporated under the laws of Ghana with its registered office address at 23rd Street, Tse Addo, Accra in the Greater Accra Region of Ghana (hereinafter called **THE SERVICE PROVIDER)** which expression shall where the context so requires or admits include its legal representatives, successors in office and assigns, acting per its Managing Director Frank Abdulai Iddrisu on the first part,

And

Kanewu Financial Services Limited, a Company incorporated under the laws of Ghana with its registered office address at H/No 8, Ohum Street, Dzorwulu, Accra in the Greater Accra Region of Ghana (hereinafter called **THE CLIENT**) which expression shall where the context so requires or admits include its legal representatives, successors in office and assigns), acting per its Managing Director Sharon Essilfie on the second part;

WHEREAS:

i. The Client is desirous of obtaining the services of the Service Provider for managed IT support services, specifically the provision of managed IT support services ("the Service").

ii. This HoA sets out the key terms agreed upon by the Parties and will serve as the basis for the final agreement.

1. Scope of Services

The Service Provider shall deliver the following Services to the Client:

1.1. Cybersecurity Services

Endpoint Protection.

- Use of advanced threat detection tools, including SIEM (Security Information and Event Management) and AI-driven analytics.

Firewall and Network Security

- Configuration, monitoring, and management of firewalls, intrusion detection/prevention systems (IDS/IPS), and network security appliances.
- Regular reviews of firewall rules and network access controls.

1.2. Cloud Management Services

- Deployment and management of endpoint protection solutions, including antivirus, anti-malware, and EDR (Endpoint Detection and Response).
- Regular updates and patches to ensure endpoint security.

1.3. Network Operations

- Supervision, monitoring, and maintenance of Internet bandwidth from Telecommunications Network service providers.
- Management of uptime, Management of Local Area Network and Wide Area Network.

- Troubleshooting as well as the management of soft distribution, updating Switch and Router Operating systems, Network performance tuning and High availability.
- Regular vulnerability scans and penetration testing to identify weaknesses in the Client's systems.
- Prioritization and remediation of identified vulnerabilities based on risk level.

1.4. Incident Response

- Establishment of an incident response plan tailored to the Client's environment.
- Implementing a state-of-the-art Next Generation Security Operations Center (SOC) where all Client assets are centrally managed by deploying the globally accepted open-source Wazuh Security Information and Event Management solution.

1.5. System Admin

- The configuration, management, security, and optimal operations of computer systems especially in multi-user computer-based environments.
- Use of Microsoft based technologies like Domain Name System, Active Directory Infrastructure Services to manage Users, Computers, Organizational Units and Group Policy Objects.
- The provision of and Management of Microsoft's Identity and Access Management (IAM) using Microsoft’s Entra service.

1.6. Compliance Support

- Assistance in meeting relevant cybersecurity compliance requirements (e.g., GDPR, ISO 27001:2022, NIST, PCI-DSS).
- Preparation of documentation and reports for compliance audits.

1.7. Additional Services

- Provision of additional services such as end user support, procurement of IT software, digital forensics, and dark web monitoring as and when needed by Client.

2. Service Levels

The Service Provider shall meet the following service levels:

2.1. Response Times

- **Critical Incidents**: Response within 1 hour of detection.
- **High-Priority Incidents**: Response within 4 hours of detection.
- **Medium-Priority Incidents**: Response within 8 hours of detection.

2.2. Incident Resolution

- **Critical Incidents**: 95% resolved within 4 hours.
- **High-Priority Incidents**: 95% resolved within 8 hours.
- **Medium-Priority Incidents**: 95% resolved within 24 hours.

2.3. Reporting

- Monthly reports detailing activity, incidents, and remediation efforts.
- Quarterly reviews and recommendations for improvement.

3. Term

The initial term of the agreement shall be valid for an initial term of 12 months, commencing on 15th January 2025. The agreement may be renewed upon mutual consent of the parties.

4. Fees and Payment Terms

- **Fees**: The Parties agree that the Client shall pay the Service Provider a monthly fee of **GHS 50,000.00** for the services outlined in this HoA.
- **Payment Terms**: The Service Provider shall issue Invoices monthly in advance to the Client, and the Client shall be expected to make payment within 30 days of receipt of all invoices.
- **Additional Costs**: Any additional services outside the agreed scope shall be charged at the Service Provider's standard rates.

5. Responsibilities of the Parties

5.1. Client Responsibilities

- Provide necessary access to systems, networks, and data for monitoring and management.

- Designate a primary point of contact for security-related issues.
- Implement recommended security measures promptly.
- Notify the Service Provider of any changes to the IT environment that may impact the services.

5.2. Service Provider Responsibilities

- Deliver the services outlined in accordance with the agreed scope and service levels.
- Maintain confidentiality and security of the Client's data.
- Provide regular updates and reports to Client.
- Notify the Client immediately of any critical threats or breaches.
- Pay the fees at the time and manner specified herein.

6. Confidentiality

61. Both parties hereby agree to maintain the confidentiality of all information exchanged during the term of this agreement and thereafter. This will include, but shall not be limited to, technical data, business processes, and security incidents.

6.2 All personal data which is processed by either party either as a data processor or controller shall be done in accordance with the provisions of the Data Protection Act 2012 (Act 843), shall not be disclosed unless required and only on a need-to-know basis to employees. All data subjects shall be informed of the use of the data and shall give their consent to such use.

7. Intellectual Property

Each party shall retain ownership of all intellectual property rights, including but not limited to patents, trademarks, copyrights, and trade secrets, that it owned or developed prior to the commencement of this agreement.

8. Force Majeure

8.1 In the event of any acts of God, but not limited to flood, fire, earthquake, war, tempest, hurricane, government restrictions or imposition of any change in law or order or any circumstances arising or action taken beyond or outside the reasonable control of the Parties hereto preventing them or any one of them from the performance of any obligation hereunder ("Force Majeure"), then the Party affected by such Force Majeure shall immediately notify the other Party forthwith as to the nature and extent of the circumstances in question.

8.2 Where a Party is (or claims to be) affected by an event of Force Majeure, it shall take all reasonable steps to mitigate the consequences of such an event upon the performance of its obligations under this Agreement, resume performance of its obligations affected by the event of Force Majeure as soon as practicable, but not more than 15 days and use all reasonable endeavours to remedy its failure to perform; and

8.3 The Party claiming relief shall serve written notice on the other Party within two (2) days of it becoming aware of the relevant event of the Force Majeure. Such initial notice shall give sufficient details to identify the event claimed to be an event of Force Majeure and add the effect of the Force Majeure on the Party's ability to perform their obligations.

8.4 Neither Party shall be held liable for failure to perform their obligations arising from a force majeure incident provided they notify the other Party and take reasonable steps to mitigate its efforts. If the affected Party is unable to resume performance of its obligations after fifteen (15) days, the Parties shall renegotiate the terms of this HoA.

9. Dispute Resolution

The Parties agree that any disputes arising out of or related to this HoA shall be resolved through arbitration under the Alternative Dispute Resolution Act, 2010 (Act 798). The arbitration panel shall be made up of three arbitrators with each party appointing one arbitrator and their appointed arbitrators shall then appoint a third arbitrator to preside. The decision of the arbitration panel shall be final, and both parties shall share the costs equally.

10. Termination

Either party may terminate this agreement by providing 30 days written notice at the above-state address or through other means of communication such as verified e-mail or WhatsApp to be provided during performance of this HoA. In the event of termination, the Service Provider shall assist in the orderly transition of services and provide all necessary documentation and reports.

11. Amendment

This HoA may only be amended by written agreement duly executed by each of the parties.

11. Governing Law

The Parties agree that this HoA shall be binding on them and shall be governed by and construed in accordance with the laws of the Republic of Ghana.

14. Next Steps

The Parties hereby agree to:

- Finalize the formal agreement within 60 days of the execution of this HoA.
- Conduct a kick-off meeting to confirm service commencement details, including access requirements and key contacts.
- In any event, to replace this HoA with the substantive Service Agreement where such Agreement is executed before the expiration of the HoA.

IN WITNESS WHEREOF the parties hereto have caused their common seals to be hereunto affixed, the day and year first above written.

SIGNED SEALED AND DELIVERED]

by the said Frank Abdulai Iddrisu for and]

on behalf of **THE SERVICE PROVIDER**]  .....

on this 24th Day of January 2025.

in the presence of:

Witness:

Name: Kweintsiwa Owusu-Twumasi

Address: House no. 6. Abebresem Street. Accra. Ghana.

Occupation: Executive Secretary.

Signature:..  ……..

on this 24th Day of January 2025.

SIGNED SEALED AND DELIVERED]

by the said Sharon Essilfie]

for and on behalf of **THE CLIENT**]  …….

on this 24th Day of January 2025.

in the presence of:

Witness:

Name: Ewoenam Kukah

Address: No. 36 Dove Lane, Airport Residential Area. Accra.

Occupation: Director.

Signature: …  ……..

on this 24th Day of January 2025.

Critique

We have read group 6's paper on their terms of agreement to develop and implement a disaster recovery and business continuity plan for Resilient Solutions Ltd (the Company). The agreement does an excellent job of capturing most of the required terms and conditions needed for such an agreement and clearly states that the agreement is to record their mutual understanding based on the company's requirements.

The scope of work is well defined and places emphasis on providing plans for all the defined works to be done. It would have been advisable to place some estimated timeline here to give the company an idea of how long these processes and plans may take.

The consideration is given as one lump sum of GHS 250,000.00 with no idea/breakdown on how this amount was reached. This may be a risk if the company decides to reduce the scope of work. There are no criteria on how the company will be billed which may be critical for the company's cash flow decisions.

The terms and termination section adequately describes the conditions under which the contract may be terminated, however due to the vague nature of the scope of work (no estimated timelines), and unless the timeline is adequately described in the executed definitive agreement, this may cause a problem during the execution of the contract.

The confidentiality and intellectual property rights are adequately described.
The service provider indemnifies the company from liability associated with the contract however there is no provision on indemnity for the service provider in case the company breaches its responsibilities under the terms.

The arbitration clause is inadequate and unsatisfactory. Under most arbitration rules, the option to use the law courts is ousted (by agreement). The arbitration clause as described in this agreement uses the arbitration settings as a first step towards the law courts which defeats the purpose of going to arbitration and may prolong the resolution of any dispute.

