

Digital Identity, Conditional Access, and Human Dignity: A Christian Policy Analysis of Biometric Governance, Surveillance Infrastructure, and Data Justice

Sixbert Sangwa^{1*}

¹Office of the President, Open Christian University, Sacramento, United States

*Correspondence: ssangwa@openchristian.education

Abstract

Background: Digital identity systems are increasingly promoted as infrastructures for legal recognition, public-service delivery, financial inclusion, fraud reduction, security, and digital transformation. Recent global policy discourse treats identity, payments, and data exchange as foundational layers of digital public infrastructure. Yet when legal identity, biometric verification, welfare delivery, mobile connectivity, banking, health systems, education, travel, programmable payments, and AI-mediated governance converge, identity can become a gatekeeping layer for social participation. **Aim:** This article develops a Christian social-epistemological and policy analysis of emerging digital identity infrastructures, examining them neither as neutral administrative tools nor as automatically apocalyptic technologies, but as socio-technical systems with documented benefits, risks, mechanisms, and theological significance. **Method:** The study employs a secondary-data qualitative design combining comparative documentary analysis, critical realist synthesis, policy analysis, conceptual analysis, and biblical-theological reflection. It draws on peer-reviewed scholarship, official policy documents, legal texts, institutional reports, human-rights analyses, and credible datasets on digital identity, biometric governance, digital public infrastructure, surveillance, data justice, and human rights. **Findings:** The analysis shows that digital identity can support recognition, welfare access, portability, financial inclusion, and rights protection, especially where persons lack official proof of identity. However, when safeguards are weak or alternatives absent, digital identity can also intensify exclusion, surveillance capacity, function creep, vendor dependency, cybersecurity exposure, data concentration, and conditional access. The article applies a ten-level layered discernment model that distinguishes verified evidence, documented patterns, plausible inference, contested interpretation, and biblical-theological discernment. **Contribution:** The article contributes to digital governance, Christian ethics, surveillance studies, and public theology by framing digital identity as identity-mediated governance infrastructure. It proposes a disciplined framework for evaluating such systems through human dignity, conscience, accountability, proportionality, data justice, and eschatological restraint, arguing that Christian critique must avoid both technocratic optimism and fear-driven speculation.

Keywords: *digital identity; conditional access; biometric governance; digital public infrastructure; surveillance infrastructure; data justice; Christian ethics and human dignity.*

Accepted: Apr 30, 2026

Published: May 02, 2026

CITATION

Sangwa, S. (2026). *Digital Identity, Conditional Access, and Human Dignity: A Christian Policy Analysis of Biometric Governance, Surveillance Infrastructure, and Data Justice*. *Open Journal of Stigmatized Knowledge & Suppressed Discourses*, Vol 2(2). Open Christian Press.

DOI:

[10.65655/OpenChristianPress.2026.111](https://doi.org/10.65655/OpenChristianPress.2026.111)

COPYRIGHT

Open Journal of Stigmatized Knowledge & Suppressed Discourses is published by Open Christian Press. This work is licensed under the Creative Commons Attribution (CC BY) license. Copyright © 2026 by author(s).

PUBLISHER INFO

Open Christian Press—the publishing arm of Open Christian University—is produced in partnership with the Center for Faith and Work.

DISCLAIMER

The views expressed in this work are solely those of the authors and do not necessarily represent the positions of the publisher, the funders, or the authors' affiliated institutions.

1. Introduction

1.1 Background and context

Digital identity has moved from a technical matter of administrative modernization to a central question of governance, rights, economic participation, and personhood. This shift is visible in global digital policy, where identity, payments, and data exchange are increasingly treated as foundational layers of digital public infrastructure (United Nations General Assembly, 2024; World Bank, 2023; World Bank, n.d.-a).

Governments, development institutions, international organizations, financial actors, technology firms, and humanitarian agencies increasingly describe digital identity as an enabling infrastructure for legal recognition, public-service delivery, digital payments, social protection, health access, education records, travel, cross-border transactions, online authentication, and private-sector innovation. This policy logic is consistent with SDG Target 16.9, which calls for legal identity for all, including birth registration, and with digital-government frameworks that connect identity to service delivery, financial inclusion, and digital transformation (United Nations Department of Economic and Social Affairs, n.d.; World Bank, n.d.-a). The latest World Bank ID4D-Global Findex estimates indicate that more than 800 million people still lack official proof of identity, while 2.8 billion people lacked access to digital ID systems for online transactions in 2024 (Pswarayi-Riddihough et al., 2025). From a development perspective, this is a serious problem. Persons without recognized identity may be excluded from school enrolment, mobile registration, welfare transfers, formal employment, bank accounts, health services, travel documentation, and legal protection (Clark et al., 2022; World Bank, n.d.-a). Figure 1 visualizes the scale of the global identity and online digital identity gap that motivates the inclusion rationale for digital identity systems.

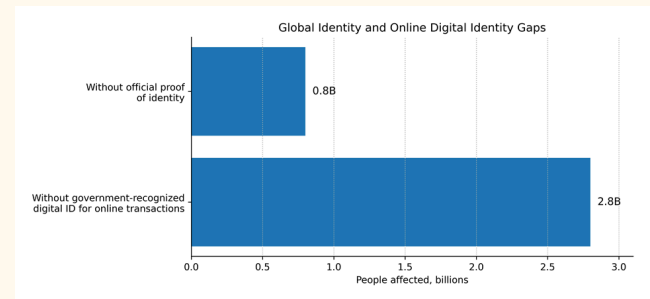


Figure 1. Global identity and online digital identity gaps. Author's visualization based on World Bank ID4D-Global Findex estimates reported by Pswarayi-Riddihough et al. (2025). The World Bank estimates that more than 800 million people lack official proof of identity and that 2.8 billion people lacked access to digital ID systems for online transactions in 2024.

At the same time, digital identity is not merely an administrative solution. It is a socio-technical infrastructure that translates human persons into datafied subjects who can be verified, authenticated, linked, authorized, excluded, monitored, corrected, or denied access. Identification systems always involve classification, but digital identification expands the scale, speed, interoperability, and persistence of classification. Once identity credentials are linked to biometric databases, welfare registries, payment systems, mobile SIM registration, education records, health platforms, tax systems, border control, or algorithmic decision-making, identity becomes a condition of participation in increasingly wide domains of life. Current ID4D data show that most foundational ID systems collect biometrics, many issue permanent identifiers, and many support digital verification or authentication across service domains (World Bank, n.d.-a). This interpretation also aligns with scholarship on datafication, classification, and infrastructure, which shows how persons and social relations can be rendered legible, actionable, and governable through data systems and standards (Bowker & Star, 1999; Star, 1999; van Dijck, 2014). This transformation raises a profound policy question: when does an infrastructure designed to include become an infrastructure capable of disciplining, sorting, or excluding?

The present article develops a Christian social-epistemological and policy analysis of digital identity systems. Its purpose is not to denounce

digital identity as inherently evil, nor to treat it as a neutral tool whose moral significance depends only on user convenience. Digital identity can serve genuine public goods. The inclusion case is recognized by the World Bank's ID4D work, which frames identification as a right, an instrument of protection, and a gateway to services, benefits, and opportunities (World Bank, n.d.-a). Digital identity can strengthen legal recognition, reduce fraud, improve portability, support emergency transfers, and lower access barriers for people previously invisible to the state. Yet it can also create new vulnerabilities through biometric capture, centralized databases, data linkage, function creep, surveillance, cybersecurity risk, algorithmic error, weak consent, vendor dependency, and conditional access to essential goods. These risks are acknowledged within mainstream digital public infrastructure governance. The Universal DPI Safeguards Framework identifies privacy vulnerability, digital insecurity, lack of recourse, discrimination, unequal access, exclusion, weak rule of law, weak institutions, and technical shortcomings as DPI risks (United Nations Development Programme [UNDP] & Office of the Secretary-General's Envoy on Technology [OSET], 2024). A mature Christian evaluation must be able to hold both realities together.

The article therefore applies a Christian social epistemology of disciplined discernment to emerging identification infrastructures. Discernment, in this study, is not suspicion as temperament. It is a morally accountable practice of judgment that tests claims, evidence, institutional mechanisms, theological meanings, and ethical implications. It resists two mirror errors. The first is institutional naivety, which treats digital identity as good because it is endorsed by governments, development agencies, technology firms, or global institutions. The second is conspiratorial credulity, which treats digital identity as evil simply because it is digital, biometric, centralized, or associated with global governance. A responsible Christian posture should not begin with fear or compliance. It should begin with evidence,

mechanism, moral analysis, rival explanations, and Scripture-governed theological discernment.

The article's central thesis is that digital identity systems should be evaluated as identity-mediated governance infrastructures. Infrastructure studies are useful here because they show that infrastructures become powerful not simply by storing information, but by embedding classifications, standards, routines, and access conditions into ordinary social life (Bowker & Star, 1999; Star, 1999). Digital identity systems are neither reducible to technical credentials nor adequately understood as isolated databases. They are embedded in legal frameworks, political economies, standards, vendor ecosystems, data protection regimes, social-service architectures, and theological narratives about the human person. The theological concern is not to claim that any present digital identity system is the mark of the beast. Such a claim would exceed the evidence and flatten the symbolic, theological, and eschatological depth of Revelation 13. Rather, the concern is to ask whether emerging systems normalize forms of conditional participation, economic dependency, identity-based authorization, behavioral legibility, and compliance architecture that should be examined with sober Christian discernment.

