Uganda Pentecostal University Journal of Sustainable Development
Journal DOI Prefix: 10.69612
Journal ISSN: 3078-2384
Issue 2

ARTIFICIAL INTELLIGENCE AS AN EMERGING CHALLENGE TO DATA PROTECTION AND PRIVACY LAW IN UGANDA

Article Authors:

Ampulira Ronald, School of Law, Kampala International University, Grotius School of Law, Uganda Pentecostal University. Email: jeremihjero@gmail.com

Adenyuma Gabriel, Kampala International University, School of Law. Email: adenyuma.gabriel@kiu.ac.ug

Ahmed Hussein Folrunsho, Faculty of Law, University of Ilorin. Email: folorunsho.ah@unilorin.edu.ng

ABSTRACT

The rapid proliferation of artificial intelligence (AI) technologies across Africa's public and private sectors has exposed fundamental inadequacies in the legal architecture governing data protection and privacy. In the particular context of Uganda which is the focus of this study the Data Protection and Privacy Act, Cap 97 (DPPA) enacted in 2019 provides a foundational framework for the regulation of personal data, yet it predates the mainstream adoption of AI and conspicuously fails to address the distinctive risks that AI-driven systems pose to the rights of data subjects as is the case in many other parts of the continent. This article critically examines the interface between artificial intelligence and Uganda's data protection law, focusing on three principal concerns: the erosion of data minimisation, transparency, and accountability principles by AI systems; the proliferation of algorithmic bias and its discriminatory effects on marginalised populations; and the deployment of AI-enabled mass surveillance technologies by state and non-state actors without adequate legal safeguards. Drawing on the DPPA, comparative jurisprudence from the European Union, Kenya, Rwanda, and India, and enforcement decisions of the Personal Data Protection Office, the article argues that Uganda's current legal framework is structurally ill-equipped to govern AI-driven data processing. It proposes targeted legislative reforms, including the enactment of dedicated AI governance provisions within the DPPA, mandatory algorithmic impact assessments, and the strengthening of the PDPO's institutional independence and technical capacity. The study sets the pace for similar studies in other parts of the African continent where similar studies have not been carried out.

Key Words: Artificial Intelligence, Data Protection, Privacy, Uganda, DPPA, Algorithmic Accountability, Surveillance, GDPR

INTRODUCTION

Artificial intelligence has emerged as one of the most transformative and disruptive forces in the contemporary digital landscape, with profound implications for the protection of personal data and the right to privacy. In Uganda, AI technologies are increasingly deployed across sectors including financial services, healthcare, agriculture, and national security. Mobile money platforms utilise machine-learning algorithms to assess creditworthiness; government agencies deploy facial recognition systems in major urban centres; and private companies harvest vast quantities of behavioural data to train predictive models. Each of these applications implicates the rights of data subjects whose personal information is collected, processed, and acted upon often without their knowledge, understanding, or meaningful consent.

Uganda's constitutional commitment to privacy is expressly stated in Article 27 of the Constitution of the Republic of Uganda, 1995, which guarantees the right to privacy of person, home, and correspondence, and prohibits unlawful interference with communications and other property. In its section 2, the Data Protection and Privacy Act, Cap 97, enacted in 2019, operationalises this constitutional guarantee by establishing a framework for the regulation of personal data collection, processing, and storage. However, the DPPA was conceived in an era when the transformative capabilities of AI had not yet manifested in Uganda's regulatory consciousness. As a consequence, the Act's provisions while commendable in their foundational principles, are silent on the governance of automated decision-making, algorithmic profiling, and AI-specific data risks, leaving a critical regulatory lacuna that jeopardises the privacy rights of millions of Ugandan citizens.

This article proceeds in eight parts. Following this introduction, Part 2 sets out the background and statement of the problem. Part 3 articulates the research objectives. Part 4 states the research questions. Part 5 outlines the methodology employed. Part 6 constitutes the body of the analysis, examining the specific AI-related challenges to data protection across the domains of data minimisation, transparency, accountability, algorithmic bias, and surveillance. Part 7 presents the key findings, and Part 8 sets out the conclusions and recommendations.

