DIGITAL GOVERNANCE INSTITUTE

POWERING THE ENGINE OF INTERNET TRUST

THE INTERNET GOVERNANCE GUIDE

ITS PAST, TODAY AND IDEAS FOR THE FUTURE

SCOTT S. PERRY, CPA, CISA
DIGITAL GOVERNANCE INSTITUTE

TABLE OF CONTENTS

INTRODUCTION

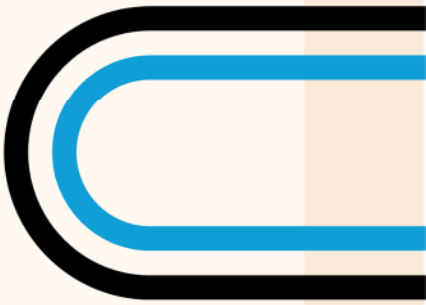
The Internet has grown from a collection of interconnected research networks into a global infrastructure essential for communication, commerce, and knowledge exchange. Governance of the Internet is essential in shaping its usage, accessibility, security, and alignment with societal values. As technological innovations continue to emerge, governance frameworks must adapt to address new challenges and opportunities.

This whitepaper aims to serve as a foundational document that I hope will spark discussions and action among stakeholders involved in Internet governance, ultimately striving for an equitable and secure digital future.

The document examines the historical evolution of Internet governance, detailing its initial frameworks, contemporary governance structures, and prospective future models. It emphasizes the transition from a decentralized approach managed by academic and governmental stakeholders to a more complex, multi-stakeholder ecosystem that incorporates the private sector, civil society, and international entities. It outlines current challenges in governance and proposes solutions aimed at fostering an inclusive, secure, and resilient Internet.

Please read on to learn more about the history, the current structures and ideas for future Internet governance. Please contact us at the Digital Governance Institute at info@digitalgovernanceinstitute.com to open a dialogue about your specific needs or questions.

EXECUTIVE SUMMARY



The Internet Governance Guide provides a comprehensive overview of the internet's governance, from its early days to the present, and offers insights into potential future directions. The internet has evolved from a research network (ARPANET) to a global infrastructure vital for communication, commerce, and knowledge exchange. The internet's governance has transitioned from a decentralized, community-driven approach to a more complex multi-stakeholder ecosystem2. This ecosystem involves governments, the private sector, civil society, and international entities.

Early Governance

- **ARPANET (late 1960s):** Funded by the U.S. Department of Defense, ARPANET's governance was informal, relying on researcher collaboration3. Key figures like Bob Taylor and Larry Roberts led the initiative.
- **Request for Comments (RFC) Series (1969):** Technical and organizational documents about the internet, evolving from informal notes to official standards and best practices.
- **Internet Assigned Numbers Authority (IANA) (1972):** Initially managed by Jon Postel, IANA manages IP addresses, the DNS root zone, and autonomous system numbers789.
- **Emergence of ICANN (1998):** ICANN was established to manage domain names and IP address distribution, marking a shift toward a more structured governance model910.

Contemporary Governance Structures

- **Multi-stakeholder Model:** Involves governments, the private sector, civil society, and technical communities.
- **ICANN:** Oversees the global domain name system and ensures the stable operation of internet identifiers.
- **International Telecommunication Union (ITU):** A UN agency coordinating telecommunication operations and services, developing standards, and facilitating policy discussions.
- **Internet Engineering Task Force (IETF):** Fosters voluntary internet standards through open processes and working groups.
- **World Wide Web Consortium (W3C):** Develops standards for web technologies to enhance interoperability, operating through working groups and a multi-step standards process.

Current Challenges

- **Conflicting Governance Models:** The absence of a global blueprint leads to conflicts between different stakeholders, each operating with its own principles and motives.
- **Digital Divide:** The gap between those with and without access to modern information and communication technology.
- **Cybersecurity Threats:** Increasingly sophisticated attacks compromise the integrity, confidentiality, and availability of information systems.
- **Misinformation Impact:** Undermines public trust, influences elections, and widens social divisions.
- **Tech Giants' Influence:** Concerns about monopolistic practices, privacy violations, and the need for regulatory oversight.
- **Net Neutrality:** The principle of equal treatment of all internet data by ISPs.
- **Government Surveillance:** Balancing national security with privacy and civil liberties.
- **Content Moderation:** Challenges in removing harmful content while protecting free speech.
- **Digital Sovereignty:** Nations' ability to control their digital infrastructure and data.
- **Privacy:** Balancing data protection with the needs of businesses and governments.
- **Regulation vs. Freedom:** The balance between government control and an open internet.