This argument matters because the future of digital identity will not be determined only by technical design. It will be shaped by moral imagination. If digital identity is imagined only as convenience, societies may overlook coercion. If it is imagined only as an apocalypse, societies may fail to design just systems that protect the vulnerable. The Christian intellectual task is to identify what is documented, interpret what it means, test what is claimed, preserve what is good, expose what is harmful, and refuse both panic and passivity.

1.2 Problem statement and research gap

The problem addressed in this article is the lack of an integrated Christian social-epistemological framework for evaluating digital identity infrastructures as simultaneously developmental,

political, technological, moral, and theological phenomena. Existing literature provides strong but often fragmented insights. Development policy emphasizes legal identity, financial inclusion, digital public infrastructure, fraud reduction, and efficient service delivery (Clark et al., 2022; Pswarayi-Riddihough et al., 2025; World Bank, n.d.-a, n.d.-b). Human rights scholarship highlights risks to privacy, data protection, non-discrimination, autonomy, and due process (Beduschi, 2019; Wodajo, 2024). Surveillance studies and critical data studies examine datafication, platform-mediated surveillance, infrastructural power, and the politics of visibility (Lyon, 2009; Masiero, 2023; Taylor, 2017; Zuboff, 2019). Policy documents increasingly recognize the need for safeguards, accountability, interoperability, user control, and rights-respecting digital public infrastructure (European Parliament & Council of the European Union, 2024; UNDP & OSET, 2024; United Nations General Assembly, 2024; World Bank, n.d.-c).

These literatures are valuable, but three gaps remain. First, much policy literature frames digital identity primarily through problem-solving language: inclusion, efficiency, resilience, trust, empowerment, and service delivery. This language is not false, but it can be incomplete. It may understate the institutional mechanisms through which identity becomes linked to access, data sharing, public-private dependency, and surveillance capacity. This concern is consistent with research on platform-mediated surveillance and infrastructure, where interoperable systems may create governance effects through architecture, standards, and third-party integration rather than through a single explicit coercive policy (Masiero, 2023; Star, 1999). Second, critical scholarship often identifies risks but may not sufficiently distinguish between documented harm, plausible risk, architectural affordance, political interpretation, and theological meaning. Without such distinctions, critique can become either too cautious to name danger or too sweeping to remain credible. Third, Christian engagement with digital identity often oscillates between general ethical concern and

eschatological alarm. It needs a disciplined framework that can address human dignity, conscience, truth, worship, coercion, and economic participation without collapsing into speculation.

The research gap is therefore both analytical and theological. Analytically, there is a need for a framework that can compare digital identity's inclusion promises with its exclusion and surveillance risks while preserving evidentiary discipline. Theologically, there is a need for a Christian account that treats digital identity as a question of personhood, authority, moral agency, and worship, not only as a question of privacy compliance. The article addresses this gap by combining comparative documentary analysis, critical realist synthesis, conceptual analysis, policy analysis, and biblical-theological reflection. Its intended contribution is a framework that can be used by scholars, churches, policymakers, and citizens to examine identity infrastructures without institutional naivety or conspiratorial credulity.

1.3 Research aim and questions

The aim of this article is to apply Christian social epistemology to emerging digital identity infrastructures by examining how they are framed, governed, contested, and theologically interpreted. The article does not seek to prove that digital identity is inherently oppressive, nor does it seek to defend digital identity as an inevitable path to development. It asks how such systems should be evaluated responsibly when they become infrastructural conditions for access to rights, services, money, mobility, communication, and public recognition.

The study is guided by five research questions. First, how are digital identity systems framed by governments, international organizations, technology-policy actors, and development institutions? Second, what documented benefits and risks are identified in academic and policy literature on digital identity, biometrics, digital public infrastructure, data governance, and social inclusion? Third, how can digital identity systems create or

intensify conditional access, exclusion, surveillance, institutional dependency, and infrastructural power? Fourth, how does a Christian social-epistemological model of disciplined discernment help distinguish verified evidence, documented patterns, plausible inference, contested interpretation, and theological discernment in this field? Fifth, how should Christian scholars, churches, policymakers, educators, and citizens evaluate digital identity systems in light of human dignity, conscience, truth, worship, moral agency, justice, and biblical warnings concerning coercive allegiance?

1.4 Conceptual definitions

Conceptual precision is essential because debates about digital identity are often shaped by morally attractive but analytically unstable language. Terms such as inclusion, trust, safety, empowerment, interoperability, privacy, surveillance, and conditional access may describe genuine public goods, but they may also obscure power relations. Table 1 defines the core concepts used in this article.

Table 1. Conceptual definitions used in the study

Concept	Working definition
Digital identity	A set of digital credentials, identifiers, attributes, processes, and authentication mechanisms used to establish, verify, or assert identity in digital or physical transactions.
Biometric identity	Identity verification or identification that uses bodily characteristics such as fingerprints, iris patterns, facial images, or other biometric data.
Digital public infrastructure	Reusable, standards-based digital systems, commonly including identity, payments, and data exchange, that support public and private service delivery.
Conditional access	A governance condition in which access to services, goods, rights, platforms, movement, or economic participation depends on successful identity verification or authentication.
Surveillance infrastructure	Technical, legal, institutional, and data-sharing arrangements that enable persistent observation, tracking, profiling, or behavioral governance.
Infrastructural power	The capacity of embedded systems to shape behavior and participation by becoming ordinary conditions of access.
Data justice	Fairness in how people are made visible, represented, classified, and treated through data systems.
Human dignity	The inherent worth of persons grounded in creation in the image of God, not in administrative legibility or digital credentials.
Moral agency	The capacity and responsibility of persons to deliberate, choose, obey conscience, and act before God and neighbor.
Biblical discernment	A Scripture-governed practice of testing claims, spirits, institutions, technologies, and fruits in relation to truth, righteousness, and worship.

Note. Author's synthesis from Beduschi (2019), Bowker and Star (1999), Masiero (2023), Star (1999), Taylor (2017), van Dijck (2014), World Bank (n.d.-a, n.d.-b, n.d.-c), and biblical-theological categories of dignity, truth, and discernment.

Figure 2 illustrates the conceptual move from digital identity as a credential to digital identity as identity-mediated governance infrastructure.

Digital Identity as Identity-Mediated Governance Infrastructure

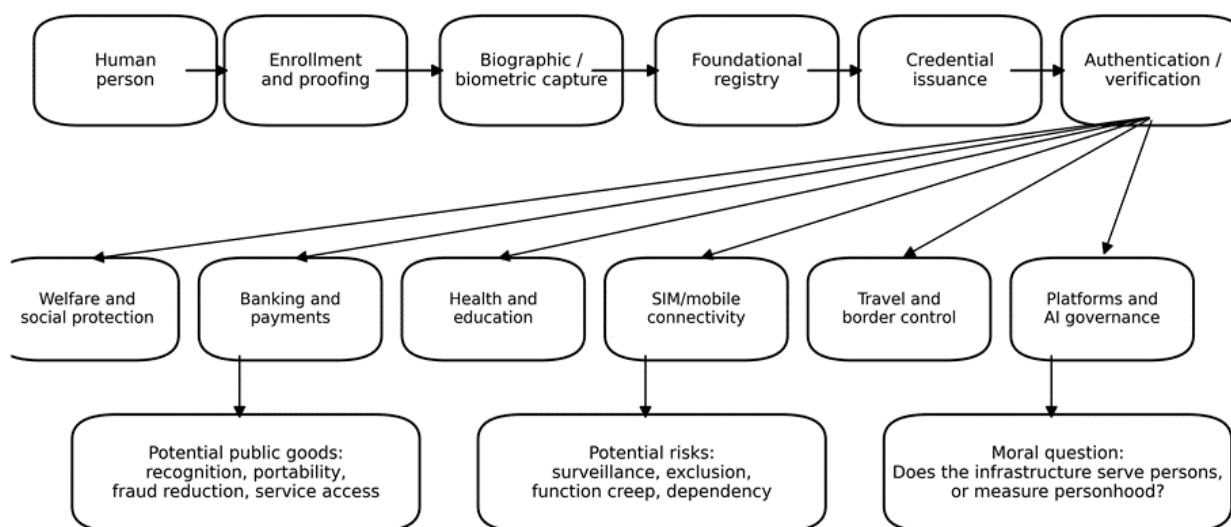


Figure 2. Digital identity as identity-mediated governance infrastructure. Author's conceptual synthesis from digital identity, digital public infrastructure, platform-mediated surveillance, infrastructure studies, data justice, and Christian social-epistemological analysis (Bowker & Star, 1999; Masiero, 2023; Star, 1999; Taylor, 2017; World Bank, n.d.-a).

2. Literature Review

2.1 Digital identity and development

The development case for digital identity begins from a serious reality: many people cannot prove who they are in ways recognized by states, banks, schools, employers, mobile operators, or service providers. The World Bank's updated ID4D-Global Findex estimates indicate that more than 800 million people lack official proof of identity and that 2.8 billion people lacked access to digital ID systems for online transactions in 2024 (Pswarayi-Riddihough et al., 2025). Clark et al. (2022) report that the identification gap is concentrated among people in lower-income countries, with children, women, the poor, rural populations, and marginalized groups especially affected. In policy terms, identification is linked to SDG Target 16.9, which calls for legal identity for all,

including birth registration (United Nations Department of Economic and Social Affairs, n.d.).