References

Primary Sources

Constitution

- The 1992 Constitution of Ghana

Legislation

- Companies Act 2019 (Act 992)
- Communications Regulations 2003 (L.I. 1719)
- Copyright Act 2005 (Act 690)
- Corporate Restructuring and Insolvency Act 2000 (Act 1015)
- Criminal Offences Act 1960 (Act 29)
- Criminal Procedure Act 1960 (Act 30)
- Cyber Security Act 2020 (Act 1038)
- Data Protection Act 2012 (Act 843)
- Electronic Communications Act 2008 (Act 775)
- Electronic Transactions Act 2008 (Act 772)
- Electronic Transfer Levy (Amendment) Act 2022 (Act 1089)
- Foreign Exchange Act 2006 (Act 723)
- Ghana Investment Promotion Centre Act 2013 (Act 865)
- Income Tax Act 2015 (Act 896)

- Immigration Act 2000 (Act 573)
- Labour Act 2003 (Act 651)
- Land Act 2020 (Act 1030)
- Land Use and Spatial Planning Act 2016 (Act 925)
- Lands Commission Act 2008 (Act 767)
- National Communications Authority Act 2008 (Act 769)
- National Identification Authority Act 2006 (Act 707)
- National Pensions Act 2008 (Act 766)
- Protection Against Unfair Competition Act 2000 (Act 589)
- Taxpayers Identification Numbering System Act 2002 (Act 632)
- The Local Governance Act 2016 (Act 936)
- Trade Marks Act 2004 (Act 664) amended by Trade Marks Act 2014 (Act 876)
- Value Added Tax Act 2013 (Act 870)
- Workmen Compensation Act 1987 (PNDCL 187)

Policies and Strategies

- African Union, *The Digital Transformation Strategy for Africa (2020–2030)* (2020)
- Cybersecurity Authority, *National Cybersecurity Policy & Strategy* (2023)
- Ministry of Communications, *Ghana ICT for Accelerated Development (ICT4AD) Policy* (2003)
- Ministry of Communications, *National Broadband Policy and Implementation Strategy* (October 2012)

Cases

- *Attorney General v Balkan Energy & 2 Ors*
- *Francis Kwarteng Arthur v Ghana Telecom Ltd and 4 Others*
- *Ghana Revenue Authority v West African Shipping Ltd* (2017)
- *Republic v NCA Ex Parte Scancom PLC*
- *DotConnectAfrica Trust v Internet Corporation for Assigned Names and Numbers* (American Arbitration Association International Centre for Dispute Resolution, 2013)

International Instruments

- African Union *Convention on Cyber Security and Personal Data Protection* (2014)
- Convention on Cybercrime (Budapest, 23 November 2001)

Secondary Sources

Books and Journal Articles

- Fong MWL, 'Technology Leapfrogging for Developing Countries' in Khosrow-Pour M (ed), *Encyclopedia of Information Science and Technology* (2nd edn, IGI Global 2008) 3707
- Grigalashvili V, 'E-Government and E-Governance: Various or Multifarious Concepts' (2022) 5 *International Journal of Scientific and Management Research* 183
- Juma C and Clark N, 'Technological Catch-Up: Opportunities and Challenges for Developing Countries' (January 2002)
- Kpessa-Whyte M and Dzisah JS, *Digitalisation of Basic Services in Ghana: State of Policies in Action and Lessons for Progress*

Reports and Policy Briefs

- SAP, 'Digitization vs. Digitalization' https://www.sap.com/africa/products/erp/digitization-vs-digitalization.html accessed 21 November 2024
- United Nations Conference on Trade and Development (UNCTAD), *Trade Policies, Structural Adjustment and Economic Growth: Trade Policy Reforms in Developing Countries and the International Support Required* (1993)
- United Nations Conference on Trade and Development, 'Look Before You Leap' (Policy Brief No 71, December 2018)
- World Bank Group, 'Ghana - Digital Acceleration Project' (Washington, DC, 2022) http://documents.worldbank.org/curated/en/938111649959522167/Ghana-Digital-Acceleration-Project accessed 9 November 2024

Web Sources

- African IGF https://igf.africa/ accessed 3 January 2025
- African Union https://au.int/ accessed 3 January 2025

- GAC ICANN, ‘Governmental Advisory Committee’ (ICANN) https://gac.icann.org/ accessed 3 January 2025
- ICANN, ‘What Does ICANN Do?’ (ICANN, 25 February 2012) https://www.icann.org/resources/pages/what-2012-02-25-en accessed 3 January 2025
- ICANN Bylaws (as amended, 28 July 2022) art 3.1 https://www.icann.org/resources/pages/governance/bylaws-en accessed 3 January 2025

Semester 2

Table of Contents

Introduction & Reflectivity Statement

This portfolio reflects my semester-long journey of exploring how law and technology constantly test each other. Over ten weeks, I moved from trying to understand the science behind robotics and artificial intelligence, to thinking through how e-commerce should be regulated, and finally to grappling with the challenges of information control online. Across these papers, one theme stands out clearly: the law is always trying to catch up with technology. Sometimes too slowly, sometimes too harshly, and sometimes managing to find the right balance.

Abstract weaving the compilation

The first part of my work, Technology Outrunning Legal Imagination, shows how I started with the basics of robotics and AI. Reading Mataric's Robotics Primer and Boadu's work on machine learning was a stretch, but it reminded me that law often has to regulate things it doesn't fully understand. Later, when I wrote about ChatGPT and the panic around its rise, I saw the same pattern: law rushing to respond without always grasping the science.

The second part, *Governance Struggling with Digital Commerce*, explores how old legal rules collide with new online business models. My papers on Section 4 of Ghana's ETA, jurisdiction in cyberspace, and online contract forms all showed me how law's traditional tools like territory, signatures and other formalities don't neatly fit digital realities.

The third part, *Information Control: Openness vs. Regulation*, tested my thinking about access and accountability. I wrote about copyright exceptions, Tony Blair's strong criticism of freedom of information, and anonymity online. I found myself torn: I value openness for its democratic benefits, but I also see how it can be abused if left unchecked.

Finally, in *Technology Weaponised: Law Chasing Harm*, my work on deepfakes and child exploitation content highlighted the darker uses of technology. Here the question was whether law can ever respond fast and effectively enough without harming legitimate uses of the same tools.

What this compilation says about me

Looking back, these papers show that I don't shy away from difficult or unfamiliar material. Even when the science felt intimidating, I kept digging until I could frame the legal questions that mattered. I've also realised I like setting Ghana's situation against what other countries are doing. It helps me see both the gaps and the opportunities at home. In my writing, I tend to test ideas and ask "what if," which sometimes means I leave room for more than one answer.

Messages I wished to convey

In the ETA Section 4 paper, I wanted to highlight how legal exclusions that seem minor can end up stifling innovation. In the anonymity essay, I argued that protecting whistleblowers and activists should not mean leaving victims of online harm without justice. And in the ChatGPT paper, I pushed back against the panic and the hype. I wanted to show that our policies should be steady and measured, not fearful.

Together, these essays reveal my growing conviction that the law's role is not merely to restrain technology, but to guide it responsibly, thus preserving innovation while upholding human dignity.

Section 1: Technology Outrunning Legal Imagination

Exploring how law struggles to regulate technologies it does not fully understand, from robotics and AI fundamentals to the global panic over ChatGPT.

1.1 A Legal & Policy Reflection on Robotics and AI - Regulating the Real, Not the Imagined

Explores how legal frameworks should respond to the actual capabilities of robotics and AI, rather than public fears or science-fiction fantasies.

Introduction

The rapid evolution of robotics and artificial intelligence (AI) has driven both scientific and legal communities to navigate emerging challenges. To understand the implications of these technologies, this essay explores selected chapters from Maja J. Matarić's *The Robotics Primer* and Boadu's book, "Machine Learning in Aluminium Reduction" on AI. Specifically, this essay explores Chapters 1, 3, 7, and 18 from Matarić and Chapters 3 and 5 from Boadu, highlighting key features, areas of confusion, and potential legal relevance.

Robotics

Mataric's *The Robotics Primer* explores the history, functions, and mechanisms of robots, defining them as "an autonomous system that exists in the physical world, can sense its environment, and can act on it to achieve specific goals."[135] This definition assumes physical embodiment is a necessary condition, overlooking software-based robots like chatbots that operate autonomously in digital spaces. A more inclusive definition would account for both physical and virtual robots. Additionally, the book

[135] Maja J Matarić, *The Robotics Primer* (MIT Press 2007)

explores cybernetics in early robotics (Chapter 2), sensor types (Chapter 7), and emergent behaviours - unexpected actions not directly programmed (Chapter 18).[136]

Mataric highlights technical issues with legal implications, noting that sensors don't perceive the world directly but provide data that robots interpret (sometimes inaccurately). Sensors can "fail" due to external factors like lighting or noise without being broken. Since robots may not detect these failures, they can act on flawed data, leading to harmful outcomes rooted in technical limitations rather than intent or error. This raises important questions about liability, due diligence, product safety, and regulatory standards. If a robot makes a harmful decision due to sensor misinterpretation, should fault lie with the manufacturer, the software developer, the user, or even the policymaker who approved its deployment? Without understanding the underlying complexity of sensor uncertainty and failure, laws may assign blame too simplistically or fail to create the right accountability frameworks.

On the other hand, some technical details, like the specific workings of analogue-to-digital conversion or voltage-level differences in sensors, are of little legal relevance. While such concepts are important for engineers, they don't typically impact decision-making or legal accountability. For legal purposes, it's more important to understand the implications of sensor *failure* or *uncertainty* rather than how sensors are built.

A specific issue that poses legal challenges is emergent behaviour. The fact that the robot can do something it was not programmed to do, raises serious concerns for legal systems.[137] For instance, if harm results from an emergent behaviour not explicitly coded by the manufacturer, who should be held responsible?

Popular culture portrays robots as conscious, intuitive beings - humanoid machines capable of general intelligence, autonomy, and even emotions[138]. However, Mataric explains that robots are built as systems of interacting hardware and software modules. Their behaviour results from designed responses and, at times, emergent outcomes from interacting subsystems. As such, they don't "think" or "feel". Hence, pop-culture's portrayal distorts public understanding, leading to exaggerated expectations about what robots can do. Such hype can be dangerous. It may pressure governments into either overregulating imagined risks or underregulating actual technical limitations. To respond

[136] Matarić, *The Robotics Primer* (n 1)
[137] A Michael Froomkin, 'Issues in Robot Law and Policy' in Research Handbook on Law and Technology 408 (2023) <https://repository.law.miami.edu/fac_books/402/> accessed 10 June 2025
[138] Pallab Ghosh, 'The People Who Think AI Might Become Conscious' (BBC News, 26 May 2025) <https://www.bbc.com/news/articles/c0k3700zljjo> accessed 10 June 2025

appropriately, law and policy must be grounded in how robots' function, not how they appear in science fiction.

In Ghana, there is currently no robot-specific legal framework. Traditional tort, consumer protection, or product liability law may be stretched to address such, but they were not designed for such scenarios. Continentally, the African Union's Digital Transformation Strategy[139] makes minimal reference to robotics. Legal reform in the form of a legal framework that spells out the principles and guidelines for the use of such emerging technologies, will address some of the legal concerns identified above that may come with the development and use of robots.

Artificial Intelligence

Artificial intelligence is the study and design of computer systems that can perform tasks that normally require human thinking. These tasks include recognizing patterns, making decisions, learning from experience, understanding language, or solving problems.[140] Neural networks enable these functions by mimicking the human brain's structure to learn patterns from data, allowing AI systems to improve performance in tasks like image recognition, language understanding, and decision-making. Chapters 3 and 5 of Boadu's *Machine Learning in Aluminium Reduction* explore the architecture and training of neural networks, demonstrating their role in AI systems.[141] Chapter 3 explains how neural networks mimic the brain to learn patterns through supervised, unsupervised, and reinforcement learning. Chapter 5 focuses on training neural networks using backpropagation and a-LMS. Boadu also warns that biased or poor-quality data can compromise AI outcomes.

Backpropagation was initially difficult to understand. It's a method that helps neural networks learn from their mistakes by adjusting internal settings to improve future predictions. Legally, its layered complexity makes AI decisions hard to explain, raising transparency and accountability concerns, especially in sensitive areas like policing, hiring, or public services.[142] This is often called the black box nature of AI systems.