Future Directions

- **Addressing the Identity Problem:** Implementing strong authentication, privacy protections, and universal digital identity standards4344. Bhutan's National Digital Identity (NDI) system is a leading example.
- **Ensuring Authentic Data:** Implementing data validation, access controls, encryption, and audit trails. The Coalition for Content Provenance and Authenticity (C2PA) is a model for combating misinformation.
- **Empowering Users with Smart Wallets:** Secure storage for sensitive information, with features like multi-factor authentication, encryption, and open standards. The EU's eIDAS 2.0 and the Open Wallet Foundation are leading examples.
- **Creating the Network of Networks:** Establishing trust registries to verify digital documents and prevent fraud. The Global Acceptance Network (GAN) is working to create standards for interoperability.
- **Traversing Cross-Border Regulation:** Harmonizing policies for digital trade, data privacy, and cybersecurity. The Canadian Digital Governance Council's conformance program supports cross-border recognition.
- **Creating Digital Unity:** Addressing the digital divide by expanding infrastructure, promoting digital literacy, and ensuring equitable access5960. The United Nations is actively working to bridge these gaps.

THE EARLY YEARS OF INTERNET GOVERNANCE

ARPANET

In the late 1960s, the **Advanced Research Projects Agency Network (ARPANET)** was developed, primarily funded by the U.S. Department of Defense. Initially, governance was informal and community-driven, relying heavily on the collaboration of researchers and academic institutions.

The Advanced Research Projects Agency (ARPA), now known as DARPA, played a vital role in the governance of ARPANET. ARPA funded and directed the project, with key figures like Bob Taylor and Larry Roberts leading the initiative. The actual construction and maintenance of ARPANET were outsourced to contractors, such as **Bolt Beranek and Newman (BBN)**, who built the **Interface Message Processors (IMPs)** that connected the network.

During that time, governance was highly collaborative, with input from various computer scientists and engineers. Leonard Kleinrock at UCLA, Steve Crocker, and Jon Postel were among those who contributed significantly to the development and management of ARPANET. Much of the decision-making happened through informal meetings, discussions, and memos rather than through formalized structures.

In 1975, operational control of ARPANET was transferred to the Defense Communications Agency, marking a shift towards more formalized governance.

THE INTERNET CONFIGURATION CONTROL BOARD

The **Internet Configuration Control Board (ICCB)** was established in 1979 by Vint Cerf, who was then a program manager at the **Defense Advanced Research Projects Agency (DARPA)**. The ICCB was created to oversee the technical aspects of the Internet and provide guidance on its development.

In 1983, the ICCB was reorganized by Barry Leiner, Cerf's successor at DARPA, into a series of task forces focusing on different technical aspects of internetting. "Internetting" refers to the process of connecting multiple computer networks together using Internet Protocol (IP) to form a larger network, commonly known as the Internet. This concept was fundamental in the development of the Internet as we know it today, enabling disparate networks to communicate and share data seamlessly. The term is often associated with the early efforts to create a global, interconnected network of networks, facilitated by protocols like TCP/IP. This reorganized group was renamed the **Internet Activities Board (IAB)**.

Finally, in **1992**, the IAB was renamed the Internet Architecture Board to better reflect its role in providing architectural oversight and guidance for the Internet. This change also marked the

Internet's transition from a U.S.-government entity to an international, public entity under the **Internet Society (ISOC).**

In the early days, there were two key governance developments: 1) the Request for Comments (RFC) Series and 2) the establishment of **the Internet Assigned Numbers Authority (IANA)**.

THE IETF AND REQUEST FOR COMMENTS (RFC) SERIES:

The Internet Engineering Task Force (IETF) was established on January 14, 1986. It was created to develop and promote voluntary Internet standards, ensuring the technical and engineering aspects of the Internet function smoothly. Initially supported by the U.S. federal government, the IETF became an independent activity under the Internet Society in 1993.