Uganda's digital economy has expanded rapidly over the past decade, driven by the penetration of mobile telephony, the proliferation of internet-based services, and ambitious government digitalisation programmes including the National Digital Identity System and e-government initiatives. This digital transformation has been accompanied by an exponential increase in the volume, variety, and velocity of personal data generated and processed within the country. Against this backdrop, AI systems which are dependent on large datasets for training, validation, and deployment have become increasingly central to both commercial and governmental operations.

The enactment of the DPPA in 2019 marked a significant legislative milestone, giving statutory expression to Article 27 of the Constitution and aligning Uganda's data protection regime with international instruments such as the EU General Data Protection Regulation and the African Union Malabo Convention. The Act in section 1 establishes the Personal Data Protection Office under the National Information Technology Authority–Uganda as the primary regulatory body, and sets out principles of lawful processing, including accountability, fairness, transparency, and security.

Notwithstanding this progress, the legal framework has been overtaken by technological developments. Concrete enforcement decisions illustrate the nature and scale of the problem. In Lubega v MTN (U) Ltd.,the High Court reiterated the fiduciary obligation of data handlers to protect subscriber data from unauthorised disclosure which is an obligation that AI-driven systems routinely strain through automated data aggregation and sharing. In the SafeBoda administrative enforcement action of 2021, NITA-U found that the ride-hailing company had shared users' geolocation data with an external analytics firm without informed consent, yet no penalty was imposed. Most significantly, in PDPO v Mugulusi Uganda's first criminal conviction under the DPPA — the Personal Data Protection Office found that the director of a microfinance application had processed borrower data, including names, telephone numbers, and photographs, without consent, using them to create shaming videos for debt recovery.These cases, while not exclusively AI-related, reveal the systemic inadequacy of the DPPA in the face of data-intensive technologies. The Act's provisions do not address algorithmic transparency, automated decision-making, AI-specific data impact assessments, or the governance of AI-enabled surveillance all of which are critical regulatory gaps in the contemporary Ugandan digital environment. It is against this backdrop that the present article offers a critical legal appraisal.

RESEARCH OBJECTIVES

1. To examine how AI systems affect the core data protection principles enshrined in Uganda's legal framework, specifically data minimisation, transparency, and accountability.
2. To identify the legislative gaps and enforcement deficiencies that prevents the DPPA from adequately governing AI-driven data processing.
3. To propose concrete legal and institutional reforms to align Uganda's data protection framework with international best practices and emerging regional standards.

RESEARCH QUESTIONS

1. How do AI systems challenge the data minimisation, transparency, and accountability principles under the DPPA and comparable international frameworks?
2. What structural legislative and institutional gaps prevent the DPPA from adequately regulating AI-driven data processing, algorithmic bias, and surveillance?

3. What legal and policy reforms are necessary to ensure that Uganda's data protection framework effectively safeguards privacy rights in an AI-driven environment?

METHODOLOGY

The article adopts a doctrinal legal research methodology, involving critical analysis and synthesis of primary legal materials including legislation, judicial and administrative decisions, and international instruments alongside secondary sources comprising scholarly articles, policy documents, and comparative legal analyses. A comparative approach is employed to situate Uganda's legal framework within the broader context of international and regional data protection standards, drawing primarily on the GDPR, the Malabo Convention(the African Union Convention on Cyber Security and Personal Data Protection), and the data protection regimes of Kenya and Rwanda. The comparative exercise is not merely illustrative: it is deployed to identify normative standards that should inform legislative reform in Uganda. The article also draws on enforcement decisions of the PDPO and NITA-U to ground the legal analysis in practical realities.

ANALYSIS: AI AND DATA PROTECTION IN UGANDA

Data Minimisation and the AI Data Appetite

The principle of data minimisation, which requires that personal data be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed, represents one of the foundational constraints on the lawful processing of personal data (General Data Protection Regulation (EU) 2016/679 (GDPR) art 5(1)(a). It is reflected in Article 13(3)(b) of the Malabo Convention and finds expression in Section 13(1)(c) of the DPPA, which requires data collectors to collect and process only adequate, relevant, and not excessive or unnecessary personal data.