---

[139] The Digital Transformation Strategy for Africa (2020–2030) (African Union Infrastructure and Energy Department, 18 May 2020) <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030> accessed 10 June 2025

[140] John McCarthy, 'What is Artificial Intelligence?' (2004) <http://www-formal.stanford.edu/jmc/whatisai/whatisai.html> accessed 10 June 2025

[141] Kwaku Boadu, Machine Learning in Aluminium Reduction: Adaptive Control of Alumina Concentration in the Hall-Héroult Cell Using Neural Network (LAMBERT Academic Publishing 2022)

[142] What are the ethical concerns with neural networks? (Milvus) <https://milvus.io/ai-quick-reference/what-are-the-ethical-concerns-with-neural-networks> accessed 10 June 2025

The technical details of backpropagation (math functions and adaptive rates) were hard to understand but are of limited legal relevance. What matters for law and policy is what backpropagation does and how it affects AI outcomes, not the underlying calculations.

Neural network training raises legal concerns around bias and transparency.[143] Since models learn from data, any bias in the training set can be reinforced in outcomes.[144] Their opaque decision-making processes, especially in deep networks, complicate legal principles for accountability, explainability, and non-discrimination.[145]

Media often exaggerates AI's capabilities, focusing on sentient robots or dystopian futures.[146] In reality, today's AI is narrow and limited, yet still capable of causing real harm e.g. biased hiring tools or misidentifying facial recognition.[147] Legal and policy responses should focus on current risks, not speculative futures. Policymakers must avoid both hype and complacency by regulating based on present capabilities and risks, not speculative futures.

Conclusion and Policy Recommendations

Policymakers must focus on regulating the impacts of AI, rather than its complexity. To this end, legal frameworks should mandate: (1) transparency obligations for developers to explain decision-making processes; (2) audits to detect and mitigate data bias; and (3) accountability mechanisms that clarify responsibility when harm occurs. Regulation should be grounded in current capabilities, not future speculations.

Critique - Robotics

We have read the assignment of Group 5 on their review and understanding of Mataric's *The Robotics Primer*. Their paper shows a great understanding of her points and raises salient issues on the material and the difficulties that other disciplines might encounter in helping to refine the discipline of robotics in general. We believe that the paper did not delve sufficiently into the potential legal issues that might arise that the question deems to be trivial. We believe that legal issues that might arise in respect include workplace liability (industrial robots), product liability, data production and contract liability

[143] ibid
[144] ibid
[145] JR Kumar and others, 'Transparency in Algorithmic Decision-making: Interpretable Models for Ethical Accountability' (2023) <https://doi.org/10.1051/e3sconf/20244910204> 1 accessed 10 June 2025
[146] K Nader, P Toprac, S Scott and others, 'Public Understanding of Artificial Intelligence through Entertainment Media' (2024) 39 AI & Society 713 <https://doi.org/10.1007/s00146-022-01427-w>
[147] AI Hype Vs AI Reality: Explained! (FiveRivers Technologies, undated) <https://fiveriverstech.com/ai-hype-vs-ai-reality-explained> accessed 10 June 2025

which are issues that existing legal precedents can help to easily resolve. Areas of law such as tort, contract and labour laws are advanced enough to adjust to these.

On the other hand, issues such as robotic autonomy, human-robot emotional relational relationships, discrimination and bias in robot behaviour are some issues that could arise in the future and would call on novelty ideas to resolve. For instance, robots target at children and some adults could lead to emotional attachments and reliance that will not be healthy and lead to dependence that could be detrimental to physical and mental health.

Other than the above, we do believe that Group 5's paper has followed the instructions of the question.

Critique - Artificial Intelligence

Group 5's submission explores AI's cognitive roots, neural network design, and system failure. The paper highlights some of the key legal concerns likely to arise such as questions about tortious liabilities like negligence during their deployment. The paper also explores the issue of overfeeding in neural networks and suggests possible liability risks if known flaws are ignored. The paper does not cover potential legal conundrum such as the potential clashes between intellectual property rights and the need to hold creators accountable for injuries/damages that may arise using their creations.

Their paper also examines how certain complex mathematical elements, like α-LMS updates, are hard to grasp. We agree with this assessment. We also note the paper also takes a cursory look at the fact that public and media portrayals of AI often exaggerate its capabilities. They however do not give examples that will reinforce the fact that current AI remains specialized and limited in application and therefore the fears of their human-like intelligence are premature and distracting from real, grounded regulatory issues.

1.2 Building Ghana's AI Regulation While Avoiding Hype and Learning from Global Experience

Evaluates sensational narratives around AI alongside early regulatory responses, offering balanced policy advice for Ghana.

This essay examines reactions to ChatGPT's launch, evaluates whether these reactions were justified, and offers policy recommendations for Ghana on AI use. In 2022, OpenAI launched ChatGPT - a large

language model trained on extensive data.[148] Subsequently, media reactions have oscillated between utopian hype and apocalyptic fear. Some headlines tout AI as a cure-all[149], while others monger fears of mass unemployment[150] or sentience.[151] Pop culture reinforces these anxieties, portraying AI as something we create but cannot control. Movies like *The Terminator*, reflect what Isaac Asimov called the "Frankenstein complex" - a deep-seated fear of losing control over our own creations.[152] Blake Lemoine, Geoffrey Hinton, and Elon Musk have also echoed such fears, with Lemoine claiming Google's LaMDA was sentient in 2022,[153] and Hinton warning in 2023 that AI could threaten humanity.[154] These narratives highlight the cultural unease surrounding unregulated technology, setting the backdrop for the regulatory dilemma this essay will examine.

Early regulatory responses to ChatGPT drew out the pacing problem - the gap between rapid technological advancement and slower legal adaptation.[155] As ChatGPT reached millions overnight, regulators struggled to apply existing laws to generative AI. The EU's AI Act[156] negotiations accelerated, with 2023 amendments adding rules for foundation models and a copyright clause requiring detailed summaries of training data sources.[157] While this aims to improve transparency and protect creators' rights, it is technically complex to comply with and may impose high compliance costs that risk stifling innovation. While the requirement exists, compliance is challenging.

---

[148] Stephanie Höppner, 'ChatGPT one year on: How has it affected the way we work?' DW (30 November 2023) <https://www.dw.com/en/chatgpt-one-year-on-how-has-it-affected-the-way-we-work/a-67588407> accessed 5 July 2025
[149] Vyacheslav Polonski, 'AI has huge potential – but it won't solve all our problems' World Economic Forum (14 June 2018) <https://www.weforum.org/stories/2018/06/ai-cannot-solve-all-our-problems/> accessed 5 July 2025
[150] ChatGPT, AI and automation: impact on jobs CNN (29 March 2023) <https://edition.cnn.com/2023/03/29/tech/chatgpt-ai-automation-jobs-impact-intl-hnk> accessed 5 July 2025
[151] CNN, '"Godfather of AI" Geoffrey Hinton quits Google to warn over the tech's threat to humanity' *CNN* (3 May 2023) <https://edition.cnn.com/videos/tech/2023/05/03/geoffrey-hinton-quits-google-danger-artificial-intelligence-lead-ldn-vpx.cnn> accessed 5 July 2025
[152] Lee McCauley, 'Countering the Frankenstein Complex' in *Papers from the 2007 AAAI Spring Symposium: Multidisciplinary Collaboration for Socially Assistive Robotics* (AAAI Press 2007) <https://aaai.org/papers/0010-ss07-07-010-countering-the-frankenstein-complex/> accessed 5 July 2025
[153] Leonardo De Cosmo, 'Google Engineer Claims AI Chatbot Is Sentient: Why That Matters' *Scientific American* (3 March 2022) <https://www.scientificamerican.com/article/google-engineer-claims-ai-chatbot-is-sentient-why-that-matters/> accessed 5 July 2025
[154] CNN (n 4)
[155] Tekla Emborg, 'The EU's Pacing Problem: Why crafting and enforcing AI regulation is hard' Verfassungsblog (19 December 2023) <https://verfassungsblog.de/the-eus-pacing-problem/> accessed 5 July 2025
[156] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending various regulations and directives (Artificial Intelligence Act) [2024] OJ L 2024/1689, 12 July 2024 <http://data.europa.eu/eli/reg/2024/1689/oj> accessed 5 July 2025
[157] Katherine Sheriff, K C Halm and John D Seiver, 'European Parliament Approves Amendments to Expand the Scope of EU AI Act' *Davis Wright Tremaine Artificial Intelligence Law Advisor Blog* (16 June 2023) https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2023/06/european-union-ai-amendments-approved accessed 5 July 2025

Italy's data protection authority also temporarily banned ChatGPT in March 2023 over clear GDPR[158] violations, including unauthorized data scraping, lack of transparency, and inadequate age controls.[159] This however, was not a knee-jerk rejection of AI, but a justified enforcement of existing privacy law. The ban compelled OpenAI to add privacy disclosures and age gating before service was restored.[160] Italy showed that fundamental rights aren't waived for technology and set a precedent that AI firms aren't above the law. Rather than stifling innovation, it proved that responsible AI requires compliance with data protection standards.

In response to media AI hysteria, I say AI can automate tasks but can't replicate the full complexity of human judgment or labor. The real risks lie in human misuse and ethical failures, not AI developing intent. Systems like ChatGPT don't "think" or have agency - they predict text based on patterns and need human prompts. They can't CHOOSE to harm humanity. Additionally, AI will disrupt jobs by automating tasks but won't eliminate entire professions. Similarly, utopian panacea claims overlook AI's technical limits. It can only generalize from existing data, not imagine new futures.

Recommendations for Ghana:

1. Regulators should address clear, demonstrable risks rather than reacting to hype or speculation, ensuring enforcement is proportionate and innovation-friendly.
2. Instead of rushing new AI law, Ghana should assess and update current laws to close gaps, especially around data use and privacy.
3. Given Ghana's early stage of AI adoption, the priority should be harnessing AI for socio-economic development rather than enforcing regulation. Ghana should resist pressure to produce strategy documents just to follow trends. Instead, it should first understand how AI supports national goals, identify real challenges through use, and craft policies based on local needs.
4. Any regulatory obligations must be realistically enforceable, particularly for local developers and startups, so we don't unintentionally shut down innovation before it starts.

Critique

[158] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1
[159] Oreste Pollicino and Giovanni De Gregorio, 'ChatGPT: lessons learned from Italy's temporary ban of the AI chatbot' *The Conversation* (20 April 2023) <https://theconversation.com/chatgpt-lessons-learned-from-italys-temporary-ban-of-the-ai-chatbot-203206> accessed 5 July 2025
[160] Ibid

1. I have read **Paciencia Abena Nketia-Boye**'s work and I think it clearly explains AI's limits and the hype in media reactions. I like the balanced policy recommendations, especially the focus on data protection and innovation. But I feel it could go further on local context—Ghana's early stage of AI adoption might not need complex classification schemes yet. Also, while the EU model is a good reference, the paper could discuss how to adapt it realistically without creating burdens that stifle local innovation or exclude small players. Overall, it's strong but could be more tailored to Ghana's needs.
2. I have read **Osiarfo Acquah**'s work and I think it does a good job explaining AI as a tool without intentions and highlighting the value of adapting existing laws. But I feel it oversimplifies things a bit, since large-scale AI systems can still cause systemic harm even without intent. The critique of the EU AI Act is interesting but could go deeper, and the "human-in-the-loop" idea needs clearer detail on how it would work in practice. Overall, I'd suggest acknowledging AI's scale and proposing more specific ways to update laws and ensure real accountability.
3. I have read **Mrs Afenyi-Donkor Esq**'s work and honestly, I find it too theoretical and not grounded enough in Ghana's reality. While it's detailed, it feels like it just imports foreign frameworks without asking if they make sense here. Ghana doesn't have widespread AI development yet, so a complex national strategy and new authority seem premature. I think it needs to focus less on copying EU-style solutions and more on practical steps, like fixing existing laws and understanding our actual AI needs first.