The Request for Comments (RFC) series is a collection of technical and organizational documents about the Internet, primarily published by the **Internet Engineering Task Force (IETF)**. Here's a brief overview of its development:

The RFC series began in 1969 as part of the ARPANET project. The first RFC, titled "Host Software," was written by Steve Crocker of UCLA. Initially, RFCs were meant to document unofficial notes and encourage discussion among researchers. Over time, they evolved into official documents describing methods, behaviors, research, and innovations applicable to the Internet.

RFCs are sequentially numbered, starting with RFC 12. As of now, there are over nine thousand documents in the series. The RFC series includes two subseries: STDs (Internet Standards) and BCPs (Best Current Practices). STDs are RFCs that define Internet standards, while BCPs provide best practices for the Internet.

Individuals or groups of engineers and computer scientists author RFCs. RFCs are submitted for peer review and, if approved, published. Some RFCs become Internet Standards, while others are informational or experimental. RFCs are published in various formats, including HTML and plain text. RFCs are freely available for download, copying, publishing, and distribution under a license granted by the IETF Trust.

ESTABLISHMENT OF THE INTERNET ASSIGNED NUMBERS AUTHORITY (IANA):

IANA was established in 1972 by Jon Postel, a graduate student at UCLA, who proposed the need for a central authority to manage socket numbers for ARPANET. Initially, IANA was managed by Postel at the Information Sciences Institute (ISI) at the University of Southern California (USC). This arrangement continued until 1998.

In 1998, the U.S. Government transferred the management of IANA to the **Internet Corporation for Assigned Names and Numbers (ICANN)**. This transition aimed to create a more globally inclusive and transparent governance model. In 2016, the stewardship of IANA was transitioned to **Public Technical Identifiers (PTI)**, an affiliate of ICANN, marking the end of U.S. Government oversight.

IANA is responsible for the global allocation of IP addresses, ensuring that each address is unique. IANA manages the root zone of the Domain Naming Service (DNS) which is essential for the functioning of Internet traffic flow. IANA also allocates autonomous system numbers, which are used to identify networks on the Internet.

EMERGENCE OF ICANN

In 1998, the **Internet Corporation for Assigned Names and Numbers (ICANN)** was established as a pivotal governance body tasked with managing domain names and IP address distribution, embodying a shift towards a more structured governance model that included various stakeholders. Before ICANN, the Internet was managed by a loose network of volunteers, governmental actors, and academic institutions.

ICANN was created as a non-profit corporation based in the U.S., with global participation. The U.S. Government recognized the need for a more formal and globally inclusive governance model for the DNS and committed to transferring the policy and technical management of the DNS to ICANN.

ICANN's early mission was to ensure the stable and secure operation of these unique identifiers, which are critical to the Internet's traffic functionality. ICANN was initially governed by a Board of Directors, which included representatives from various stakeholder groups, including governments, businesses, and technical experts. From its inception, ICANN aimed to be a globally inclusive organization, with participation from stakeholders around the world.

CONTEMPORARY INTERNET GOVERNANCE STRUCTURES

As the Internet expanded, so did its governance complexities. Today, Internet governance operates through a multi-stakeholder model involving key players from government, private sector, civil society, and technical communities.

The following organizations are recognized as pillars for current Internet governance:

- **Internet Corporation for Assigned Names and Numbers (ICANN)**: Oversees the global domain name system and ensures the stable operation of Internet identifiers.
- **International Telecommunication Union (ITU)**: A UN agency coordinating telecommunication operations and services.
- **Internet Engineering Task Force (IETF)**: Fosters voluntary Internet standards through open processes.
- **World Wide Web Consortium (W3C)**: Develops standards for web technologies to enhance interoperability.

ICANN

ICANN (Internet Corporation for Assigned Names and Numbers) plays a crucial role in the governance of the Internet, particularly in managing the Domain Name System (DNS). Here are some detailed aspects of how ICANN governs:

ICANN is governed by a Board of Directors, which includes voting members and non-voting liaisons. The Board is responsible for overseeing ICANN's operations and ensuring that it fulfills its mission. ICANN operates according to a set of bylaws and policies that guide its activities. These documents outline the organization's structure, decision-making processes, and responsibilities. The Affirmation of Commitments document, signed in 2009, outlines ICANN's commitments to the global Internet community and includes mechanisms for accountability and transparency.

ICANN's primary mission is to ensure the stable and secure operation of the Internet's unique identifier systems, such as domain names and IP addresses. It coordinates the DNS at a global level, ensuring that it remains interoperable and resilient. It employs open, transparent, and bottom-up policy development processes, involving stakeholders from the private sector, civil society, the technical community, academia, and end users.