Digital identity systems are therefore often framed as enabling infrastructures. The World Bank's ID4D initiative describes identification as a gateway to rights, services, and economic opportunities, while also acknowledging the need for privacy, user rights, and trust (World Bank, n.d.-a, n.d.-b). The World Bank's digital public infrastructure work links identity, data sharing, and payments as reusable digital rails for inclusion, resilience, and innovation; it reports that ID4D and G2Px have supported more than 60 countries and helped issue more inclusive, secure, user-centered digital IDs to 550 million people (World Bank, 2023). The African Union's Digital Transformation Strategy for Africa identifies digital government, digital financial services, digital health, digital education, and digital trade among the pillars of continental transformation (African Union, 2020). This continental framing aligns with broader

global digital public infrastructure discourse in which identity, payments, and data exchange are treated as reusable public-interest digital rails (United Nations General Assembly, 2024; World Bank, 2023).

The inclusion case should not be dismissed. Without recognized identity, people may remain administratively invisible, economically excluded, and politically vulnerable. Identity can protect refugees, support social transfers, enable financial inclusion, and reduce forms of fraud that divert resources away from intended beneficiaries. A Christian analysis concerned with the poor and marginalized must take these benefits seriously. To reject digital identity without considering these public goods would be morally careless. However, the same developmental logic can become coercive when identity becomes mandatory, biometric, interoperable, and required for essential services without meaningful alternatives, appeal mechanisms, or rights protections.

2.2 Human rights, privacy, and non-discrimination

Human rights scholarship emphasizes that digital identity systems may strengthen recognition but also produce new forms of vulnerability. Beduschi (2019) argues that digital identity technologies can help people without legal documentation become visible and less vulnerable to abuse, but only if providers mitigate discrimination risks and promote high standards of privacy and data protection. Access Now (n.d.) similarly argues that digital identity systems can affect education, healthcare, work, movement, autonomy, privacy, and equality, especially when mandatory systems become the only accepted route to essential services. The Universal DPI Safeguards Framework likewise states that access should not become limiting, conditional, or mandatory, either explicitly or in practice, and calls for digital and non-digital channels (UNDP & OSET, 2024). The World Bank's ID4D Practitioner's Guide acknowledges that digital ID can amplify privacy and data-protection risks through cybersecurity vulnerabilities, large-scale data correlation, unique

identifiers, centralized databases, metadata tracking, function creep, and biometric collection (World Bank, n.d.-c). The updated ID4D dataset reports that most foundational ID systems collect biometrics and that at least 134 of 175 systems issue permanent ID numbers, underscoring the scale at which digital identity can become persistent and linkable (World Bank, n.d.-a).

The risk is not merely individual privacy loss. Wodajo (2024) argues that biometric ID programmes in Africa create societal and structural risks that are not adequately addressed by individualistic privacy frameworks alone. A people-centric account of privacy is needed because biometric identity systems affect groups, communities, and populations, not only isolated data subjects. This is especially important in contexts where religious, ethnic, political, refugee, gender, or stateless populations may be profiled or discriminated against. Data protection rules are necessary, but they are insufficient if they do not address structural power, unequal access, institutional weakness, weak rule of law, and the possibility of identity infrastructures being repurposed for exclusion.

The Universal DPI Safeguards Framework explicitly recognizes risks such as privacy vulnerability, digital insecurity, physical insecurity, lack of recourse, discrimination, unequal access, exclusion, disempowerment, digital distrust, weak rule of law, weak institutions, technical shortcomings, and unsustainability (UNDP & OSET, 2024). This is significant because it shows that concern about digital identity is not merely a fringe anxiety; it is acknowledged by mainstream global governance actors. The policy dispute is therefore not whether risks exist, but how risks should be assessed, governed, mitigated, and theologically interpreted.

2.3 Biometric governance, platform-mediated surveillance, and exclusion

Biometric digital identity systems raise particular concerns because they connect legal identity to bodily data such as fingerprints, iris scans, facial

images, or other biometric identifiers. Biometric identifiers can reduce impersonation and duplication, but they are difficult or impossible to replace if compromised. NIST guidance on authentication and authenticator management emphasizes lifecycle management, backup or alternate authenticators, and recovery processes, which becomes especially important where authentication failure affects access to essential services (Temoshok et al., 2025). Biometrics can also fail in unequal ways. NIST research on face recognition documented demographic differentials across algorithms, contexts, and image quality, while Buolamwini and Gebru (2018) found substantial disparities in commercial gender classification systems, with darker-skinned females experiencing error rates up to 34.7% compared with 0.8% for lighter-skinned males. These findings do not mean all biometric systems are equally unreliable. They do mean that biometric claims of accuracy must be evaluated in context, especially when authentication failure can affect access to food, benefits, education, banking, or movement.

India's Aadhaar system is the most frequently studied large-scale biometric identity case. Rao and Nair (2019) describe Aadhaar as India's national biometric identification programme and analyze how it governs through acts of micro-inclusion. Menon's (2018) study of Aadhaar-based biometric authentication for the public distribution system in Ranchi district found that only 52% of ration-card-holding households successfully bought their ration in August 2016, with compulsory biometric authentication contributing to low transaction rates through technical and administrative failures. Carswell and De Neve (2021) similarly show that digital and biometric systems can transform social protection through transparency, exclusion, and mediation. These empirical studies complicate the simple claim that digital identity either includes or excludes. It may do both, depending on design, implementation, alternatives, recourse, infrastructure, and the vulnerability of users.

Masiero (2023) deepens this critique by describing digital identity as platform-mediated surveillance. In this view, the issue is not merely that identity systems have a dark side. Rather, platform architecture itself can enable surveillance outcomes by linking a core identity database to multiple complements and third-party uses. This platform perspective matters because conditional access is rarely built in one step. It emerges gradually through interoperability, API connections, legal mandates, service integration, and normalization. A system introduced for welfare targeting may later become a basis for banking, taxation, policing, telecommunications, health access, education, travel, or platform authentication. This incremental expansion is also consistent with infrastructure theory: systems often become most powerful when their standards, interfaces, and dependencies become ordinary and backgrounded (Star, 1999).

2.4 Data justice, surveillance capitalism, and infrastructural power

Data justice provides a wider framework for evaluating digital identity. Taylor (2017) argues that data justice concerns fairness in how people are made visible, represented, and treated as a result of the digital data they produce. Her three pillars, visibility, engagement with technology, and anti-discrimination, are especially relevant because digital identity systems often promise to make the poor visible to the state. Visibility can be empowering when it enables rights and recognition, but it can become harmful when visibility is compulsory, one-sided, extractive, or punitive.

Surveillance studies and political economy add further depth. Lyon (2009) shows that identity cards and identification systems are embedded in surveillance practices. Zuboff's (2019) account of surveillance capitalism argues that human experience can be converted into behavioral data for prediction and control. Although state digital identity is not identical to surveillance capitalism, the two may interact when public identity systems become linked to private-sector authentication, data brokers, mobile

platforms, financial services, or AI-mediated profiling. The Christian ethical concern is not only privacy invasion, but the deeper question of whether human persons are being reduced to governable data objects whose agency depends on compliance with institutional classification.

Infrastructural power is also crucial. Digital identity becomes powerful not simply because it stores data, but because it becomes embedded in the ordinary conditions of access. Star (1999) argues that infrastructure is often relational, ecological, and mundane, becoming visible especially when it breaks down or excludes users. Infrastructure often becomes invisible when it works, but its power becomes visible when people cannot pass through it. When a person cannot authenticate, cannot appeal, cannot correct data, cannot use an alternative credential, or cannot access a service without biometric verification, identity infrastructure becomes an authority over everyday life. Scott's (1998) account of administrative legibility is useful here because modern governance often simplifies complex social realities into categories that can be counted, monitored, and administered. This is where digital identity becomes a question of dignity rather than merely convenience.

2.5 Christian ethics, theological anthropology, and discernment

Christian ethics begins not with data subjects but with persons created in the image of God. Human dignity is not granted by state recognition, biometric uniqueness, database inclusion, or digital credentials. It is grounded in God's creative act and covenantal knowledge of persons (Gen. 1:26-28; Ps. 139, CSB). This does not make civil registration unimportant. Legal recognition can protect persons from exploitation, statelessness, and exclusion. Yet a Christian anthropology refuses to let administrative identity become ontological identity. A person is not reducible to a number, biometric template, QR code, wallet credential, database record, or risk profile. This claim is consistent with theological accounts of human knowledge and personhood in which the

human creature is known before God prior to all social or administrative recognition (Bavinck, 2003; Frame, 1987).

Christian social epistemology also attends to deception, authority, and institutional trust. Scripture commands believers to test all things and hold on to what is good (1 Thess. 5:21, CSB), to test the spirits (1 John 4:1, CSB), to avoid captivity through deceptive philosophy (Col. 2:8, CSB), and to be wise as serpents and innocent as doves (Matt. 10:16, CSB). These texts do not authorize panic or technological determinism. They require sober testing. Theologically, digital identity should be evaluated through questions of truth, justice, conscience, neighbor-love, stewardship, worship, and coercion.

Revelation 13 is relevant but must be handled with restraint. The text brings together worship, political power, deception, economic participation, and coercive allegiance. It should not be used to label contemporary digital identity systems as the mark of the beast. That would be an overreach. However, the passage legitimately sensitizes Christian ethics to systems where access to buying and selling becomes tied to imposed allegiance. The point is not sensational prediction, but moral vigilance regarding the convergence of identity, authority, economics, worship, and coercion.

3. Theoretical Framework

The theoretical framework integrates Christian social epistemology, critical realism, theological anthropology, public theology, surveillance studies, data justice, and infrastructural power. Christian social epistemology provides the governing posture: digital identity must be evaluated by evidence, institutional mechanisms, moral consequences, theological categories, and humility before God. It refuses both institutional naivety and conspiratorial credulity.