Section 2: Governance Struggling with Digital Commerce

Examining how traditional legal concepts like jurisdiction, signatures, and exclusions, clash with the realities of borderless online trade.

2.1 Rethinking Section 4 of Ghana's ETA Through the Lens of Global Norms on E-Commerce

Critically assesses how Section 4 of Ghana's Electronic Transactions Act may stifle innovation, especially when compared with international e-commerce standards.

Introduction

Act 772[161] governs digital commerce in Ghana. However, Section 4, which excludes certain transactions from the Act's scope, raises concerns about its impact on e-commerce innovation. This essay assesses the implications of these exclusions, and compares Act 772 to international frameworks - UNCITRAL Model Law, US UETA, EU e-Commerce Directive, and the Ker-Optika decision. The essay critiques Ghana's exclusions in digital commerce, arguing against its rigidity and making recommendations to curb the same.

Section 4 Effect on Innovation

Section 4 of Ghana's ETA excludes certain transactions - such as wills, land sales, negotiable instruments, affidavits, and company registrations - from the scope of electronic recognition.[162] While this exclusion provides legal clarity and protects against digital fraud in sensitive areas, it significantly limits innovation. It delays e-government reform by restricting digital company registration and affidavit processes. It also hinders digitalisation in sectors like real estate and legal services, keeping them reliant on manual systems. Additionally, it hinders the development of smart contracts[163] and

[161]Ghana, *Electronic Transactions Act* 2008 (Act 772)
[162]Ibid, s 4.
[163]IBM, 'What are Smart Contracts?' (IBM, 2023) <https://www.ibm.com/topics/smart-contracts> accessed 14 June 2025

blockchain applications. Consequently, innovations in digital finance, tokenized property, and trustless legal agreements[164] become outright impossible within Ghana's e-commerce landscape.

Comparative Critique

Unlike Ghana's ETA, which adopts a broad exclusionary approach, international frameworks generally adopt a more open and innovation-friendly method. The UNCITRAL Model Law[165] allows exclusions but emphasises functional equivalence and encourages states to recognise electronic documents when reliability conditions are met. Its Guide cautions that overly broad exclusions may weaken the effectiveness of e-commerce laws and reduce public trust in digital systems.[166] The US UETA[167] is more progressive and excludes only wills and testamentary trusts. Similarly, the EU e-Commerce Directive[168] requires member states to ensure the legal enforceability of electronic contracts and discourages broad exclusions, limiting them to only a few sensitive transactions. In *Ker-Optika*,[169] the Court of Justice of the EU held that restrictions on online services hinder cross-border commerce and breach internal market principles. The case reinforces that national laws must not disproportionately restrict digital activity. Hungary's ban was found disproportionate and in breach of EU rules on the free movement of services.Compared to these frameworks, Ghana's Section 4 appears overly cautious, broad and inflexible, limiting the scope of e-commerce innovation. By maintaining a blanket approach to exclusions, Ghana risks slowing digital transformation and deterring investment in its e-commerce ecosystem.

Recommendations

Section 4 should be reviewed and modernised. Instead of banning entire categories, the law could allow electronic transactions if secure technologies are used. This safeguards e-commerce and allows innovation. Ghana could also adopt the US UETA[170] model by retaining exclusions only where absolutely necessary, such as wills. The government can also explore a gradual phase-in mechanism for high-risk documents. This would promote innovation without compromising trust. Although Section 4(i) gives the Minister some power to add exclusions via Gazette notice, it does not allow for removing them. Reducing exclusions to modernise the law currently requires a full parliamentary amendment.

[164]GetJara, 'The Role of Smart Contracts in Automation: How Blockchain Enables Trustless Agreements' (GetJara, 2023) <https://getjara.xyz/the-role-of-smart-contracts-in-automation-how-blockchain-enables-trustless-agreements-2/> accessed 14 June 2025
[165] UNCITRAL, *Model Law on Electronic Commerce* (adopted 16 December 1996) UN Doc A/RES/51/162, art 1
[166]UNCITRAL, *Guide to Enactment of the Model Law on Electronic Commerce* (1996) https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce accessed 14 June 2025
[167] United States, *Uniform Electronic Transactions Act* (1999), para 8
[168] European Union, *Directive 2000/31/EC* of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-Commerce Directive)
[169] *Ker-Optika bt v Állami Népegészségügyi és Tisztiorvosi Szolgálat (ANTSZ)* (Case C-108/09) EU:C:2010:725
[170] UETA 1999

Parliament should explicitly empower the Minister to both add and remove exclusions through subsidiary legislation. This would make Ghana's e-commerce laws more flexible and responsive to emerging technologies.

Conclusion

While Section 4 served a protective role in 2008, its rigidity now risks making Ghana's e-commerce regime outdated. Reforming it in line with global best practices will strengthen investor confidence, enable digital transformation, and unlock new use cases for digital commerce and governance.

Critique

I read my friend Pacey's work and this is what I think. Pacey's work is well-organised and makes a strong case against the rigidity of Section 4. I especially liked how she framed the argument around the contradiction between the Act's purpose and its exclusions. That said, I think her analysis could have been even stronger if she unpacked Section 4 a bit more. Additionally, I think there's room to push her recommendations further. She can suggest giving the Minister power to both add and remove exclusions, or propose a phased digitisation strategy based on risk. Overall though, her work was really well written!

2.2 Who Has the Right to Hear? Jurisdictional Challenges in Cross-Border Online Disputes

Analyzes the complex principles of jurisdiction in cyberspace and their implications for resolving global digital disputes.

Introduction

Jurisdiction is a court's authority to hear a dispute and defines the territory over which its power extends.[171] It ensures cases are heard in a competent forum and preserves legal order.[172] Without it, proceedings are void.[173] Cyberspace (a borderless IT network enabling timeless interaction.[174])

[171] Jurisdiction, LexisNexis Legal Glossary (LexisNexis UK) <https://www.lexisnexis.co.uk/legal/glossary/jurisdiction> accessed 13 July 2025

[172] Ryan C Williams, 'Jurisdiction as Power' (2022) 89 U Chi L Rev 1389 <https://lawreview.uchicago.edu/print-archive/jurisdiction-power> accessed 13 July 2025

[173] County Office Law, 'Why Is Jurisdiction Important For The Court System? - CountyOffice.org' (YouTube, 11 December 2024) <https://www.youtube.com/watch?v=8v11LVCaxSg> accessed 13 July 2025

[174] Cybersecurity Act, 2020 (Act 1038) (Ghana) s 97

challenges these territorial principles. This essay discusses the general principles and derogations of jurisdiction in cross-border online disputes using conventions, regulations, and case law, and considers lessons for Ghana's future framework.

General Rule

Traditionally, jurisdiction depends on the defendant's domicile. The Brussels I Regulation,[175] The Recast Brussels Regulation (Article 4),[176] and the Lugano Convention[177] contain this default. However, cyberspace complicates this. Some argue it is borderless, and that territorial boundaries should be obsolete.[178] Courts have resisted that view. In *LICRA v Yahoo*,[179] a French court asserted jurisdiction over the U.S.-based website hosting Nazi memorabilia, requiring compliance with French law despite Yahoo's U.S. base.

The Zippo Test

For online disputes, the Zippo[180] test asks: (1) Did the defendant purposefully avail themselves of the forum? (2) Do claims arise from those contacts? (3) Is it reasonable to litigate there? *World-Wide Volkswagen v Woodson* refined this by requiring contacts that make it foreseeable to be sued there.

Boschetto v Hansing[181] limits this. A single eBay sale did not create enough ties to California. Courts avoid overreach by demanding purposeful conduct toward the forum state.

Derogations

1. **Defamation**

   In *Dow Jones v Gutnick*,[182] Australian courts held that online defamation occurs where the content is accessed and causes most harm, not where it is uploaded. This raises concerns about exposing publishers to global liability. In Europe, *Shevill v Presse Alliance*[183] allowed claims where harm was suffered but only for damage there. *eDate Advertising* and *Martínez*[184] adapted

[175] Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1
[176] Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L351/1, art 4
[177] Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Lugano Convention) (signed 30 October 2007, entered into force 1 January 2010) [2009] OJ L147/5
[178]David R Johnson and David G Post, 'Law and Borders: The Rise of Law in Cyberspace' (Harvard Law School Berkman Klein Center) <https://cyber.harvard.edu/is02/readings/johnson-post.html> accessed 13 July 2025
[179] LICRA v Yahoo! Inc (Tribunal de grande instance de Paris, 22 May 2000)
[180] Zippo Manufacturing Co v Zippo Dot Com Inc 952 F Supp 1119 (WD Pa 1997)
[181] Boschetto v Hansing 539 F3d 1011 (9th Cir 2008)
[182] Dow Jones & Company Inc v Gutnick (2002) 210 CLR 575 (HCA)
[183] Case C-68/93 Shevill and Others v Presse Alliance SA [1995] ECR I-415
[184] Joined Cases C‑509/09 and C‑161/10 eDate Advertising GmbH v X and Martínez v MGN Ltd [2011] ECR I‑10269

this, letting plaintiffs sue where the publisher is established or where they have their "centre of interests," recognising online harm's borderless nature.

2. **Contracts**

   For contracts (Article 7(1))[185], jurisdiction depends on the place of performance or parties' agreement. *Pammer/Hotel Alpenhof* [186] clarified that a trader must target the consumer's state, not merely have a passive website. *Mühlleitner v Yusufi*[187] confirmed jurisdiction applies even without distance selling if the trader directed activity there. Exclusive jurisdiction clauses are also enforceable, as seen in *Ryanair v Billigfluege.de*.[188]

3. **Safe Havens**

   Legal differences create "safe havens." U.S. constitutional protections for hate speech and pornography[189] contrast with tighter controls elsewhere, while data privacy is a fundamental right in many jurisdictions outside the U.S. These gaps let actors base operations in permissive states, complicating enforcement and highlighting the need for harmonised rules.

International Instruments

The Budapest[190] and Malabo Conventions[191] provide frameworks for cooperation on cybercrime and jurisdictional overlaps. They support mutual legal assistance and cross-border claims but focus mainly on criminal law, offering little guidance for civil or commercial disputes, highlighting why Ghana needs clear domestic rules.

Implications for Ghana

Ghana lacks specific rules for cyberspace jurisdiction. A framework could use domicile-based jurisdiction as default, include derogations for defamation and consumer contracts, recognise choice-of-court clauses with safeguards for weaker parties, adopt targeting-based tests for online business, and align with conventions like Budapest and Malabo.

Conclusion

Jurisdiction in cyberspace is complex. Traditional territorial rules need adaptation. By learning from

[185] Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L351/1, art 7(1)
[186] Joined Cases C‑585/08 and C‑144/09 Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Heller [2010] ECR I‑12527
[187] Case C‑190/11 C R Mühlleitner v Ahmad Yusufi and Wadat Yusufi ECLI:EU:C:2012:542
[188] Case C‑292/10 Ryanair Ltd v Billigfluege.de GmbH (ECJ, 15 March 2012)
[189] US Constitution amend I
[190] Convention on Cybercrime (Budapest Convention) (opened for signature 23 November 2001, entered into force 1 July 2004) ETS No 185
[191] African Union, *Convention on Cyber Security and Personal Data Protection (Malabo Convention)* (adopted 27 June 2014)

conventions, regulations, and case law, Ghana can create a framework which ensures access to justice and legal certainty.