ICANN manages the allocation and maintenance of domain names, ensuring that they are unique and properly registered. It oversees the distribution of IP addresses, ensuring that they are assigned in a fair and efficient manner. It develops policies related to the DNS and other Internet-related issues, often through a multistakeholder process that includes input from various stakeholders.

ICANN holds regular public meetings where stakeholders can participate in discussions and decision-making processes. It has established review panels to assess its performance and ensure accountability. It often includes public comment periods for proposed policies and changes, allowing for input from the global Internet community.

ICANN is continually adapting to technological advancements, such as the introduction of new top-level domains (TLDs) and the increasing use of IPv6. It emphasizes the importance of global collaboration and seeks to involve stakeholders from around the world in its governance processes. It aims to ensure that its operations are sustainable and that it can continue to fulfill its mission in the long term.

ICANN's governance model is designed to be flexible and responsive to the changing needs of the Internet community, ensuring that it remains a stable and secure platform for global communication and innovation.

do so, it must know the objective of the audit requirement and how the client application meets that standard. There are tools and services that can be used to document those assertions that we will cover in the next section. If an audit client does not have a complete set of controls to meet audit requirements, the auditor will need to expend extra time and resources to finalize the control set.

ITU

The International Telecommunication Union (ITU) plays a significant role in Internet governance. The ITU develops international standards (ITU-T Recommendations) that ensure seamless interconnection and interoperability of communication systems. These standards cover various aspects of telecommunications, including Internet protocols and technologies. ITU facilitates international public policy discussions on Internet-related issues. It brings together governments, private sector, and other stakeholders to develop policies that promote the growth and stability of the Internet.

The highest decision-making body of the ITU gathers at the plenipotentiary conference, held every four years, where member states set the Union's general policies. The governing body of the ITU between plenipotentiary conferences is the Council, which is responsible for overseeing the implementation of ITU's policies and programs.

Private sector companies and other organizations contribute to ITU's work through financial contributions and participation in ITU's activities. It has various study groups that focus on specific areas of telecommunications and information technology, developing standards and recommendations.

The ITU has several future directions specific to the governance of the Internet. ITU plans to:

- Work to close the digital divide by promoting policies and initiatives that facilitate universal access to the Internet.

- Develop and promote international standards and best practices for cybersecurity, helping to protect users and infrastructure from cyber threats.
- Work with governments and other stakeholders to create policies that promote an open, free, inclusive, and secure digital future.
- Offer technical assistance and capacity-building programs to support the development of Internet infrastructure in underserved regions.
- Facilitate discussions and collaborations among governments, private sector, and other stakeholders to develop policies that promote the sustainable and equitable use of Internet resources.

These future directions reflect ITU's commitment to ensuring that the Internet remains a global, inclusive, and secure resource for all.

IETF

The Internet Engineering Task Force (IETF) is a key player in the development of Internet standards. Here's a detailed look at how the IETF governs:

- Internet Architecture Board (IAB): The IAB oversees the IETF's external relationships and provides long-range technical direction for Internet development. It also manages the Internet Research Task Force (IRTF), which focuses on long-term research issues1.
- Internet Engineering Steering Group (IESG): The IESG is responsible for the technical management of IETF activities and the Internet standards process. It reviews and approves standards documents and manages the overall direction of the IETF.
- Working Groups (WGs): The IETF operates through a series of working groups, each focusing on specific areas of Internet technology. These groups are open to anyone who wants to participate, and they hold discussions on open mailing lists and at IETF meetings.

The IETF standards process works similarly like many other standards bodies. Anyone can submit a proposal for a new standard or an improvement to an existing standard. If there is sufficient interest, a working group is formed to develop the standard. The working group is led by two co-chairs who guide the discussion and decision-making process. The working group collaborates to draft the standard, which is then reviewed and revised through multiple iterations. The draft is open for public comment, allowing for input from the broader Internet community. Once the draft is finalized, it is submitted to the IESG for approval. If approved, the standard is published as an RFC (Request for Comments).

The IETF is open to anyone who wants to participate, with no formal membership requirements. This ensures a diverse range of perspectives and expertise. It operates on a bottom-up model, where working groups drive the development of standards based on community consensus. Participants in the IETF are volunteers, often supported by their employers or other sponsors. This volunteer-driven model fosters a collaborative and inclusive environment.