AI systems are structurally antithetical to data minimisation. Machine learning models particularly deep learning architectures require vast quantities of data for training, and their performance frequently improves with the quantity and diversity of the datasets on which they are trained. In Uganda's context, the deployment of AI-enabled drones, CCTV systems with facial recognition capabilities, and mobile health applications that harvest biometric and behavioural data routinely captures personal information far in excess of what is necessary for the stated purpose.

The DPPA does not guide how the data minimisation principle applies to AI training datasets, validation sets, or inference processes. Unlike the GDPR, which requires data controllers to implement appropriate technical and organisational measures to ensure that, by default, only personal data which are necessary for each specific purpose of processing are processed,1 the DPPA contains no "privacy by design and by default" obligation, no prohibition on the collection of data for undefined future AI applications, and no requirement

that data collected for one purpose be algorithmically segregated from data used for a different purpose. This regulatory silence permits data controllers and processors to accumulate personal data on a speculative basis, what scholars have termed "data hoarding" in anticipation of future AI applications that may not yet be defined at the time of collection.

Transparency and The Opacity Of Algorithmic Systems

Transparency in data processing requires that data subjects receive clear and adequate information about how their personal data is being collected and used. This principle is foundational to the exercise of other data subject rights: one cannot meaningfully object to processing, request erasure, or seek redress for harm if one does not understand that processing is occurring. The DPPA's transparency requirement, reflected in Section 13(1)(f), obliges data controllers to "ensure transparency and participation of the data subject."

The AI systems pose a lot of challenges (Kurata 2025). It poses a fundamental challenge to transparency. The "black box" problem such as the inherent opacity of deep learning algorithms whose internal decision-making processes are not intelligible even to their designers means that compliance with a formal transparency obligation may be technically impossible in respect of many AI systems. A mobile money operator that uses a machine learning model to determine whether to approve a loan application cannot, in most cases, provide a data subject with a meaningful explanation of why the decision was reached, because the model itself does not generate human-interpretable reasoning.

The GDPR addresses this challenge through Article 22, which grants data subjects the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal or similarly significant effects, and the right to obtain human review and a meaningful explanation of such decisions. Uganda's DPPA contains no equivalent provision. Section 27 of the DPPA provides limited protection against unfair automated processing but does not confer a right to explanation, a right to human review, or a right to challenge algorithmic decisions. The Personal Data Protection Office Decision in Ssekamwa Frank & Ors v Google LLC of 2017, while significant as an assertion of the Personal Data Protection Office's extraterritorial jurisdiction, did not engage with the transparency of Google's algorithmic data processing, a reflection of both the institutional limitations of the Personal Data Protection Office and the absence of statutory obligations requiring algorithmic explainability.

Accountability and Ai Governance Gaps

The accountability principle requires data controllers and processors to be demonstrably responsible for compliance with data protection obligations. Under Regulation 12 of the Data Protection and Privacy Regulations 2021, entities processing high-risk data are required to conduct Data Protection Impact

Assessments (DPIAs). The GDPR similarly mandates DPIAs prior to any processing likely to result in a high risk to individuals, particularly where new technologies are used in terms of article 35.

In practice, however, the Personal Data Protection Office has reported very low rates of DPIA compliance, even among entities processing sensitive personal data on a large scale. This is attributable partly to low awareness, partly to the Personal Data Protection Office's limited capacity to monitor compliance, and partly to the absence of meaningful sanctions for non-compliance with the DPIA requirement. AI systems which by definition involve large-scale processing, automated decision-making, and frequently the use of sensitive personal data are precisely the systems for which DPIAs are most necessary and least performed.

Accountability is further complicated by the multi-stakeholder architecture of modern AI systems. An AI credit-scoring system deployed by a Ugandan fintech company may be developed by a software vendor in the United States, trained on data processed in a cloud infrastructure in Europe, and deployed through a mobile application accessible to Ugandan users. In such a supply chain, the allocation of data protection responsibility among developers, data providers, and deployers is unclear under the Data Protection and Privacy Act, which does not contain provisions equivalent to the GDPR's joint controllership framework under Article 26. The result is an accountability vacuum in which each actor can argue that responsibility rests elsewhere.