Critique

1. Paciencia Abena Nketia-Boye's work is clear and well-structured, with good use of examples like LICRA v Yahoo and Ivanov. However, it mostly describes rather than critiques. The discussion of derogations like comity could explore risks of forum shopping or under-enforcement. The targeting test section explains but doesn't assess effectiveness or fairness. Also, while recommendations are sensible, they are general. More concrete proposals would strengthen the conclusion. Finally, there's little engagement with whether expansive jurisdiction, like in Gutnick, is justified. Overall, her work has a solid coverage but limited critical evaluation.
2. Osiarfo Acquah's work is well-structured. However, it explains EU and US rules without fully analysing their suitability for Ghana's context. The recommendations are broad and don't critically assess enforcement or practical challenges Ghana might face adopting harm-based jurisdiction. It also omits other derogations like party autonomy limits or safe haven issues. Overall, it outlines jurisdictional models well but needs sharper, more critical evaluation and context-specific recommendations to fully answer the question.

2.3 How Ghanaian Law Handles Transactions Requiring Writing and Signature in Cyberspace

Examines how Ghana's legal framework validates or restricts electronic records and signatures for transactions traditionally requiring writing.

The shift from physical to digital contracting has disrupted traditional rules requiring certain transactions to be "in writing" and "signed." The Electronic Transactions Act, 2008 (Act 772), governs electronic transactions in Ghana and the validity of forms of online contracting.[192] This essay examines how Ghana interprets writing and signature in cyberspace and assesses the enforceability of online contracts.

1. Traditional Writing and Signature Requirements

Traditionally, a valid contract requires offer, acceptance, consideration, and intention to create legal

[192] Electronic Transactions Act 2008 (Ghana, Act 772)

relations.[193] However, cyber law is non-prescriptive, merely requiring consensus ad idem, regardless of form.[194] Postal contracts follow the postal rule,[195] while instantaneous communications - telephone and now email - follow the delivery rule, requiring receipt for acceptance rather than mere dispatch.[196]

The Electronic Transactions Act 2008 (Act 772) treats electronic records as "writing",[197] and accepts digital signatures-or any mutually agreed secure method-as equivalent for signature requirements.[198] It also validates notarisation or certification by electronic signature,[199] and expressly upholds contracts formed wholly or partly via electronic means.[200] This function-over-form approach mirrors the UNCITRAL Model Law (1996)[201] and UN Convention on Electronic Communications (2005),[202] both of which reject denial of legal effect solely because a transaction is electronic.

2. Email Contracts

Email is the simplest bridge between paper and cyberspace. It meets the ETA's writing requirement, and a contract forms upon receipt of acceptance.[203] Both the UK[204] and the US[205] recognise emails as valid evidence of contract formation. However, under the delivery rule, misaddressed or undelivered emails do not bind the offeror, preserving fairness.[206]

3. Shrinkwrap, Clickwrap, and Browsewrap Agreements

Shrinkwrap: A software license included with a packaged product; opening or using it constitutes acceptance.[207]

Clickwrap: A contract formed when a user actively clicks an "I agree" button after being shown the terms.[208]

---

[193]NTHC v Antwi (2009) SCGLR 117, High Court (2023)
[194] Electronic Transactions Act, s 23
[195] *Adams v Lindsell* (1818) 1 B & Ald 681
[196] *Entores Ltd v Miles Far East Corporation* [1955] 2 QB 327 (CA); *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelsgesellschaft mbH* [1983] 2 AC 34 (HL)
[197] Electronic Transactions Act, ss 5–6.
[198] Ibid, ss 10-12
[199] Ibid, s 15
[200] Ibid, s 23
[201] UNCITRAL Model Law on Electronic Commerce 1996, arts 5 and 11
[202] United Nations Convention on the Use of Electronic Communications in International Contracts (2005)
[203] Electronic Transactions Act
[204] Athena Brands Ltd v Superdrug Stores Plc [2019] EWHC 3503 (Comm)
[205] Uniform Electronic Transactions Act (UETA) 1999
[206] LJ Korbetis v Transgrain Shipping BV [2005] EWHC 1345 (QB)
[207] PrivacyTerms.io, 'Clickwrap vs Shrinkwrap vs Browsewrap' (PrivacyTerms.io, 2024) <https://privacyterms.io/terms/clickwrap-vs-shrinkwrap-vs-browsewrap/> accessed 2 August 2025
[208] Ibid

Browsewrap: A contract where continued website use counts as acceptance via hyperlink terms - without any affirmative click.[209]

Although Act 772 does not explicitly name clickwrap, browsewrap, or shrinkwrap agreements, section 23 validates any contract formed wholly or partly electronically,[210] and section 20 covers conduct via automated systems.[211] Ghana courts would likely treat shrinkwrap as implied consent if terms are visible; clickwrap as explicit assent (functionally equivalent to a signature); and browsewrap as weakest, enforceable only with clear notice. Section 13 further imposes a duty of care on those relying on digital signatures.[212] This blend of case-law and statutory backing provides a firm foundation for assessing enforceability.

4. Limitations

While Act 772 broadly enables electronic contracting, Section 4 explicitly excludes certain transactions from its scope: notably, wills, negotiable instruments, and the grant of powers of attorney, which must still comply with traditional formalities.[213]

4. Comparative and Policy Insights

The US UETA and UCITA s.202(a) adopt a minimalist approach, recognising contracts formed through any conduct, including by electronic agents, without strict offer-and-acceptance rules.[214] The EU takes a stricter stance, requiring clear consumer consent.[215] Ghana's ETA gives little guidance on passive agreements or agent-driven transactions, creating legal uncertainty.

5. Recommendations

1. Statutorily define passive-consent thresholds *e.g.* conspicuous notice plus explicit assent.
2. Explicitly recognise electronic agent contracting (UCITA § 202(a)),[216] with liability safeguards.

[209] Ibid
[210] Electronic Transactions Act, s 23
[211] Ibid, s 20
[212] Ibid, s 13
[213] Ibid, s 4
[214] Uniform Electronic Transactions Act (UETA) 1999 (US); Uniform Computer Information Transactions Act (UCITA) 2002, s 202(a)
[215] General Data Protection Regulation (EU) 2016/679, arts 4(11), 6(1)(a) and recital 32; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37, art 5(3)
[216] UCITA 2002, § 202(a)

Conclusion

Ghana's ETA modernises writing and signature rules, making email and clickwrap contracts reliable, while shrinkwrap and especially browsewrap remain uncertain. Clearer rules on passive consent and alignment with international best practices would make Ghana's digital contracting framework more predictable, innovative, and globally consistent.

Critique

I have read my colleague Osiarfo Acquah (22260709)'s work, and he does a great job of demonstrating his understanding of the question in his introductory paragraph. He also explains well how traditional contracts are handled under Ghana's Act 772, before moving on to digital signatures and then to browsewrap, shrinkwrap, and clickwrap agreements, discussing how the law treats each of them. However, Osiarfo did not contrast the Ghanaian regime with that of other jurisdictions such as the US, UK, and the European Union. Doing so would have demonstrated greater scholarship and critical analysis. In addition, he did not make any policy recommendations on how Ghana's legal regime could be improved. Aside from these points, the work was strong, and I have no further feedback.

Section 3: Information Control: Openness vs. Regulation

Reflecting on how law negotiates the fine line between promoting access and curbing abuse, from copyright and FOI to anonymity in cyberspace.

3.1. Rethinking Copyright Exceptions in Ghana for an Open Information Society

Considers whether Ghana's copyright law adequately supports knowledge sharing and proposes reforms for a more open information regime.

"**The Power of Open**" is a campaign by Creative Commons to champion the idea that *openness* - in terms of licensing, access, and participation - can promote creativity, innovation, education, and equitable knowledge distribution for the public good.[217] This essay examines Ghana's Copyright exceptions in the light of openness and argues that Ghana's copyright exceptions are limited and should be reformed to promote broader access and innovation.

[217] Creative Commons, *The Power of Open: Stories of Creators Sharing Knowledge, Art & Data Using Creative Commons* (2011) https://thepowerofopen.org/ accessed 22nd June 2025

Ghana's **Copyright Act, 2005 (Act 690)**[218], amended by Act 844, includes "permitted uses" in Sections 19–22, allowing for limited, specific uses of copyrighted material. These include uses for education, private study, reporting current events, etc. While these exceptions are necessary to balance the rights of authors with broader social interests, they are narrow in scope and do not fully support a culture of open access to knowledge. This is especially worrying when the works in question are publicly funded.[219] The dependence on traditional fair dealing criteria, limits practical use, especially in education and research contexts where flexibility is essential. For example, section 19(1)(c) permits use for education, but only when the reproduction is compatible with fair practice and limited to the extent justified by the purpose. This vague and restrictive wording makes it difficult for modern digital learning platforms to rely on the provision confidently. Ghana's copyright framework also falls short in supporting digitisation for accessibility, given Ghana's ratification of the Marrakesh Treaty,[220] which requires states to improve access for persons with visual impairments

In comparison with other international laws, Ghana's copyright law reflects the principles of fair dealing and fair practice, consistent with the Commonwealth approach and the Berne Convention, respectively. As a signatory to the Berne Convention, Ghana incorporates its requirement that certain uses, such as quotation or education, must be "compatible with fair practice" and must not unreasonably prejudice the legitimate interests of the author (Articles 10(1) and (2)).[221] In contrast, the United States follows a more flexible fair use doctrine under 17 U.S.C. § 107,[222] allowing courts to assess fairness case-by-case, beyond a closed list of purposes.

Consequently, to promote knowledge sharing, it is necessary to amend the Copyright Act to reflect the realities of the digital age and promote openness. Ghana's Copyright Act should include a "fairness" clause for non-commercial, socially beneficial uses, and broaden exceptions to cover digital learning. This would support e-learning goals and SDG 4[223]. The law should also recognise open licenses like Creative Commons and mandate their use for publicly funded content, in line with UNESCO's Open Science Recommendation[224] to promote innovation and development. Beyond legal reform, public

[218] Copyright Act 2005 (Act 690) (Ghana)
[219] James Boyle, 'Public information wants to be free' Financial Times (24 February 2005) https://www.ft.com/content/cd58c216-8663-11d9-8075-00000e2511c8 accessed 22 June 2025
[220] Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled (adopted 27 June 2013, entered into force 30 September 2016) 52 ILM 1321
[221] Berne Convention for the Protection of Literary and Artistic Works (as amended on 28 September 1979) art 10(1)–(2) https://www.wipo.int/treaties/en/ip/berne/ accessed 22 June 2025
[222] 17 USC § 107 (2012) (US)
[223] UN General Assembly, *Transforming our world: the 2030 Agenda for Sustainable Development* (21 October 2015) UN Doc A/RES/70/1, Goal 4 https://sdgs.un.org/goals/goal4 accessed 22 June 2025
[224] UNESCO, UNESCO Recommendation on Open Science (adopted 23 November 2021) https://unesdoc.unesco.org/ark:/48223/pf0000379949 accessed 22 June 2025

awareness campaigns, copyright literacy training, and institutional open access policies can be explored. Government and donor initiatives can further support Open Educational Resources[225], open data platforms, and digital archives. These efforts will build a culture of openness and inclusive access to knowledge.