The IETF holds three meetings per year, known as IETF meetings, where working groups hold face-to-face sessions to discuss and advance their work. These meetings are open to anyone who registers, with significant discounts available for students and remote participants.

The IETF continues to evolve, addressing emerging technologies and challenges. It remains committed to its principles of open participation, bottom-up development, and volunteer-driven collaboration, ensuring that the Internet remains a robust and innovative platform.

W3C

The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web. Here's a detailed look at how the W3C governs:

- **Board of Directors**: The W3C is governed by a Board of Directors, which includes representatives from member organizations, partner organizations, and the general public. The Board has ultimate authority over W3C's strategic direction and ensures that the organization fulfills its mission.
- **Advisory Board**: The Advisory Board provides guidance on technical and policy matters to the Board of Directors. It includes experts from various fields who contribute to the development of W3C standards.
- **Membership**: W3C has over 450 member organizations, including companies, universities, and government agencies. Members participate in working groups and contribute to the development of standards.

The W3C operates through a series of working groups, each focusing on specific areas of Web technology, such as HTML, CSS, and Web Payments. These groups are open to anyone who wants to participate, and they collaborate to develop and maintain standards. Task forces are temporary groups formed to address specific issues or projects. They work on tasks that require focused attention and are dissolved once their objectives are achieved.

Anyone can submit a proposal for a new standard or an improvement to an existing standard. If there is sufficient interest, a working group is formed to develop the standard. The working group is led by co-chairs who guide the discussion and decision-making process. The working group collaborates to draft the standard, which is then reviewed and revised through multiple iterations. The draft is open for public comment, allowing for input from the broader Web community. Once the draft is finalized, it is submitted to the Advisory Board and the Board of Directors for approval. If approved, the standard is published as a W3C Recommendation.

The W3C holds annual meetings, known as TPAC (Technical Plenary and Advisory Committee) meetings, where working groups and task forces gather to discuss and advance their work. These meetings are held in different cities each year to facilitate global participation. It also

organizes public events, such as workshops and conferences, to engage with the broader community and promote the adoption of Web standards.

The W3C has a comprehensive set of policies that govern its operations, including membership, standards development, and intellectual property rights. These policies ensure that W3C operates transparently and inclusively. The organization provides detailed legal information on its website, including licenses, copyright, trademarks, and terms and conditions. This information helps members, and the public understand their rights and responsibilities when participating in W3C activities.

The W3C continues to adapt to emerging technologies and trends, ensuring that Web standards remain relevant and effective. It emphasizes the importance of global collaboration and seeks to involve stakeholders from around the world in its governance processes. Finally, it aims to ensure that its operations are sustainable and that it can continue to fulfill its mission in the long term.

By maintaining a transparent, inclusive, and collaborative governance model, W3C plays a crucial role in shaping the future of the Web.

CURRENT CHALLENGES IN INTERNET GOVERNANCE

CONFLICTING GOVERNANCE MODELS

The Internet is a globally distributed network, and no single entity owns or governs it entirely. Instead, it is managed by a decentralized and international multistakeholder network of interconnected autonomous groups consisting of these major players, some introduced earlier:

- Internet Corporation for Assigned Names and Numbers (ICANN)
- Internet Service Providers (ISPs)
- Governments
- Private Sector Tech Players
- Civil Society and Academia
- International Organizations

The challenge here is that each of these players operate independently, directed by their own principles, missions, and motives, which often clash. There is no global blueprint or architecture for Internet governance, so progress is often stalled by players taking actions driven for their own benefit that are detrimental to the principles and mission in other groups.

The debate over Internet regulation revolves around finding the right balance between protecting users and preserving the open nature of the internet. Key issues include content moderation, privacy, and the role of government in regulating online activities. These clashes in governance models exacerbate the following other challenges with no end in sight.

Digital Divide

The digital divide refers to the gap between those who have access to modern information and communication technology and those who do not. This gap can be due to a range of factors such as geographic location, socioeconomic status, and education. Bridging this divide is crucial for ensuring equal opportunities in education, employment, and access to essential services. Efforts to address this issue include improving infrastructure, providing affordable internet access, and promoting digital literacy.