Algorithmic Bias and Discrimination

AI systems are trained on historical data that frequently reflects and replicates existing social inequalities. When deployed in contexts such as credit scoring, recruitment, policing, or access to public services, AI systems can perpetuate and amplify discrimination against marginalised groups, including women, ethnic minorities, persons with disabilities, and rural communities. This phenomenon, algorithmic bias represents a significant emerging challenge that Uganda's Data Protection and Privacy Act is not equipped to address.

The EU AI Act, adopted in 2024, classifies a range of AI applications including those used in employment, education, law enforcement, and access to essential services as "high-risk systems" requiring conformity assessments, documentation of training data characteristics, human oversight mechanisms, and ongoing monitoring for bias. Uganda has no equivalent classification regime. Section 27 of the Data Protection and Privacy Act offers partial protection against unfair automated processing but does not require algorithmic audits, does not mandate diverse and representative training datasets, and does not provide any mechanism for independent review of AI systems used in consequential decisions.

The comparative experience of Kenya is instructive in this regard. In Okiya Omtatah Okoiti v Communication Authority of Kenya of 2018, the Kenyan High Court invalidated a mass surveillance tool that lacked statutory precision and was found to operate in a discriminatory manner without adequate legal basis. While the case

concerned surveillance rather than algorithmic bias per se, the reasoning that the deployment of powerful data processing technologies requires a clear, accessible, and proportionate legal basis that protects against discrimination is directly applicable to AI systems in Uganda.

STATE SURVEILLANCE, AI, AND THE NATIONAL SECURITY EXCEPTION

The intersection of AI and state surveillance presents the most acute challenge to Uganda's data protection framework. Evidence has emerged that Ugandan security agencies have acquired and deployed AI-enabled CCTV systems with facial recognition capabilities in Kampala's central business district, as well as tools for monitoring digital communications. These systems are capable of tracking the movements and associations of individuals across public space, enabling the creation of detailed profiles without any individual act of interception that would trigger the safeguards under the Regulation of Interception of Communications Act.

Section 6(b) of the DPPA exempts from its application the processing of personal data by a public body in the interests of national security or public order. This broad exemption, which contains no proportionality safeguard, no requirement of judicial authorisation, and no independent oversight mechanism effectively insulates the most powerful and intrusive AI surveillance systems from any form of data protection scrutiny. The Ugandan Constitutional Court's decision in Andrew Karamagi & Anor v Attorney General of 2022, in which provisions of the Computer Misuse Act were struck down for failing the legality standard under Article 28 of the Constitution, signals a growing judicial recognition of the need for precise and proportionate legal frameworks governing state interference with digital rights. However, the DPPA's national security exemption remains unreformed.

The European Court of Human Rights, in Big Brother Watch v United Kingdom of 2021, held that a bulk interception regime that lacked sufficient safeguards against abuse violated Article 8 of the European Convention on Human Rights, emphasising that surveillance must be lawful, necessary, and proportionate, and must be subject to independent oversight. The Supreme Court of India in Justice K.S. Puttaswamy v Union of India of 2017, likewise affirmed that privacy is a fundamental constitutional right that constrains state surveillance and requires that any limitation be grounded in law, serve a legitimate aim, and be proportionate to that aim. Uganda's failure to incorporate these standards into its data protection and surveillance legislation represents a serious human rights deficit.

CROSS-BORDER DATA FLOWS AND AI SUPPLY CHAINS

AI development and deployment is inherently transnational. Training data, model infrastructure, and inference endpoints frequently straddle multiple jurisdictions. Section 19 of the DPPA prohibits the transfer of personal data outside Uganda unless the recipient country ensures an adequate level of protection or contractual safeguards are in place. However, the PDPO has not published an adequacy list, standard contractual

clauses, or binding corporate rules framework. In the absence of these instruments, the transfer regime is effectively unenforceable against the global technology companies including those providing AI infrastructure that process Ugandan personal data on a daily basis.