Critical realism provides the philosophical bridge between observed events and underlying mechanisms. Digital identity harm may not appear as

one dramatic act of coercion. They may emerge from mechanisms such as database centralization, unique identifiers, interoperability mandates, biometric failure, vendor contracts, weak appeals, institutional dependency, or data sharing across agencies. Critical realism allows the study to identify mechanisms without assuming centralized malicious intent. It also supports fallibilism: claims about mechanisms must remain open to revision when better evidence appears (Bhaskar, 2008).

Theological anthropology grounds the article's normative claim that human dignity precedes administrative recognition. Public theology frames digital identity as a public moral issue rather than a private religious concern. Surveillance studies show how identity systems can produce visibility, classification, and control. Data justice clarifies how digital systems affect recognition, representation, anti-discrimination, and the freedom not to be compulsorily datafied (Taylor, 2017). Infrastructural power explains how technical systems become politically significant when they mediate ordinary access to essential goods.

The framework evaluates digital identity through five questions. What is documented? How does the system operate? Who benefits and who is exposed? What rival explanations exist? How should Christians interpret and respond in light of Scripture? These questions protect the analysis from overclaiming while allowing serious critique.

4. Methodology

4.1 Research design

This article uses a secondary-data qualitative design combining comparative documentary analysis, critical realist synthesis, policy analysis, conceptual analysis, and biblical-theological reflection. This design is appropriate because the article examines policy frameworks, institutional claims, legal texts, academic literature, and theological meanings rather than collecting new empirical data from participants.

Documentary analysis is suitable because policy documents, institutional reports, legal instruments, and public frameworks reveal how digital identity is justified, governed, constrained, and contested (Bowen, 2009). Conceptual analysis clarifies contested terms such as digital identity, conditional access, surveillance infrastructure, data justice, and human dignity. Critical realist synthesis identifies mechanisms that may generate exclusion, surveillance, dependency, or accountability. Biblical-theological reflection evaluates documented realities through Scripture and Christian doctrine.

4.2 Document corpus and selection criteria

The document corpus was built from five source categories: peer-reviewed academic literature, official institutional reports, legal and policy texts, human-rights and civil-society analyses, and Christian theological sources. Inclusion criteria were relevance to digital identity, biometrics, digital public infrastructure, surveillance, data justice, platform governance, human rights, public-service access, or Christian ethics; institutional credibility or peer-review status; availability of a stable DOI or official URL where possible; and relevance to the article's research questions. The design follows guidance for conceptual scholarship in which the contribution lies in clarifying a focal phenomenon, integrating theoretical domains, and proposing a framework for further empirical testing (Jaakkola, 2020). Exclusion criteria were anonymous claims, sensational or unverifiable sources, partisan commentary without analytical value, and materials that make strong claims about digital identity without evidence or methodological transparency.

Table 2. Document corpus and analytical role

Corpus category	Illustrative sources	Analytical role
Development and digital public infrastructure policy	World Bank ID4D/G2Px; UN Global Digital Compact; Universal DPI Safeguards Framework; African Union digital strategy	Identifies policy framings, benefits, governance commitments, and safeguards.
Legal frameworks	EU Digital Identity Framework Regulation; data protection and rights instruments where relevant	Shows how rights, control, interoperability, and cross-border reliance are encoded in law.
Academic literature	Digital identity, biometrics, data justice, surveillance studies, social protection, platform governance	Provides peer-reviewed evidence and theoretical lenses.
Civil-society and human-rights analysis	Access Now and rights-focused digital ID resources	Highlights risks, mandatory-use concerns, exclusion, and autonomy.
Theological sources	Scripture, Christian epistemology, theological anthropology, public theology	Provides normative criteria concerning dignity, truth, conscience, worship, and moral agency.

Note. The corpus was selected to balance institutional, legal, academic, civil-society, and theological perspectives.

4.3 Analytical procedure

The analysis proceeded in five steps. First, policy and development documents were examined to identify dominant framings of digital identity as inclusion, efficiency, security, trust, resilience, interoperability, and innovation. Second, academic and human-rights literature was reviewed to identify documented risks, including exclusion, privacy vulnerability, surveillance, biometric error, function creep, and weak recourse. Third, critical realist synthesis was used to distinguish observed outcomes from underlying mechanisms. Fourth, rival explanations were considered, including development needs, fraud reduction, administrative modernization, crisis governance, market incentives, bureaucratic rationalization, ideological convergence, and intentional control. Fifth, biblical-theological reflection interpreted the findings through human dignity, conscience, truth, stewardship, worship, and warnings concerning coercive allegiance.

The method deliberately avoids adjudicating whether any specific digital identity system is eschatologically final or inherently malicious. The purpose is to construct a disciplined evaluative framework for Christian and public-policy analysis. The article distinguishes verified evidence, documented patterns, plausible inference, contested interpretation, and theological discernment. This distinction is essential for avoiding both technocratic optimism and fear-driven speculation. As a

conceptual-documentary study, the framework should be read as a theory-building contribution that clarifies mechanisms, normative criteria, and future empirical test points rather than as a substitute for fieldwork (Bowen, 2009; Jaakkola, 2020). Figure 3 operationalizes the layered discernment model used to move from empirical documentation to ethical and biblical-theological evaluation.

Ten-Level Layered Discernment Model Applied to Digital Identity

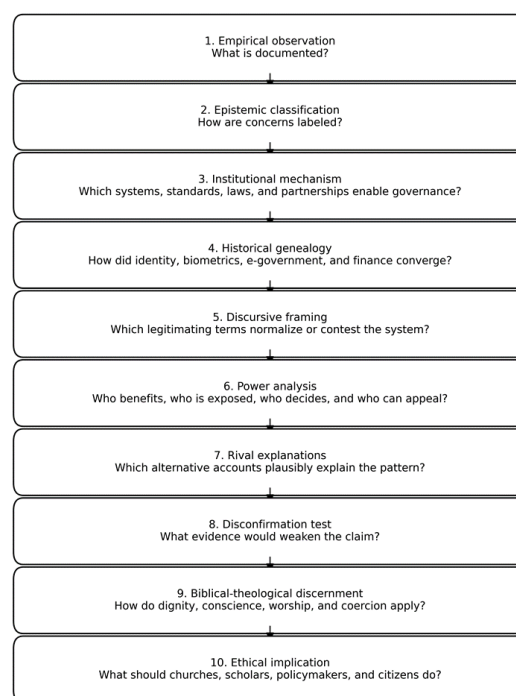


Figure 3. Ten-level layered discernment model applied to digital identity. Author's synthesis from Christian social epistemology,

critical realism, policy analysis, and biblical-theological discernment (Bhaskar, 2008; Jaakkola, 2020).

5. Findings and Thematic Analysis

Figure 4 provides the article’s evaluative matrix for distinguishing rights-respecting inclusion from conditional-access infrastructure. The matrix underscores a central claim of the study: digital identity should not be judged by digitization alone, but by the relation between safeguards, voluntariness, cross-sectoral integration, and the availability of meaningful alternatives.

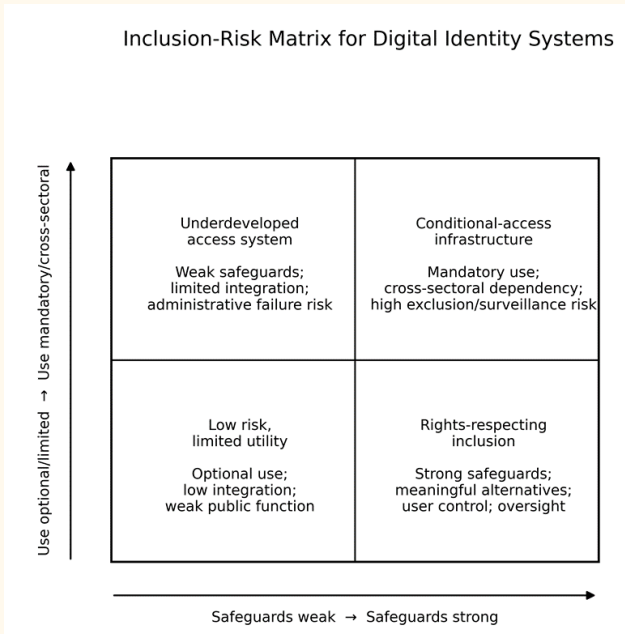


Figure 4. Inclusion-risk matrix for digital identity systems. Author’s synthesis from World Bank ID4D principles, the Universal DPI Safeguards Framework, and the article’s Christian social-epistemological analysis (UNDP & OSET, 2024; World Bank, n.d.-b).

5.1 Digital identity as inclusion and administrative infrastructure

The first finding is that digital identity systems respond to genuine problems of exclusion and administrative weakness. The absence of recognized identity can prevent people from accessing services, rights, opportunities, and protection. The latest World Bank data indicate that more than 800 million people

lack official proof of identity, while 2.8 billion lacked access to digital ID systems for online transactions in 2024 (Pswarayi-Riddihough et al., 2025). In contexts where paper systems are fragmented, lost, inaccessible, or easily forged, digital identity can improve portability, reduce duplication, support birth registration, enable welfare transfers, and facilitate financial inclusion.

Digital identity is also increasingly embedded within digital public infrastructure. Digital public infrastructure is commonly described as a set of reusable digital systems that support identity, payments, and data exchange across public and private services. The Global Digital Compact recognizes resilient, safe, inclusive, and interoperable digital public infrastructure as potentially beneficial for delivering services at scale and increasing social and economic opportunities (United Nations General Assembly, 2024). The EU Digital Identity Wallet represents a high-regulation model that emphasizes user control, selective disclosure, cross-border recognition, open-source components, pseudonyms, transaction logs, and interoperability (European Parliament & Council of the European Union, 2024). These features show that digital identity can be designed with rights-protective goals.