In conclusion, Ghana's copyright exceptions are too limited to realise the transformative vision of the Power of Open. Legal reform, supported by policy and community action, is essential for an inclusive knowledge ecosystem.

Critique

Abena Paciencia's work is well-written, well-structured, and clearly argued. She shows a solid understanding of Ghana's copyright exceptions and connects them well to global movements like Creative Commons, Open Educational Resources, and the Marrakesh Treaty. Her comparison between Ghana's fair dealing model and the U.S. fair use approach is very insightful, and her policy recommendations are practical and relevant. The essay also balances legal critique with forward-thinking reforms, and her use of cases like Authors Guild v Google strengthens her points. Overall, her essay is strong and engaging. It reflects good legal and policy reasoning. Well done to Paciencia!

3.2 Are Freedom of Information Laws Unnecessary? Assessing Blair's Critique of the UK's Freedom of Information Act.

Reflects on the value and limitations of freedom of information laws in promoting transparency and democratic accountability.

In his memoir, former UK Prime Minister Tony Blair expressed regret for championing the Freedom of Information Act (FOIA)[226]. This essay critiques that stance by examining the law's purpose, its limits - including exemptions and privacy rights - and whether Blair's regret reflects genuine institutional harm or discomfort with accountability. While Blair's concerns are valid, they arguably undermine the democratic value of transparency.

[225] UNESCO, *Recommendation on Open Educational Resources* (adopted 25 November 2019) https://unesdoc.unesco.org/ark:/48223/pf0000370936 accessed 16 June 2025

[226] Freedom of Information Act 2000

The FOIA[227] passed in 2000 and effective from January 2005, aimed - like Ghana's RTI Act - to grant citizens access to information held by public institutions.[228] Its core purpose was to promote transparency, accountability, and fight corruption. Article 19 of the 1948 Universal Declaration of Human Rights[229] guarantee the right to seek, receive, and impart information. Ghana mirrors this in Article 21(1)(f) of its 1992 Constitution,[230] affirming every person's right to information. This right is further expanded in The Right to Information Act (RTI), 2019 (Act 989)[231] which outlines its scope and procedures.

Although RTI is constitutionally guaranteed, FOI laws are not absolute. Sections 5-16 of Act 989[232] outline exemptions for sensitive information, but Section 17 introduces a public interest override, allowing disclosure where benefits outweigh potential harm. The Act also balances this right with privacy concerns, notably in Section 16, which exempts personal information unless public interest justifies access.

FOI laws improve standards of governance by compelling public institutions to act with accountability and foresight. The real issue often lies in implementation. In Ghana, poor record-keeping,[233] untrained staff, and a culture of secrecy have undermined the RTI Act's effectiveness.[234] Blair's regret seems less about FOIA's failure and more about the discomfort transparency brings to power.[235] The 2009 UK MPs' Expenses Scandal, exposed through FOIA, revealed unethical practices and triggered public outrage.[236] Blair argued the law was weaponised by journalists and opponents rather than used democratically by citizens.[237] However, this reflects a fear of scrutiny, not a flaw in the law itself.

---

[227] Ibid
[228] *What is the Freedom of Information Act and why did Tony Blair call it stupidity?*, *Politics Teaching* (22 January 2024) https://politicsteaching.com/2024/01/22/what-is-the-freedom-of-information-act-and-why-did-tony-blair-call-it-stupidity/ accessed 17 July 2025
[229] Universal Declaration of Human Rights (adopted 10 December 1948 UNGA Res 217 A(III)) art 19
[230] Constitution of the Republic of Ghana 1992, art 21(1)(f)
[231] Right to Information Act 2019 (Ghana) (Act 989)
[232] Ibid ss 5–16
[233] *Freedom of Information Access: Key Challenges, Lessons Learned and Strategies for Effective Implementation*, World Bank (Washington, DC, 1 June 2020) <https://hdl.handle.net/10986/34155> accessed 17 July 2025
[234] *Institutional culture of silence and secrecy hindering RTI law implementation – Kojo Oppong Nkrumah*, *GhanaWeb* (14 December 2023) <https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Institutional-culture-of-silence-and-secrecy-hindering-RTI-law-implementation-ndash-Kojo-Oppong-Nkrumah-1898165> accessed 17 July 2025.
[235] Maurice Frankel, 'The roots of Blair's hostility to Freedom of Information', *openDemocracy* (7 September 2010) https://www.opendemocracy.net/en/freedom-of-information/roots-of-blairs-hostility-to-freedom-of-information/ accessed 17 July 2025
[236] *What is the Freedom of Information Act and why did Tony Blair call it stupidity?*, *Politics Teaching* (22 January 2024) <https://politicsteaching.com/2024/01/22/what-is-the-freedom-of-information-act-and-why-did-tony-blair-call-it-stupidity/> accessed 17 July 2025
[237] Frankel (n 10)

While FOI laws promote transparency and accountability, they also present challenges including the potential for misuse, administrative burdens on public bodies, and the risk of exposing sensitive information. However, balancing mechanisms within the law - such as exemptions and harm tests - help prevent such disclosures. In Ghana, any unlawful disclosure of exempt information is punishable under Sections 81, 82 Act 989.[238] Similarly, the UK's FOIA complements the Data Protection Act, ensuring transparency without undermining privacy. Requests involving personal data are assessed under both laws.

Freedom of information laws are not foolish, but essential to democratic accountability. Though they present challenges (e.g. privacy and administrative concerns), safeguards in Act 989, such as ss16, 17 address these. Blair's dismissal reflects governmental transparency's political cost, not its democratic value.

Recommendation:
Governments must promote transparency as a governance norm by proactively publishing non-sensitive institutional information online like budgets etc.

Critique

I have read my colleague Felix Aboagye (222579877)'s work and found it clear and well-structured. I particularly appreciate how he outlined the merits and demerits of freedom of information. I agree with him that access to information supports development and fosters transparency and accountability. While his reference to Tony Blair was insightful, I believe his critique of Blair's concerns could have been more critically explored, especially in questioning whether governmental discomfort is a necessary trade-off in democratic societies.

3.3 Anonymity, Accountability, and the Law in the Digital Age

Weighs the benefits of online anonymity against the harms it can enable, suggesting ways to balance privacy with responsibility.

Anonymity in cyberspace enables netizens to share information without revealing their identity, creating a legal dilemma - how should the law respond when harm results? This question sits at the

[238] Act 989 (n 6) ss 81, 82

intersection of constitutional freedoms, privacy rights, and public interest. On one hand, anonymity protects whistleblowers, journalists, and vulnerable individuals, yet also enables defamation, harassment, and privacy violations. This paper argues for preserving anonymity as a constitutional and human rights safeguard, coupled with a regulated and judicially overseen unmasking processes to balance free expression with effective remedies for victims.

Per my understanding, online disclosures can be categorised into three categories: (1) justified disclosure of true information; (2) unjustified disclosure of true information; and (3) defamation. Each demands balancing the subject's privacy rights, the discloser's freedom of expression, and the public's right to know. In Ghana, Article 21 of the 1992 Constitution[239] protects freedom of expression, including anonymous speech, consistent with Article 9 of the African Charter,[240] the US First Amendment,[241] and Article 10 of the ECHR.[242]

However, article 18 of the constitution also grants individuals the right to privacy.[243] This supports the popular saying that where one's right begins is where another's ends. Thus, where a person's right to privacy begins is where another's freedom of expression ends. In the same way, a person's right to privacy ends where public safety, national interests and the greater good of the economy begins. For example, a blog alleging a man's BDSM practices and dishonest business dealings could be defamatory if false, or a privacy violation if true but lacking public interest. If dishonest business practices genuinely defraud the public, disclosure may be justified. Such scenarios illustrate why the law must be context-sensitive rather than absolutist.

In the US, Section 230 of the Communications Decency Act shields platforms from liability for user content if they act as a publisher.[244] Ghana's Electronic Transactions Act 2008, section 90, takes a similar stance if they acted as a "mere conduit".[245] While this protects open discourse, it also makes it harder to hold platforms accountable for anonymous abuse.

The internet's architecture (IP masking, encryption, decentralisation) amplifies privacy while undermining traceability, and its borderless nature strains territorial legal systems. Real-name

[239] Constitution of the Republic of Ghana 1992, art 21
[240] African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) art 9
[241] US Constitution amend I
[242] European Convention on Human Rights (1950) art 10
[243] Constitution of Ghana 1992, art 18
[244] Communications Decency Act 1996, s 230 (US)
[245] Electronic Transactions Act 2008 (Ghana), s 90

mandates, as seen in South Korea,[246] chill speech and endanger vulnerable voices, while broad platform liability risks stifling innovation. A balanced solution is regulated anonymity. Platforms retain minimal identifying data under strict safeguards, releasing it only through court orders that meet clear statutory thresholds, such as the US Dendrite test[247] or UK Norwich Pharmacal orders.[248] Remedies should include unmasking orders, injunctions, and damages.

Policy recommendations

- Enact statutory "regulated anonymity" provisions requiring platforms to retain but protect minimal identifying data for lawful unmasking.
- Set a high legal threshold for unmasking, including prima facie proof of unlawful harm and judicial oversight.
- Harmonise cross-border enforcement to address the global reach of online harm.
- Establish safe harbours for whistleblowers and public interest disclosures.
- Require transparency reports on unmasking requests and outcomes.
- Invest in digital literacy to build public resilience against reputational harm.

In sum, anonymity should remain the default in cyberspace, grounded in fundamental rights, but paired with targeted, rights-respecting legal tools for accountability. Precision regulation, not blanket bans, offers the most sustainable path for balancing privacy, expression, and the public interest in the digital age.

Critique

I have read Felix Aboagye (2225798710)'s paper and I like it. It is well-structured and defines key terms clearly, which helps the reader follow the argument easily. It thoughtfully balances the merits and demerits of online anonymity, grounding the discussion in Ghana's legal framework and international guidance. The inclusion of specific rights like privacy, data protection, freedom of expression, and their linkage to anonymity is a strong point. Additionally, the remedies section, though brief, acknowledges multiple legal responses, showing practical awareness.

[246] BBC News, 'Facebook and Twitter to face new EU rules' (29 August 2012) <https://www.bbc.com/news/technology-19357160> accessed 10 August 2025
[247] Dendrite International, Inc v Doe No 3 775 A 2d 756 (NJ Super Ct App Div 2001)
[248] Norwich Pharmacal Co Ltd v Customs and Excise Commissioners [1974] AC 133 (HL)

Section 4: Technology Weaponised: Law Chasing Harm

Considering how deepfakes and AI-driven crime test the law's ability to respond quickly, effectively, and without stifling legitimate innovation.

4.1 When Truth Becomes Synthetic: Legal and Social Responses to Deepfakes

Examines how deepfakes blur the line between truth and fabrication, and what legal and non-legal tools might contain their risks.

ANALYSIS OF THE ETHICAL AND LEGAL IMPLICATIONS OF DEEPFAKE TECHNOLOGY

Deep Fakes are synthetic media generated using sophisticated algorithms to create computer-generated media that did not actually occur[249]. While innovative, this controversial technology manipulates digital content, raising questions about authenticity, consent, and the potential for misuse[250]. Its rapid advancement has ignited crucial discourse on its ethical and legal implications[251], which we explore in this paper.