The challenge of exercising jurisdiction over foreign AI developers and deployers is compounded by the PDPO's institutional limitations. As the Ssekamwa v Google LLC decision demonstrated, the PDPO is willing to assert extraterritorial jurisdiction, but its practical ability to enforce compliance against entities without a physical presence in Uganda is severely constrained. The absence of binding regional mutual assistance arrangements under either the Malabo Convention or the EAC Protocol on Cyber Laws leaves Ugandan data subjects without meaningful protection against AI systems operated by foreign entities.

FINDINGS

The foregoing analysis yields four principal findings.

First, Uganda's Data Protection and Privacy Act, while providing foundational data protection principles, is structurally inadequate to govern AI-driven data processing. The Act was enacted before the mainstream adoption of AI in Uganda and contains no provisions specifically addressing automated decision-making, algorithmic transparency, AI-driven profiling, or the distinctive data risks of machine learning systems. This anachronism has been identified as a critical weakness by the Personal Data Protection Office itself and by civil society researchers.

Second, the Personal Data Protection Office lacks the institutional independence, human capacity, and technical expertise necessary to effectively regulate AI systems. The Office's budget dependence on the executive, its limited complement of technically trained staff, and its predominantly reactive, complaint-driven enforcement model collectively render it incapable of proactively supervising the deployment of AI technologies across Uganda's rapidly digitalising economy.

Third, the broad national security exemption in Section 6(b) of the Data Protection and Privacy Act creates an accountability vacuum that enables state actors to deploy AI surveillance technologies without any data protection oversight. This exemption is incompatible with Uganda's international human rights obligations under the art 17 of International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) the Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR) art 12 and the Malabo Convention previously cited , and has been implicitly criticised by Ugandan courts in cases challenging the legality of broad surveillance-enabling legislation.

Fourth, the absence of enforceable cross-border data transfer mechanisms renders the Data Protection and Privacy Act ineffective against the transnational AI supply chains through which most of the personal data of Ugandan citizens is processed. Without adequate transfer instruments and regional enforcement cooperation, the rights of Ugandan data subjects in the context of global AI systems are formally recognised but practically unprotected.

CONCLUSIONS

Uganda's Data Protection and Privacy Act represents a commendable legislative achievement that has provided a foundational framework for privacy protection in the digital age. However, the analysis in this article demonstrates that the Act's provisions are fundamentally inadequate to address the distinctive challenges posed by artificial intelligence. The gap between the law on the books and the law in action — a gap that legal realism has long highlighted as the central concern of effective legal regulation is nowhere more apparent than in Uganda's data protection regime's inability to grapple with AI-driven data processing.

RECOMMENDATIONS

Three clusters of reform are recommended

The first is legislative reform. Parliament should amend the DPPA to introduce dedicated provisions on automated decision-making, congruent with Article 22 of the GDPR,1 granting data subjects the right to explanation, human review, and challenge of consequential algorithmic decisions. Mandatory algorithmic impact assessments analogous to DPIAs but calibrated specifically to the risks of AI systems should be required before the deployment of high-risk AI applications. The national security exemption in Section 6(b) should be amended to require judicial authorisation, proportionality assessment, and independent oversight for AI-enabled surveillance. The definition of sensitive personal data should be expanded to expressly include biometric data and genetic data, as in the GDPR and Rwanda's data protection law. Rwanda Law No 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy under articles 18–22

The second cluster concerns institutional reform. The PDPO must be restructured as a constitutionally entrenched independent regulatory authority, analogous to South Africa's Information Regulator under the Protection of Personal Information Act 4 of 2013 (South Africa), particularly section 107, with its own appropriated budget, legal personality, and accountability to Parliament rather than the executive. The Office requires substantial investment in technical capacity, including the recruitment of AI specialists, data scientists, and cybersecurity experts, to enable proactive supervision of AI systems and effective investigation of AI-related data protection breaches.

The third cluster involves regional and international cooperation. Uganda should urgently ratify the Malabo Convention and engage constructively in the development of a harmonised EAC data protection framework that addresses cross-border AI data flows, mutual enforcement assistance, and the joint regulation of transnational AI platforms. The PDPO should establish formal memoranda of understanding with its counterparts in Kenya and Rwanda both of which have more developed AI governance frameworks to develop a regional approach to the oversight of AI-enabled data processing.