A Christian policy analysis should therefore avoid dismissing digital identity as merely oppressive. Identification can protect the vulnerable when it enables recognition, access, and accountability. The poor, refugees, stateless persons, rural populations, migrants, and people without birth certificates may be harmed when the state cannot recognize them. Legal identity can serve justice when it enables persons to claim rights and participate in society. The first ethical question is not whether identity systems should exist, but whether they serve persons rather than reducing persons to administrative objects.

Table 3. Selected evidence points for inclusion, access, and exclusion

Evidence area	Key data or claim	Source	Analytical significance
Global ID gap	More than 800 million people lack official proof of identity.	Pswarayi-Riddihouh et al. (2025); World Bank (n.d.-a)	Supports the inclusion rationale.
Digital ID capability gap	2.8 billion people lacked access to digital ID systems for online transactions in 2024.	Pswarayi-Riddihouh et al. (2025)	Shows that online digital identity is a separate gap from basic ID.
DPI scale	World Bank ID4D/G2Px reports supporting more than 60 countries and helping issue inclusive, secure, user-centered digital IDs to 550 million people.	World Bank (2023)	Shows institutional scale of DPI initiatives.
EU wallet	EU law establishes a European Digital Identity Wallet framework emphasizing user control, selective disclosure, pseudonyms, transaction logs, and cross-border access.	European Parliament & Council of the European Union (2024)	Illustrates a highly regulated design model.
Aadhaar exclusion evidence	In one Ranchi district study, only 52% of ration-card-holding households successfully bought their ration during the observed period; biometric authentication contributed to low transactions.	Menon (2018)	Shows implementation risk when ID is tied to welfare access.

Note. The table distinguishes documented evidence from broader interpretation. It does not imply that all systems produce the same outcomes.

5.2 Digital identity as surveillance and dependency infrastructure

The second finding is that digital identity can become a surveillance and dependency infrastructure when design choices intensify data concentration, interoperability, and mandatory verification. Digital systems amplify risks because data can be copied, linked, queried, retained, breached, repurposed, and analyzed at scale. Such amplification is central to datafication and dataveillance, where data generated for one purpose may become part of broader systems of observation, prediction, and governance (van Dijck, 2014; Zuboff, 2019). The World Bank's own guidance identifies risks associated with centralized databases, unique identifiers across systems, biometrics, data sharing, metadata tracking, surveillance, and function creep (World Bank, n.d.-c). These concerns are not speculative; they are recognized by mainstream development institutions.

Digital identity's surveillance capacity increases when identity credentials become platform-like. A foundational ID database may begin as a registry, but it becomes more powerful when connected to banking, telecommunications, taxation, welfare,

border control, health, education, and payments. Masiero (2023) argues that a platform view is essential because digital identity systems can construct complements around a core identity infrastructure, creating surveillance outcomes through architecture rather than a single explicit surveillance policy. This is a critical insight: conditional governance may emerge from interoperability, not only intention. Infrastructure studies similarly show that social power can be embedded in standards, interfaces, routines, and dependencies without requiring a single centralized actor (Bowker & Star, 1999; Star, 1999).

Dependency also matters. When a digital ID becomes the trusted source of identity across multiple services, citizens become dependent on the system's uptime, accuracy, appeal mechanisms, vendor contracts, cybersecurity posture, and bureaucratic discretion. A person wrongly excluded, mismatched, or unable to authenticate may face cascading consequences. The question is not only whether data are collected, but whether the person has meaningful agency, correction rights, alternatives, and recourse.

5.3 Conditional access and exclusion

The third finding is that digital identity becomes morally acute when it functions as a condition for access to essential services. Conditional access occurs when participation in welfare, banking, healthcare, schooling, mobile connectivity, transport, travel, employment, public services, or online platforms depends on successful identity verification. Conditional access is not always wrong. Some services require authentication for legitimate reasons. However, the moral risk increases when the condition is mandatory, biometric, failure-prone, difficult to appeal, and attached to necessities of life. This is why the Universal DPI Safeguards Framework states that access should not become limiting, conditional, or mandatory, explicitly or in practice, and calls for digital and non-digital channels (UNDP & OSET, 2024).

Empirical literature from India illustrates this risk. Menon (2018) found that compulsory Aadhaar-based biometric authentication contributed to low ration transactions in Ranchi district, with incomplete seeding, biometric failure, administrative gaps, and inadequate backup systems affecting access to food entitlements. Carswell and De Neve (2021) show that digital and biometric systems can mediate social protection in ways that produce both transparency

and exclusion. These studies do not prove that all biometric systems are excluded. They show that inclusion claims must be tested against implementation realities, especially among elderly persons, manual laborers, people with disabilities, rural users, and those with limited digital access.

Conditional access also appears in policy design beyond welfare. The EU Digital Identity Wallet framework anticipates uses in transport, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education, and telecommunications where strong user authentication is legally or contractually required (European Parliament & Council of the European Union, 2024). The EU framework emphasizes voluntary user request, selective disclosure, and control; these safeguards matter. Yet the breadth of potential service domains illustrates why digital identity should be evaluated as infrastructure. Where identity credentials become the gate to multiple sectors, safeguards are not secondary. They are morally constitutive. Figure 5 traces how identity-mediated service delivery can move from verification to exclusion when fallback systems, human review, or appeal mechanisms are absent.

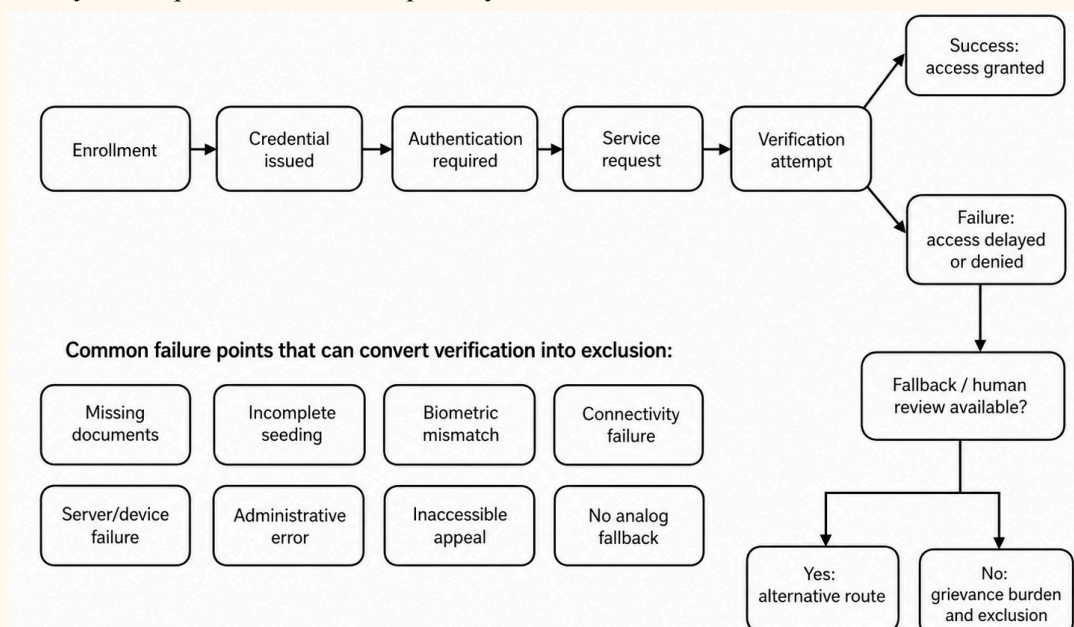


Figure 5. Conditional access and exclusion pathway. Author's synthesis from Menon's (2018) study of Aadhaar-based biometric authentication in Ranchi district and the article's policy analysis of conditional access.

5.4 Discursive framing and legitimacy

The fourth finding is that digital identity is legitimated through morally attractive language. This concern is consistent with scholarship on datafication and digital governance, which warns that terms such as trust, efficiency, and innovation can carry normative assumptions about what should count as legitimate social ordering (van Dijck, 2014). Policy documents frequently invoke inclusion, trust, safety, resilience, empowerment, innovation, interoperability, convenience, and fraud prevention. These words often describe real goods. Inclusion matters. Fraud prevention matters. Secure authentication matters. The problem is not the vocabulary itself. The problem arises when morally attractive language prevents examination of trade-offs, coercive effects, or structural vulnerabilities.

The Global Digital Compact frames digital public infrastructure as a driver of inclusion and development while also recognizing risks, human-rights obligations, and the need for safeguards (United Nations General Assembly, 2024). The Universal DPI Safeguards Framework similarly emphasizes safe and inclusive DPI, identifying risks and pathways for legal, institutional, technical, capacity, and whole-of-society safeguards (UNDP & OSET, 2024). Regulation (EU) 2024/1183 requires European Digital Identity Wallets to enable user control, selective disclosure, pseudonyms, transaction logs, data download where feasible, and source-code disclosure for wallet software components subject to defined limits (European Parliament & Council of the European Union, 2024). These discourses are not empty. They show growing awareness that legitimacy depends on trust, rights, and safeguards.

Yet legitimacy language can still conceal asymmetry. A person may be told that a system empowers them while having no realistic ability to opt out. A system may promise trust while requiring citizens to trust opaque institutions. A system may promise

convenience while making alternative access routes disappear. A Christian social-epistemological analysis therefore asks: Who defines the good? Who controls the infrastructure? Who can contest errors? Who benefits from data linkage? Who bears the risk when the system fails?