Relationship between legitimate commentary and propaganda and lies

Propaganda is defined as "information, ideas, opinions, or images, often only giving one part of an argument, that are broadcast, published, or in some other way spread with the intention of influencing people's opinions."[252]

Biased commentary occurs when a commentator seeks to present their viewpoints as factual. It articulates a perspective, frequently curating facts to bolster an argument but may be legitimate though

[249]D Gamage, J Chen and K Sasahara, 'The Emergence of Deepfakes and Its Societal Implications: A Systematic Review' (presented at the *Conference for Truth and Trust Online*, USA, October 2021) https://www.researchgate.net/publication/355583941_The_Emergence_of_Deepfakes_and_its_Societal_Implications_A_Systematic_Review accessed 26 June 2025.

[250] Ibid

[251]Law Librarianship Editorial, 'The Ethical and Legal Implications of Deepfake Technology' (Law Librarianship, 28 March 2025) https://lawlibrarianship.com/the-ethical-and-legal-implications-of-deepfake-technology/ accessed 26 June 2025

[252]Cambridge Dictionary, 'Propaganda' https://dictionary.cambridge.org/dictionary/english/propaganda accessed 21 June 2025

biased. Deepfake technology makes this distinction much more imprecise. Biased comments turn into propaganda and lies when deepfakes are used to assign untrue statements to specific people, producing persuasive but fake information. Presenting a biased viewpoint generates into purposefully misleading the audience by creating "evidence," - eroding credibility and truth[253].

Impact of fake news

Fake news profoundly distorts public understanding by spreading misinformation and creating "alternative facts" where existing biases are reinforced. This causes the public to view traditional media with dismay and distrust, undermining confidence in reliable sources[254]. An example is the Sandy Hook school shooting, which some believe never happened because of fake spread by others[255].

If all views are considered equally valid, then objectivity and balance lose their essential significance. Factual accuracy is reduced to merely another "perspective" in such situations, undermining the journalistic pursuit of truth[256]. This liberal viewpoint may cause society to become fractured and unable to discern between intentional lies and verifiable facts, endangering democratic processes and well-informed decision-making.

Difference in the way different demographics use and respond to fake news

Older persons, especially those over 65, may be more likely to believe and spread fake news, especially on platforms like WhatsApp and Facebook. While technologically adept, younger generations are susceptible to false information, especially on platforms, like TikTok and Twitter.

---

[253]Liam Scott, 'Deepfakes a "Weapon Against Journalism," Analyst Says' *VOA News* (16 January 2024) https://www.voanews.com/a/deepfakes-a-weapon-against-journalism-analyst-says-/7442897.html accessed 26 June 2025
[254]Cornell University Library, 'Misinformation, Disinformation, and Propaganda: Fake News' (LibGuides) https://guides.library.cornell.edu/evaluate_news accessed 22 June 2025
[255]Joanna Slater, 'Connecticut Jury Orders Alex Jones to Pay Nearly $1 Billion to Sandy Hook Families' *The Texas Tribune* (12 October 2022) https://www.texastribune.org/2022/10/12/alex-jones-sandy-hook-shooting/ accessed 21 June 2025
[256]AK Schapals and A Bruns, 'Responding to "Fake News": Journalistic Perceptions of and Reactions to a Delegitimising Force' (2022) 10(3) *Media and Communication* 5 https://doi.org/10.17645/mac.v10i3.5401 accessed 25 June 2025

Higher education is frequently associated with an improved ability to distinguish between real and misleading news. Socioeconomic issues might affect critical media literacy and access to trustworthy information.

Men may be more prone to come across political fake news than women, according to some studies, although both sexes are susceptible to deception.[257] People are also likely to trust news from trusted sources or news that confirms their existing biases, regardless of veracity.

Proposed Solutions

Legal

a. Empower courts to adjudicate fake information cases.
b. Pass laws that criminalise harmful deepfakes[258] and require labeling of deepfake content and biometric data[259].
c. Severe repercussions for platforms and individuals who intentionally disseminate deepfake and fake content.

Non-Legal

A. Provide whistleblower protection and safe reporting channels.

B. Provide AI and deepfake detection tools for government institutions.

C. Media literacy training for schools, churches, and identifiable groups.

D. Fact checking collaborations between media organizations, scholars, and digital businesses.

[257]G Rampersad and T Althiyabi, 'Fake News: Acceptance by Demographics and Culture on Social Media' (2019) 17(1) *Journal of Information Technology & Politics* 1 https://doi.org/10.1080/19331681.2019.1686676 accessed 25 June 2025
[258]US Congress, *DEEP FAKES Accountability Act*, HR 3230, 116th Congress (2019) https://www.congress.gov/bill/116th-congress/house-bill/3230 accessed 25 June 2025
[259]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence ('AI Act') (OJ L 1689, 12 July 2024) https://eur-lex.europa.eu/eli/reg/2024/1689/oj accessed 23 June 2025

E. Empower traditional and religious authorities to enforce cultural virtues of integrity among followers.

Conclusion

The 1992 Constitution guarantees freedom of speech and expression - with exceptions for fairness, justice, and truth. Fully implementing provisions in legislation, like Act 775[260], Act 772, and Act 29,[261] which prohibit dissemination of false information, will combat fake news.

Critique

We have read Group 5's work; their write-up offered an insightful analysis of the deepfake phenomenon within the broader crisis of digital misinformation, effectively combining legal and technological aspects as well.

As social perspectives, it referenced Ghana's existing legal framework and drew from international legislation to propose actionable policy solutions. However, it concentrated too much on punitive measures without sufficiently addressing enforcement challenges, risking freedom of expression and the nuanced distinction between harmful and benign synthetic media. A more holistic framework balancing robust regulation, technological innovation, digital literacy, and rights-based safeguards would enhance its effectiveness and make it a stronger foundation for national and regional policy making in IT law**.**

[260]Electronic Communications Act 2008 (Ghana) s 76
[261]Criminal Offences Act 1960 (Ghana) ss 185, 208

4.2 Project Safeguard: An investigative AI System for Combating Online Child Sexual Exploitation in Oseikrom

Designs and critiques an AI-driven investigative tool, probing its legality, evidentiary value, and cross-border implications.

Introduction

With rising online Child Sexual Exploitation (CSE) cases, Oseikrom's President tasked the National Security Office (NSO), in partnership with the Cybersecurity Authority (CSA) and the Ministry of Justice, to explore a tech-enabled solution. This paper outlines the solution (an AI system for detecting CSE) designed by technical, legal, and national security experts. Oseikrom's laws are modeled on Ghana's cybercrime, data protection, and child protection frameworks.

PART 1

1.1 NSO Requirements

The NSO brief required a smart, automated system that worked with minimal human input in early stages to avoid tipping anyone off, support cross-border investigations, and allow collaboration with international agencies. The system also needed to gather secure, tamper-proof evidence and scan both the regular internet and dark web to spot and disrupt CSE networks.

1.2 Technical Design of IT Solution by CSA

This system comprises six integrated modules working in concert to detect, investigate, and escalate online CSE cases.

The **Autonomous Crawling Module** deploys intelligent bots to scan the surface, deep, and dark web for CSE content. They mimic human browsing behavior to bypass anti-bot defenses, prioritize high-risk websites using heuristic signals, and continuously monitor target sites for updates.

The **AI Detection Engine** processes image, text, and audio content. It leverages Convolutional Neural Networks (CNNs) and tools like PhotoDNA for visual analysis, Natural Language Processing (NLP) for detecting grooming language, and audio analysis for distress cues. A feedback loop refines detection accuracy based on analyst input.

The **Digital Forensics & Evidence Collection Module** captures entire web pages, media files, and interaction logs while maintaining legal admissibility. It applies cryptographic hashes, logs metadata

such as timestamps and IP addresses, preserves chain of custody, encrypts sensitive data, and enables exportable reports for prosecutorial use.

The **Secure Data Management & Compliance Module** operates in a secure, air-gapped environment with strict Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and intrusion detection. It follows privacy-by-design and data minimization principles, automatically purging non-suspicious data. Security is reinforced by disabling web-server directory listing, stripping file metadata, using strong encryption algorithms like Blowfish, disabling caching, and employing File Integrity Monitoring. For threat detection and incident response, the system integrates the open-source Wazuh platform.

The **Interoperability & Intelligence Sharing Module** facilitates integration with other agencies. It cross-references case data with Oseikrom's CSA, shares threat intelligence under legally defined protocols, and generates real-time alerts that enable analysts to act swiftly.

Finally, the **Human Oversight & Legal Coordination Module** empowers analysts to review system alerts, validate AI decisions, and escalate or dismiss cases. It supports cross-border collaboration through tools for Mutual Legal Assistance Treaty (MLAT) requests, INTERPOL referrals, and reporting to entities such as the Cybercrime Unit and the U.S.-based National Center for Missing and Exploited Children (NCMEC).

Part 2: Legal Analysis

Q1: Under Ghanaian/Oseikrom law, the use of AI-powered investigative tools for intelligence gathering is lawful, provided it aligns with constitutional safeguards, statutory authorizations, and principles of relevance, admissibility, proportionality and necessity. Act 1038,[262] empowers the CSA[263] and national security agencies to combat cybercrimes and protect children online. Act 560[264] justifies the search of premises where a child is kept if there is a suspicion of child abuse. Although offline, it can be interpreted to justify the deployment of investigative surveillance tools when read in conjunction with Acts 772 and 1038. Intelligence use must be subject to judicial or administrative authorization and comply with privacy standards under the Data Protection Act, 2012 (Act 843). We were guided by the

[262] Cybersecurity Act 2020 (Act 1038)
[263] Sections 3 and 45 of Act 1038
[264] Children's Act, 1998 (Act 560) Sections 19

ACPO guidelines[265] in designing the tool. These require competent persons to access original data, leaving data unchanged, keeping an audit trail, and legal compliance.

Q2: For evidence collected by the system to be admissible:

- It must be **relevant**, **reliable**, and **legally obtained**. Under Ghana's Evidence Act[266], only relevant evidence with probative value is admissible unless excluded for reasons of fairness or public policy.
- However, AI-generated evidence raises concerns about accuracy and constitutional compliance. Unlawfully obtained data e.g. through rights violations, may be rejected. While courts may accept such evidence if it meets legal thresholds, Act 772 requires updating to accommodate the complexities of AI and cybersecurity investigations. The Supreme Court however held that in criminal cases involving grievous crime, where police infraction of the accused's rights was unavoidable in obtaining evidence, the evidence would be admitted[267].
- **Section 62** of Act 1038 covers child pornography, while **Section 141** of Act 772 governs the handling and disclosure of seized digital material. These provisions provide a legal basis for ensuring that software-driven investigations align with domestic law and international standards. Expert testimony can also explain the system's workings, similar to how digital forensics experts testify in cybercrime cases.[268] The system's automated logging and secure storage can also prove that the data collection was lawful.

Q3: An **online search** involves the automated or manual exploration of online systems to locate specific information or evidence. While both online and offline searches aim to retrieve evidence, they differ significantly:

Crawling and Scraping: Using web crawlers to access public or semi-public websites may not require a warrant, especially if the content is openly accessible. However, where tools bypass authentication or access protected content, judicial authorization may be necessary[269].

---

[265] Association of Chief Police Officers of England, Wales & Northern Ireland Good Practice Guidelines for Digital Evidence https://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf

[266] Evidence Act, 1975 (NRCD 323) Sections 51 and 52

[267] Raphael Cubagee v. Michael Yeboah Asare and 2 Others (Ref NO. J6/04/2017)

[268] Sections 67 and 112 of NRCD 323

[269] Edmund Addo v A-G & IGP [2017] DLHC 3835 (SUIT NO. HR/0080/2017)

Ghanaian Law Perspective: Under Act 1038, online investigations must respect personal data rights. Investigating private online spaces (e.g., encrypted chatrooms) is analogous to entering private premises and may need a cyber warrant[270].