In conclusion, the right to privacy enshrined in Article 27 of Uganda's Constitution can only be rendered meaningful in the AI era through legislative modernisation, institutional strengthening, and regional cooperation. The cost of inaction is not merely regulatory non-compliance: it is the systematic erosion of the dignity, autonomy, and fundamental rights of Ugandan citizens in an increasingly data-driven world.

AUTHOR RIGHTS & COPYRIGHT

REFERENCES

Legislation

Computer Misuse Act Cap 96 (Uganda)

Constitution of the Republic of Uganda 1995 (as amended)

Data Protection and Privacy Act Cap 97 (Uganda)

Data Protection and Privacy Regulations 2021, SI No 1 of 2021 (Uganda)

EU AI Act (Regulation (EU) 2024/1689)

General Data Protection Regulation (EU) 2016/679

Kenya Data Protection Act 2019

Protection of Personal Information Act 4 of 2013 (South Africa)

Regulation of Interception of Communications Act Cap 101 (Uganda)

Rwanda Law No 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy

Cases

Andrew Karamagi & Anor v Attorney General, Constitutional Petition No 9 of 2022 (unreported)

Big Brother Watch v United Kingdom (Application No 58170/13) [2021] ECHR 597

Dr Stella Nyanzi v Uganda, Criminal Session Case No 21 of 2019 (unreported)

Human Rights Network Uganda v Attorney General (unreported, 2023)

Justice K.S. Puttaswamy (Retd) and Another v Union of India and Others (2017) 10 SCC 1

Kasha Jacqueline Nabagesera v Rolling Stone Ltd & Anor [2010] UGHC 103

Lubega v MTN (U) Ltd, Civil Suit No 156 of 2009 (High Court, Uganda) (unreported)

Muwanga Kivumbi v Attorney General, Constitutional Petition No 9 of 2005

Nabirye v Uganda Communications Commission, Misc Cause No 45 of 2021 (unreported)

Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 Ors [2018] eKLR

PDPO v Mugulusi (Makindye Magistrates Court, 10 July 2025) (unreported)

SafeBoda Investigation by NITA-U [2021] (administrative enforcement action, unpublished)

Ssekamwa Frank & Ors v Google LLC, Complaint No 08/11/24/6683 (PDPO Decision, 18 July 2025)

Tito Magoti v Attorney General (Miscellaneous Civil Application No 12 of 2020) (unreported)

International Instruments

African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) 2014

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171

Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III)

Books

Bygrave LA, Data Privacy Law: An International Perspective (Oxford University Press 2014)

Lynskey O, The Foundations of EU Data Protection Law (Oxford University Press 2015)

Solove DJ, Understanding Privacy (Harvard University Press 2008)

Westin AF, Privacy and Freedom (Atheneum 1967)

Journal Articles

Aaronson S, "Why Trade Agreements are Not Setting Information Free" (2015) 14(4) World Trade Review 671

Bygrave LA, "Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling" (2001) 17 Computer Law and Security Review 17

Kurata, L., Ayanwale, M. A., Molefi, R. R., & Sanni, T. (2025). Teaching religious studies with artificial intelligence: A qualitative analysis of Lesotho secondary schools teachers' perceptions. International Journal of Educational Research Open, 8, 100417.

Muhangi K, "Data Protection in Uganda in the Era of AI and IoT" (2022) 12 Uganda Law Review 120

Wachter S, Mittelstadt B and Floridi L, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (2017) 7(2) International Data Privacy Law 76

Reports and Other Sources

CIPESA, "AI Governance and Data Protection in Uganda: A Rights-Based Assessment" (2025)

Foundation for Human Rights Initiative, "Surveillance, Privacy and the Rule of Law in Uganda" (FHRI Report 2021)

National Information Technology Authority Uganda, "Annual Report 2023" (NITA-U, 2023)

Personal Data Protection Office, Annual Report 2022–2023 (PDPO 2023)

Report of the Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age, UN Doc A/HRC/51/17 (4 August 2022)