5.5 Data sovereignty, human rights, and institutional accountability

The fifth finding is that digital identity requires accountability across legal, technical, institutional, and theological levels. Data protection is necessary, but insufficient. Privacy rules may protect individual data transactions while leaving wider structural risks, group harms, and infrastructural dependencies insufficiently addressed (Taylor, 2017; Wodajo, 2024). A system may comply formally with privacy rules while still producing exclusion, dependency, or unjust profiling. Accountability must include data minimization, purpose limitation, cybersecurity, independent oversight, transparency, accessible correction, alternatives to digital or biometric authentication, proportionality, procurement accountability, vendor neutrality, and remedies for harm.

The Principles on Identification for Sustainable Development provide a useful policy baseline. They call for universal coverage without discrimination, removal of barriers, robust and secure identity, interoperability, open standards, vendor neutrality, user privacy and control, sustainability without compromising accessibility, legal safeguards, accountability, independent oversight, and adjudication of grievances (World Bank, n.d.-b). These principles are important because they show that a responsible pro-identification position must include safeguards, not merely enrollment targets. Figure 6 translates the article's policy and theological argument into a safeguard architecture for rights-respecting digital identity.

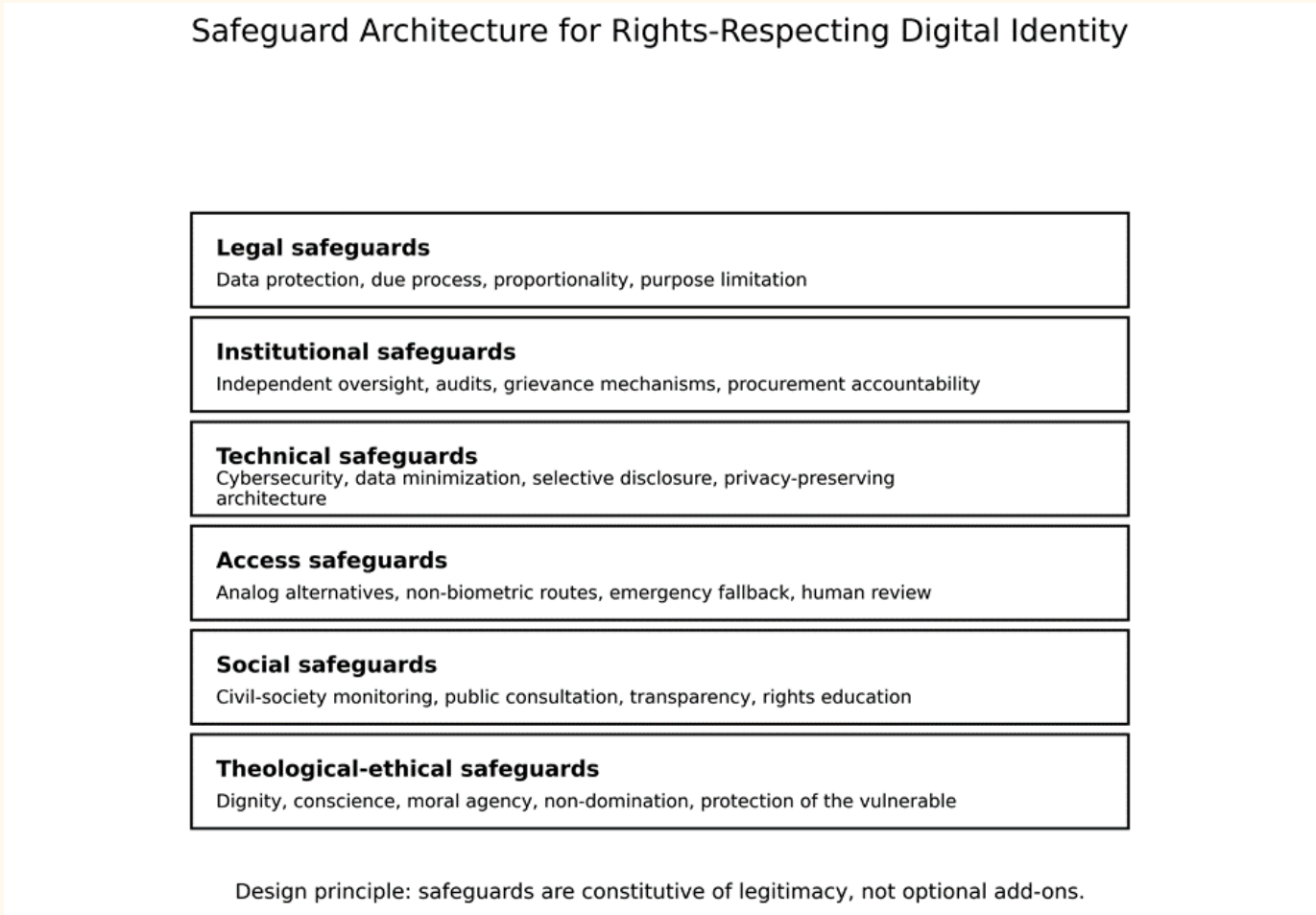


Figure 6. Safeguard architecture for rights-respecting digital identity. *Author's synthesis from the Universal DPI Safeguards Framework, EU Digital Identity Framework, World Bank ID4D principles, and Christian public ethics (European Parliament & Council of the European Union, 2024; UNDP & OSET, 2024; World Bank, n.d.-b).*

Human rights scholarship adds that digital identity systems must be evaluated by their effects on privacy, non-discrimination, autonomy, and social participation (Beduschi, 2019; Wodajo, 2024). Data justice adds that fairness concerns how people are made visible, represented, and treated by data systems (Taylor, 2017). Christian ethics adds that accountability is not merely procedural. It concerns whether institutions honor persons as image-bearers, protect the vulnerable, preserve conscience, refuse domination, and remain answerable to truth.

5.6 Rival explanations and disconfirmation

The sixth finding is methodological. Digital identity critique must distinguish between different explanations for the same pattern. A welfare authentication failure may result from coercive intent,

but it may also result from poor connectivity, weak training, outdated biometric capture, low-quality devices, bureaucratic neglect, procurement failures, or inadequate grievance mechanisms. A global emphasis on digital public infrastructure may indicate technocratic convergence, but it may also reflect lessons from pandemic-era service delivery, financial inclusion goals, interoperability needs, or donor coordination. A Christian scholar must not treat every pattern as proof of malicious design. Critical realism supports this caution by distinguishing observable events from underlying mechanisms and by requiring fallible, revisable explanation rather than immediate causal closure (Bhaskar, 2008).

Rival explanations are ethically necessary because accusations concerning surveillance, control, or coercion can harm reputations and public trust. The

responsible posture is to ask what evidence would weaken stronger claims. Claims about coercive control would be weakened if systems remain optional, analog alternatives remain meaningful, data are decentralized or minimized, independent oversight is effective, appeal mechanisms work, audits are public, and service denial is prohibited when authentication fails. This criterion is consistent with DPI safeguards requiring effective remedy and redress, non-exclusion, non-discrimination, and user agency (UNDP & OSET, 2024). Claims about mere administrative neutrality would be weakened if digital identity becomes mandatory across essential

sectors, biometric alternatives disappear, data sharing expands beyond original purposes, vendors control core infrastructure, error correction is inaccessible, and dissenting concerns are classified as misinformation without examination.

This disconfirmation logic is central to disciplined discernment. It allows the article to take risks seriously without overstating causality. It also prevents institutions from dismissing concerns as conspiratorial when the concerns are grounded in architecture, incentives, and documented harms.

Table 4. Rival explanations and disconfirmation tests

Observed issue	Possible explanations	Disconfirmation or clarification test
Inclusion failure	Weak connectivity, device failure, incomplete registration, bureaucratic neglect, biometric mismatch, or intentional exclusion.	Examine logs, error rates, fallback use, grievance records, and user testimony.
Data concentration	Efficiency, interoperability, vendor architecture, security logic, or deliberate centralization of power.	Review legal mandates, procurement, data-sharing agreements, and architecture.
Policy convergence	Learning, donor coordination, crisis governance, market incentives, technocratic ideology, or coordinated control.	Compare timelines, documents, funding flows, and independent policy origins.
Conditional access	Fraud prevention, risk management, legal compliance, commercial convenience, or coercive compliance.	Assess voluntariness, alternatives, essential-service links, appeals, and proportionality.
Theological interpretation	Documented moral pattern, speculative symbolism, genuine spiritual deception, or overextended eschatology.	Apply Scripture after empirical analysis; identify what would revise the claim.

Note. Responsible Christian analysis should test rival explanations before moving from pattern to accusation or theological interpretation. The table draws on critical realist explanation, documentary policy analysis, and the article's layered discernment framework (Bhaskar, 2008; Bowen, 2009).

5.7 Biblical-theological discernment

The seventh finding is that digital identity raises theological questions because it concerns recognition, naming, embodiment, authority, conscience, worship, and economic participation. Scripture affirms that human beings are made in the image of God (Gen. 1:26-28, CSB). Human dignity is therefore prior to state recognition and cannot be reduced to administrative legibility. Psalm 139 presents divine knowledge of the person as intimate, creative, and covenantal, unlike bureaucratic knowledge that classifies from outside.

This does not mean state identification is wrong. Scripture recognizes the legitimate role of public authority in ordering common life (Rom. 13:1-7,

CSB), and administrative numbering appears in biblical narratives. Christian political theology has long distinguished legitimate public authority from idolatrous or absolutized authority, a distinction that is crucial when administrative systems become conditions of participation (O'Donovan, 1996). Yet Scripture also warns against systems that reduce persons to instruments of imperial power, economic control, or idolatrous allegiance. The theological question is not whether a number exists, but what authority the number serves, whether it protects or dominates, whether it honors the vulnerable, and whether access to life's necessities becomes bound to coercive conformity.