Q4: Cross-border investigations raise jurisdictional challenges. Ghana cannot unilaterally access data or conduct investigations abroad without breaching state sovereignty.[271] Its laws have no extraterritorial effect unless extended by treaty. The Budapest Convention on Cybercrime, to which Ghana is a party, enables international cooperation through mutual legal assistance.[272] Ghana's Data Protection Act 2012 (Act 843) lacks explicit rules on cross-border data transfers but requires controllers to ensure adequate safeguards and register transfer destinations with the Data Protection Commission.[273] Contractual safeguards are also expected when using foreign processors.[274] Unlike Ghana, countries like Germany (GDPR) and India (DPDP Act 2023) impose stricter rules on outbound data. Accessing foreign servers without authorization risks breaching their laws.[275]

Solution:

- Use **Mutual Legal Assistance Treaties (MLATs)** or INTERPOL channels.
- Collaborate with foreign CERTs[276] or national cybersecurity bodies.
- Use geo-fencing features to pause autonomous functions in foreign jurisdictions unless prior clearance exists.

Conclusion and Recommendations

"Project Safeguard" offers a lawful, AI-driven approach to tackle online child sexual exploitation in Oseikrom. Its use for intelligence is permissible but must operate under strict oversight and legal safeguards. Cross-border features require strong international cooperation.

We recommend:

- Updating laws on digital forensics and surveillance.
- Ensuring independent oversight and full audit trails.

---

[270] Section 70(1)(c) and (2) of Act 1038
[271] Charter of the United Nations 1945, art 2(1)
[272] Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185, arts 23–35
[273] Data Protection Act 2012 (Act 843), s 45; *Navigating Cross-Border Data Protection: Evaluating Our Legal Framework Against International Standards*, B&FT Online (Accra, 28 March 2025) <https://thebftonline.com/2025/03/28/navigating-cross-border-data-protection-evaluating-our-legal-framework-against-international-standards> accessed 27 July 2025
[274] ibid
[275] European Union, Regulation (EU) 2016/679 (General Data Protection Regulation); India, Digital Personal Data Protection Act 2023
[276] Computer Emergency Response Team (created by sections 41-44 of Act 1038)

- Joining global frameworks like the Budapest Convention.

Critique

We peer reviewed the work of Group 5. The group started with an introduction and subsequently mentioned some functional requirements for the system like the need for the system to have Crawler Manager, Classifier Pipeline amongst others. They also mentioned non-functional requirements like human oversight and welfare. Again they mentioned the need for Threat Intelligence feeds. In terms of security and the compliance engine, the Group mentioned applying best coding practices and keeping Software Bill of materials for supply chain checks as well as mentioning the need for a red-team to fight cyber threat actors. However, they failed to mention controls that will counter the known OWASP Top Ten vulnerabilities or mention the implementation of a File Integrity Monitor to reveal any changes to the content of the data as a measure to ensure data integrity of the system. In respect of admissibility of digital evidence, the Group mentioned that they will ensure that they obtain digital evidence lawfully through a judicial warrant, ensure that data is compliant with the Data Protection ACT 2012 (ACT 843) and the Electronic Transactions ACT 2008 (ACT 772). It is our opinion that Digital evidence might not be admissible in court if it fails to follow the requirements of ACPO Principles of electronic evidence .i.e. “No action performed on digital evidence should change the data”, “Data should be accessed in such a way that integrity of the data is preserved”, “A chain of Custody of all processes must be recorded in a way that another expert can easily replicate the process and obtain the same results” and “The responsibility of analyzing Digital evidence lies with the Digital Forensics Examiner who has the responsibility of ensuring that the collection and handling of digital evidence is lawful and proportionate.

Compiled References

Cases

- *Adams v Lindsell* (1818) 1 B & Ald 681
- *Athena Brands Ltd v Superdrug Stores Plc* [2019] EWHC 3503 (Comm)
- *Brinkibon Ltd v Stahag Stahl und Stahlwarenhandelsgesellschaft mbH* [1983] 2 AC 34 (HL)
- *Entores Ltd v Miles Far East Corporation* [1955] 2 QB 327 (CA)
- *Ker-Optika bt v Állami Népegészségügyi és Tisztiorvosi Szolgálat (ANTSZ)* (Case C-108/09) EU:C:2010:725

- *LJ Korbetis v Transgrain Shipping BV* [2005] EWHC 1345 (QB)

Legislation

- *Copyright Act 2005* (Act 690) (Ghana)
- *Constitution of the Republic of Ghana 1992*
- *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-Commerce Directive)*
- *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector* [2002] OJ L201/37
- *Electronic Transactions Act 2008* (Ghana, Act 772)
- *Freedom of Information Act 2000* (UK)
- *General Data Protection Regulation (EU) 2016/679* [2016] OJ L119/1
- *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending various regulations and directives (Artificial Intelligence Act)* [2024] OJ L 2024/1689, 12 July 2024 http://data.europa.eu/eli/reg/2024/1689/oj
- *Right to Information Act 2019* (Ghana) (Act 989)
- *Uniform Computer Information Transactions Act (UCITA) 2002* (US)
- *Uniform Electronic Transactions Act (UETA) 1999* (US)
- *17 USC § 107 (2012)* (US)

International Instruments & Treaties

- *Berne Convention for the Protection of Literary and Artistic Works* (as amended on 28 September 1979) art 10(1) - (2) https://www.wipo.int/treaties/en/ip/berne/ accessed 22 June 2025
- *Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled* (adopted 27 June 2013, entered into force 30 September 2016) 52 ILM 1321

- *UNCITRAL, Guide to Enactment of the Model Law on Electronic Commerce* (1996) https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce accessed 14 June 2025
- *UNCITRAL, Model Law on Electronic Commerce* (adopted 16 December 1996) UN Doc A/RES/51/162
- *UN General Assembly, Transforming our world: the 2030 Agenda for Sustainable Development* (21 October 2015) UN Doc A/RES/70/1, Goal 4 https://sdgs.un.org/goals/goal4 accessed 22 June 2025
- *United Nations Convention on the Use of Electronic Communications in International Contracts 2005*
- *Universal Declaration of Human Rights* (adopted 10 December 1948 UNGA Res 217 A(III))
- *UNESCO, Recommendation on Open Educational Resources* (adopted 25 November 2019) https://unesdoc.unesco.org/ark:/48223/pf0000370936 accessed 16 June 2025
- *UNESCO, UNESCO Recommendation on Open Science* (adopted 23 November 2021) https://unesdoc.unesco.org/ark:/48223/pf0000379949 accessed 22 June 2025

Secondary Sources

- Ambolley J, 'Institutional culture of silence and secrecy hindering RTI law implementation – Kojo Oppong Nkrumah' *GhanaWeb* (14 December 2023) https://www.ghanaweb.com/GhanaHomePage/NewsArchive/Institutional-culture-of-silence-and-secrecy-hindering-RTI-law-implementation-ndash-Kojo-Oppong-Nkrumah-1898165 accessed 17 July 2025

- Boyle J, 'Public information wants to be free' *Financial Times* (24 February 2005) https://www.ft.com/content/cd58c216-8663-11d9-8075-00000e2511c8 accessed 22 June 2025
- ChatGPT, *AI and automation: impact on jobs* CNN (29 March 2023) https://edition.cnn.com/2023/03/29/tech/chatgpt-ai-automation-jobs-impact-intl-hnk accessed 5 July 2025
- CNN, '"Godfather of AI" Geoffrey Hinton quits Google to warn over the tech's threat to humanity' *CNN* (3 May 2023) https://edition.cnn.com/videos/tech/2023/05/03/geoffrey-hinton-quits-google-danger-artificial-intelligence-lead-ldn-vpx.cnn accessed 5 July 2025

- Creative Commons, *The Power of Open: Stories of Creators Sharing Knowledge, Art & Data Using Creative Commons* (2011) https://thepowerofopen.org/ accessed 22 June 2025
- De Cosmo L, 'Google Engineer Claims AI Chatbot Is Sentient: Why That Matters' *Scientific American* (3 March 2022) https://www.scientificamerican.com/article/google-engineer-claims-ai-chatbot-is-sentient-why-that-matters/ accessed 5 July 2025
- Emborg T, 'The EU's Pacing Problem: Why crafting and enforcing AI regulation is hard' *Verfassungsblog* (19 December 2023) https://verfassungsblog.de/the-eus-pacing-problem/ accessed 5 July 2025
- Frankel M, 'The roots of Blair's hostility to Freedom of Information' *openDemocracy* (7 September 2010) https://www.opendemocracy.net/en/freedom-of-information/roots-of-blairs-hostility-to-freedom-of-information/ accessed 17 July 2025
- GetJara, 'The Role of Smart Contracts in Automation: How Blockchain Enables Trustless Agreements' (GetJara, 2023) https://getjara.xyz/the-role-of-smart-contracts-in-automation-how-blockchain-enables-trustless-agreements-2/ accessed 14 June 2025
- Höppner S, 'ChatGPT one year on: How has it affected the way we work?' *DW* (30 November 2023) https://www.dw.com/en/chatgpt-one-year-on-how-has-it-affected-the-way-we-work/a-67588407 accessed 5 July 2025
- IBM, 'What are Smart Contracts?' (IBM, 2023) https://www.ibm.com/topics/smart-contracts accessed 14 June 2025
- McCauley L, 'Countering the Frankenstein Complex' in Papers from the 2007 AAAI Spring Symposium: Multidisciplinary Collaboration for Socially Assistive Robotics (AAAI Press 2007) https://aaai.org/papers/0010-ss07-07-010-countering-the-frankenstein-complex/ accessed 5 July 2025
- Pollicino O and De Gregorio G, 'ChatGPT: lessons learned from Italy's temporary ban of the AI chatbot' *The Conversation* (20 April 2023) https://theconversation.com/chatgpt-lessons-learned-from-italys-temporary-ban-of-the-ai-chatbot-203206 accessed 5 July 2025

- Polonski V, ‘AI has huge potential – but it won’t solve all our problems’ *World Economic Forum* (14 June 2018) https://www.weforum.org/stories/2018/06/ai-cannot-solve-all-our-problems / accessed 5 July 2025
- Politics Teaching, *What is the Freedom of Information Act and why did Tony Blair call it stupidity?* (22 January 2024) https://politicsteaching.com/2024/01/22/what-is-the-freedom-of-information-act-and-why-did-tony-blair-call-it-stupidity/ accessed 17 July 2025
- PrivacyTerms.io, ‘Clickwrap vs Shrinkwrap vs Browsewrap’ (PrivacyTerms.io, 2024) https://privacyterms.io/terms/clickwrap-vs-shrinkwrap-vs-browsewrap/ accessed 2 August 2025
- Sheriff K, Halm KC and Seiver JD, ‘European Parliament Approves Amendments to Expand the Scope of EU AI Act’ *Davis Wright Tremaine Artificial Intelligence Law Advisor Blog* (16 June 2023) https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2023/06/european-union-ai-amendments-approved accessed 5 July 2025
- World Bank, *Freedom of Information Access: Key Challenges, Lessons Learned and Strategies for Effective Implementation* (1 June 2020) https://hdl.handle.net/10986/34155 accessed 17 July 2025