Revelation 13 should therefore be used with sobriety. It does not authorize careless identification of current

technologies with final eschatological fulfillment. However, it does reveal that beastly power can unite worship, political authority, deception, image, and economic exclusion. Digital identity systems should be assessed in light of that warning when they connect identity, access, compliance, and economic participation. The Christian concern is not technological novelty but moral allegiance: whether systems train persons to accept conditional participation as normal, unavoidable, and beyond moral question.

6. Discussion

The analysis shows that digital identity is best understood as a morally ambivalent infrastructure. Its benefits are genuine where it enables legal recognition, portability, service delivery, financial inclusion, and protection for people previously excluded. Its risks are genuine where it creates biometric dependency, function creep, surveillance capacity, data concentration, algorithmic exclusion, weak recourse, and mandatory access conditions. The Christian contribution is not to choose a simplistic side, but to insist that infrastructures be tested by truth, dignity, justice, and worship.

The article's first contribution is conceptual. It shifts the debate from digital identity as a tool to digital identity as identity-mediated governance. A tool can be used or not used. Infrastructure reorganizes the environment in which agency becomes possible. This claim reflects a wider tradition in science and technology studies that treats artifacts and infrastructures as politically significant because they configure possibilities for action, dependency, and participation (Star, 1999; Winner, 1980). When digital identity becomes infrastructure, the moral question changes from "Is this convenient?" to "What forms of participation, dependency, visibility, and authority does this system create?"

The second contribution is methodological. By applying a layered discernment model, the article distinguishes empirical observation from theological

interpretation. It can affirm verified evidence such as the global ID gap, documented patterns such as biometric exclusion, plausible inferences about function creep, contested interpretations about surveillance intent, and theological discernment concerning dignity and allegiance. This prevents both technological optimism and speculative accusation.

The third contribution is theological. The article argues that Christian ethics must evaluate digital identity through the image of God, conscience, truth, stewardship, neighbor-love, justice, and warnings concerning idolatrous power. The point is not to baptize privacy liberalism with religious language. It is to insist that persons belong first to God, not to administrative systems. Identity systems may serve people, but they must never become the measure of personhood or the unappealable gate to social existence.

The fourth contribution is policy-oriented. The article identifies criteria for responsible digital identity: meaningful alternatives, proportionality, data minimization, selective disclosure, decentralized or privacy-preserving architectures where possible, independent oversight, public audits, accessible correction, non-discrimination, cybersecurity, vendor accountability, and protection from service denial when authentication fails. These criteria are consistent with World Bank ID principles, the Universal DPI Safeguards Framework, and the EU Digital Identity Framework's emphasis on user control and selective disclosure (European Parliament & Council of the European Union, 2024; UNDP & OSET, 2024; World Bank, n.d.-b). These safeguards are deepened, in this article, by Christian concern for the vulnerable, truthful witness, and resistance to coercive allegiance.

7. Implications for Church, Academy, Policy, and Society

7.1 Implications for the church

Churches should teach digital discernment as part of discipleship. Digital identity debates are often handled either with fear or silence. Both are

insufficient. Congregations need formation in how to evaluate technological systems, distinguish evidence from speculation, recognize real public goods, identify risks to the vulnerable, and resist false witness. Pastors should avoid declaring every digital ID initiative apocalyptic, but they should also avoid treating identity-mediated access as morally neutral. Churches should advocate for people who are excluded by identification systems, especially the poor, elderly, displaced, disabled, rural, stateless, and digitally marginalized. World Bank data show that identity gaps remain concentrated among marginalized and vulnerable groups, including children without birth registration, women in low-income countries, rural populations, and poorer adults (Pswarayi-Riddihough et al., 2025; World Bank, n.d.-a).

7.2 Implications for theological education

Seminaries and Christian universities should integrate technology ethics, social epistemology, public theology, media literacy, and digital governance into ministerial and leadership formation. This curricular need follows from the article's claim that digital governance is now a public-theological issue, not merely a technical specialization. Future pastors and Christian scholars must understand digital public infrastructure, biometric governance, AI-mediated classification, data justice, and platform power. Apologetics in the digital age must include not only defense of doctrine but also formation in truth, evidence, public reason, and moral courage.

7.3 Implications for the academy

Scholars should study digital identity without dismissing concerns as irrational or accepting them uncritically. Research should examine concrete systems, legal frameworks, vendor arrangements, failure rates, appeals, data-sharing agreements, and lived experience. The academy should support interdisciplinary work that brings together law,

information systems, theology, surveillance studies, development studies, and political philosophy. Christian scholarship can contribute by articulating a thicker account of dignity, conscience, worship, and moral agency than is often available in technical policy discourse.

7.4 Implications for policy

Policymakers should treat safeguards as constitutive rather than optional. A digital identity system should not be considered successful merely because enrollment numbers are high. Success should also be measured by equitable access, low exclusion rates, correction speed, user understanding, opt-out possibilities, availability of analog alternatives, independent oversight, breach response, auditability, and non-discrimination. Mandatory biometric systems should face especially high justification burdens because biometric systems can create persistent, difficult-to-remediate risks when they are mandatory, centralized, or linked to essential services (Beduschi, 2019; Grother et al., 2019; World Bank, n.d.-c; Wodajo, 2024). Where digital identity is linked to essential services, denial of service due to authentication failure should be prohibited unless alternative verification and emergency recourse are available.

Public authorities should also avoid framing concerns as misinformation simply because they challenge digital-transformation agendas. Some claims will be false or exaggerated, but many concerns are grounded in documented risks acknowledged by mainstream institutions. Trust is strengthened not by demanding compliance, but by practicing transparency, contestability, and accountability. This aligns with DPI safeguards calling for transparency, accountability, effective remedy, public oversight, and participatory governance across the DPI lifecycle (UNDP & OSET, 2024).

Table 5. Normative criteria for ethically responsible digital identity

Criterion	Policy meaning	Christian-social-epistemological test
Human dignity	Treat identity as a service to persons, not a measure of personhood.	Avoid exclusion where authentication fails; preserve human review.
Proportionality	Collect and use only what is necessary for a legitimate purpose.	Reject excessive data collection and indefinite retention.
Plural access	Maintain meaningful alternatives, including analog or non-biometric routes.	Prevent mandatory digital ID from becoming a single point of social failure.
User control	Enable selective disclosure, consent clarity, logs, correction, and portability.	Make control practical, not merely rhetorical.
Accountability	Ensure independent oversight, public audit, appeal, redress, and vendor transparency.	Build trust through verifiable accountability rather than demands for compliance.
Theological restraint	Do not overstate eschatological claims; do not ignore coercive patterns.	Interpret Revelation 13 as a moral warning about allegiance and economic coercion, not as a shortcut to prediction.

Note. The criteria translate policy safeguards into a Christian ethical vocabulary centered on dignity, truth, conscience, and accountable power.

7.5 Implications for society

Citizens should resist both passive adoption and reflexive rejection. A healthy public sphere requires informed debate about identity, privacy, inclusion, access, and power. Civil society should monitor implementation, document exclusion, demand alternatives, and defend vulnerable populations. Digital identity will shape the conditions of participation in the coming decades. It should therefore be governed not only by engineers, vendors, and administrators, but by a whole-of-society conversation about dignity, justice, and freedom. The Universal DPI Safeguards Framework likewise treats DPI governance as requiring a whole-of-society approach rather than a purely technical or administrative process (UNDP & OSET, 2024).

8. Limitations

This article has several limitations. First, it is conceptual and documentary rather than based on original fieldwork. It synthesizes existing literature and policy documents but does not collect interviews, survey data, or ethnographic observations from users of digital identity systems. Second, the comparative scope is broad; the article analyzes digital identity as a global governance phenomenon rather than providing a detailed case study of one country. Third, the biblical-theological reflection is constructive

rather than exhaustive. Each biblical theme, including the image of God, conscience, idolatry, and Revelation 13, deserves fuller treatment. Fourth, the article's Christian worldview may limit reception in some secular journals, although its policy and ethical arguments are intended to be intelligible beyond confessional contexts. Fifth, evidence concerning future forms of conditional access remains partly inferential. The article therefore distinguishes documented realities from plausible risks and contested interpretations.

9. Recommendations for Future Research

Future research should apply the framework to specific digital identity systems through comparative case studies. Suitable cases include Aadhaar, the EU Digital Identity Wallet, national digital ID systems in Africa, refugee biometric registration, SIM registration regimes, and digital identity-linked social protection systems. UNHCR's Biometric Identity Management System captures fingerprints, iris images, and facial photographs for biometric enrollment of refugees and stores them in a centralized consolidated database to support globally unique identity management (United Nations High Commissioner for Refugees, 2023). Each case should examine enrollment procedures, biometric dependencies, authentication failure, data-sharing

arrangements, legal safeguards, appeal mechanisms, and user experience.

Second, empirical research should study Christian communities' perceptions of digital identity. Interviews and focus groups could examine how pastors, theologians, educators, and lay Christians distinguish biblical discernment from fear-driven speculation. Third, policy research should examine how digital identity interacts with CBDCs, programmable payments, financial compliance, and platform access. Fourth, theological research should develop a fuller doctrine of administrative identity, exploring naming, numbering, embodiment, state authority, conscience, and worship. Fifth, technical research should evaluate privacy-preserving alternatives, decentralized credentials, selective disclosure, zero-knowledge proofs, and analog fallback systems from the perspective of justice for vulnerable users. Regulation (EU) 2024/1183 is relevant here because it embeds selective disclosure, pseudonyms, and transaction logs into the European Digital Identity Wallet framework, while NIST digital identity guidance emphasizes backup or alternate authenticators when authentication mechanisms are compromised or unavailable (European Parliament & Council of the European Union, 2024; Temoshok et al., 2025).

10. Conclusion

Digital identity is becoming one of the most consequential infrastructures of the twenty-first century. It promises recognition, inclusion, efficiency, fraud reduction, and access to digital services. These goods should not be dismissed. Yet digital identity also raises serious risks concerning surveillance, exclusion, data concentration, function creep, dependency, and conditional participation. These risks should not be minimized.

This article has argued for a Christian social-epistemological and policy analysis that evaluates digital identity through disciplined discernment. Such discernment begins with evidence, asks how systems operate, considers rival

explanations, tests claims, and interprets documented realities under Scripture. It refuses institutional naivety because human institutions are morally vulnerable. It refuses conspiratorial credulity because false witness remains sin, even when directed against powerful actors.

Theologically, the human person is not a database record. Human dignity is grounded in the image of God, not in biometric uniqueness or digital verification. Identification systems may serve justice when they protect and include. They become morally dangerous when they convert access to life's necessities into a function of opaque, mandatory, and unappealable credentials. Revelation 13 should not be used carelessly, but it rightly sensitizes Christians to the convergence of authority, worship, deception, and economic exclusion.

The task before churches, scholars, and policymakers is therefore not to reject every digital identity system, nor to accept every system in the name of progress. The task is to insist that identity infrastructures remain accountable to truth, dignity, justice, conscience, and the common good. Digital identity must serve persons. It must never become the measure of personhood.

Declarations

Conflict of Interest: The author declares no conflict of interest.

Funding: This research received no external funding.

Data Availability Statement: Data sharing is not applicable because no empirical datasets were generated or analyzed. The article is based on published academic literature, policy documents, institutional reports, legal texts, and biblical texts cited in the reference list.

AI Use Statement: Generative AI was used only for editorial assistance, source organization, language refinement, and manuscript-polishing support. The author reviewed, verified, revised, and approved the final manuscript and remains fully responsible for its content, argumentation, citations, and conclusions.

References

- Access Now. (n.d.). Digital identity. Retrieved May 2, 2026, from <https://www.accessnow.org/issue/digital-identity/>
- African Union. (2020). The digital transformation strategy for Africa (2020-2030). <https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030>
- Bavinck, H. (2003). Reformed dogmatics: Vol. 1. Prolegomena (J. Vriend, Trans.; J. Bolt, Ed.). Baker Academic. (Original work published 1895)
- Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, 6(2), 1-6. <https://doi.org/10.1177/2053951719855091>
- Bhaskar, R. (2008). A realist theory of science. Routledge. <https://doi.org/10.4324/9780203090732>
- Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal*, 9(2), 27-40. <https://doi.org/10.3316/QRJ0902027>
- Bowker, G. C., & Star, S. L. (1999). Sorting things out: Classification and its consequences. MIT Press. <https://doi.org/10.7551/mitpress/6352.001.0001>
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 77-91. <https://proceedings.mlr.press/v81/buolamwini18a.html>
- Carswell, G., & De Neve, G. (2021). Transparency, exclusion and mediation: How digital and biometric technologies are transforming social protection in Tamil Nadu, India. *Oxford Development Studies*, 49(2), 126-141. <https://doi.org/10.1080/13600818.2021.1904866>
- Christian Standard Bible. (2020). Holman Bible Publishers. <https://www.biblegateway.com/versions/Christian-Standard-Bible-CSB/>
- Clark, J., Metz, A., & Casher, C. (2022). ID4D global dataset 2021, volume 1: Global ID coverage estimates. World Bank. <https://hdl.handle.net/10986/38440>
- European Commission. (n.d.). European digital identity. Retrieved May 2, 2026, from https://commission.europa.eu/topics/digital-economy-and-society/european-digital-identity_en
- European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. Official Journal of the European Union. <http://data.europa.eu/eli/reg/2024/1183/oj>
- Frame, J. M. (1987). The doctrine of the knowledge of God. P&R Publishing.
- Grother, P., Ngan, M., & Hanaoka, K. (2019). Face Recognition Vendor Test (FRVT) part 3: Demographic effects (NISTIR 8280). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8280>
- Jaakkola, E. (2020). Designing conceptual articles: Four approaches. *AMS Review*, 10, 18-26. <https://doi.org/10.1007/s13162-020-00161-0>
- Lyon, D. (2009). Identifying citizens: ID cards as surveillance. Polity Press.
- Masiero, S. (2023). Digital identity as platform-mediated surveillance. *Big Data & Society*, 10(1), 1-5. <https://doi.org/10.1177/20539517221135176>
- Menon, S. (2018). Aadhaar-based biometric authentication for PDS and food security: Observations on implementation in

- Jharkhand's Ranchi district. *Indian Journal of Human Development*, 11(3), 392-397. <https://doi.org/10.1177/0973703017748384>
- Murphy, K. P., Sun, T., Zhou, Y. S., Tsuda, N., Zhang, N., Budau, V., Solomon, F., Kao, K., Vucinic, M., & Miggiani, K. (2024). Central bank digital currency data use and privacy protection. *IMF Fintech Notes*, 2024(004). <https://doi.org/10.5089/9798400286971.063>
- O'Donovan, O. (1996). *The desire of the nations: Rediscovering the roots of political theology*. Cambridge University Press. <https://doi.org/10.1017/CBO9780511598234>
- Plantinga, A. (2000). *Warranted Christian belief*. Oxford University Press. <https://doi.org/10.1093/0195131932.001.0001>
- Pswarayi-Riddihough, I., Singh, K., Ansar, S., & Wolff, J. (2025, October 30). Global progress in identification: 3 findings from the latest data. *World Bank Blogs*. <https://blogs.worldbank.org/en/digital-development/global-progress-in-identification--3-findings-from-the-latest-da>
- Rao, U., & Nair, V. (2019). Aadhaar: Governing with biometrics. *South Asia: Journal of South Asian Studies*, 42(3), 469-481. <https://doi.org/10.1080/00856401.2019.1595343>
- Sangwa, S. (2025). Global digital identity systems: Interdisciplinary insights into surveillance, governance, and prophetic implications. *Open Journal of Science, Philosophy & Theology*, 1(2). <https://doi.org/10.65655/v186sm55>
- Sangwa, S. (2026). Disciplined discernment and stigmatized knowledge: A Christian social epistemology of conspiracy labels, institutional trust, and knowledge control. *Open Journal of Stigmatized Knowledge & Suppressed Discourses*, 2(1). <https://doi.org/10.65655/OpenChristianPress.2026.110>
- Sangwa, S., & Mutabazi, P. (2025). Programmable CBDCs, digital identity, ISO 20022, and AI: Reconfiguring power in payment infrastructures. *Open Journal of Stewardship Economics & Ethical Innovation*, 1(2). <https://doi.org/10.65655/p0w2r666>
- Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. Yale University Press. <https://yalebooks.yale.edu/book/97803000078152/seeing-like-a-state/>
- Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist*, 43(3), 377-391. <https://doi.org/10.1177/00027649921955326>
- Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, 4(2), 1-14. <https://doi.org/10.1177/2053951717736335>
- Temoshok, D., Choong, Y.-Y., Regenscheid, A., Galluzzo, R., Fenton, J. L., Richer, J., & Lefkovitz, N. (2025). *Digital identity guidelines: Authentication and authenticator management (NIST Special Publication 800-63B-4)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-63B-4>
- United Nations Department of Economic and Social Affairs. (n.d.). Goal 16: Peace, justice and strong institutions. United Nations. Retrieved May 2, 2026, from <https://sdgs.un.org/goals/goal16>
- United Nations Development Programme & Office of the Secretary-General's Envoy on Technology. (2024). *The universal digital public infrastructure safeguards framework: A guide to building safe and inclusive DPI for societies*. <https://safedpi.gitbook.io/safeguards/about-the-universal-dpi-safeguards-initiative/key-outputs/a-guide-to-building-safe-and-inclusive-dpi-for-societies>
- United Nations General Assembly. (2024). *The Pact for the Future: Resolution adopted by the*

- General Assembly (A/RES/79/1).
<https://digitallibrary.un.org/record/4061879>
- United Nations High Commissioner for Refugees. (2023, May 10). UNHCR's biometric tools in 2023.
<https://www.unhcr.org/blogs/unhcrs-biometric-tools-in-2023/>
- Vanhoozer, K. J. (1998). Is there a meaning in this text? The Bible, the reader, and the morality of literary knowledge. Zondervan.
- van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, 12(2), 197-208.
<https://doi.org/10.24908/ss.v12i2.4776>
- Winner, L. (1980). Do artifacts have politics? *Daedalus*, 109(1), 121-136.
<https://www.jstor.org/stable/20024652>
- Wodajo, K. (2024). Societal and structural risks of biometric ID: Towards people's right to privacy. *Bulletin of Science, Technology & Society*, 29(4).
<https://doi.org/10.1177/09717218241281941>
- World Bank. (2023, October 12). Creating digital public infrastructure for empowerment, inclusion, and resilience.
<https://www.worldbank.org/en/results/2023/10/12/creating-digital-public-infrastructure-for-empowerment-inclusion-and-resilience>
- World Bank. (n.d.-a). Data: Identification for Development. Retrieved May 2, 2026, from <https://id4d.worldbank.org/global-dataset>
- World Bank. (n.d.-b). Principles on identification for sustainable development. Retrieved May 2, 2026, from <https://id4d.worldbank.org/guide/1-principles>
- World Bank. (n.d.-c). Assess risks. Identification for Development. Retrieved May 2, 2026, from <https://id4d.worldbank.org/guide/assess-risks>
- Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.