Cybersecurity Threats

Cybersecurity threats encompass a wide range of malicious activities aimed at compromising the integrity, confidentiality, and availability of information systems. Common types of cyberattacks include malware, phishing, ransomware, and denial-of-service (DoS) attacks. The rise of advanced technologies like AI and quantum computing has introduced new threats,

making it essential for organizations to adopt robust cybersecurity measures and stay updated on emerging threats.

Misinformation Impact

Misinformation can have significant social, political, and economic consequences. It can undermine public trust, influence elections, and widen social divisions. Addressing misinformation requires a multi-faceted approach, including media literacy education, fact-checking initiatives, and responsible content moderation by platforms.

Tech Giants' Influence on Internet Governance

Tech giants like Google, Facebook, and Amazon wield noteworthy influence over internet governance due to their control over vast amounts of data and user interactions. Their policies and practices can shape the digital landscape, raising concerns about monopolistic practices, privacy violations, and the need for regulatory oversight. While these companies exhort benevolent intentions, they are still driven by a profit motive backed by their responsibilities to their shareholders and employees.

Net Neutrality

Net neutrality is the principle that internet service providers should treat all data equally, without discriminating or charging differently based on user, content, or platform . The controversy stems from debates over whether ISPs should be allowed to prioritize certain types of traffic, which could impact innovation, competition, and consumer choice.

Government Surveillance

Government surveillance involves monitoring individual's activities to ensure national security. While it can help prevent crime and terrorism, it also raises concerns about privacy, civil liberties, and the potential for abuse. Balancing security and privacy are a complex issue that requires careful consideration of legal frameworks and oversight mechanisms.

Content Moderation on Social Media

Content moderation involves the removal or restriction of harmful or inappropriate content on social media platforms. This is a challenging task due to the sheer volume of content and the need to balance free speech with community safety. Platforms use a combination of algorithms, human moderators, and user reports to manage content, but controversies often arise over inconsistent enforcement and bias.

Digital Sovereignty

Digital sovereignty refers to a nation's ability to control its digital infrastructure and data. This concept is gaining importance as countries seek to protect their citizens data from foreign surveillance and influence. It involves policies and regulations that ensure data is stored and

processed within national borders and that digital services comply with local laws. However, different countries are implementing divergent regulations that can lead to a fractured Internet.

Privacy

The collection and use of personal data by governments and companies raise significant privacy concerns. Striking a balance between data protection and the legitimate needs of businesses and governments is an ongoing challenge.

Regulation vs. Freedom

The balance between government regulation and the freedom of the Internet is a contentious issue. Some countries advocate for more government control, while others emphasize the importance of maintaining an open and unrestricted Internet.

FUTURE DIRECTIONS IN INTERNET GOVERNANCE

Given the origins of Internet governance and the multiparty stakeholder operation that exists today, we've created so many barriers that inhibit real progress. The stakes are high as most Internet challenges are over ten years old and not going away. We need to shed our selfish motivations and work together for the greater good of our digital society. Here are a few of knotty challenges that we must face together so we can have a safe, inclusive, and trustworthy Internet we can leave to our children and grandchildren:

FIXING THE IDENTITY PROBLEM

The Internet was built without a transport protocol tied to an authentic and verifiable identity. The anonymity of transactions creates massive fraud and blindfolds Internet governance. To fix the Internet identity problem, we need to implement strong authentication methods like multi-factor and biometric authentication, enhance privacy protections through data minimization and encryption, develop universal digital identity standards for interoperability, foster collaboration among stakeholders, educate and empower users with digital literacy, and address legal and regulatory frameworks to ensure compliance and user control over their digital identities. This multifaceted approach aims to create a secure, private, and user-friendly digital identity system.

The **Government of Bhutan** is pioneering a **National Digital Identity (NDI**) system, launched in October 2023, to provide secure and verifiable identity-related credentials to its citizens. Envisioned by His Majesty the King and developed by **the Government Technology (GovTech) Agency** and **DHI InnoTech**, the NDI system is based on self-sovereign identity (SSI) principles and decentralized identifier (DID) technology. This initiative empowers citizens by giving them control over their personal data, ensuring privacy, and promoting digital inclusion. The NDI system facilitates access to government and business services while maintaining high standards of data security and user consent. The Bhutan NDI system is a model for a fully realized government identity system.

CHANGING DATA BLOBS TO AUTHENTIC DATA

In addition to the lack of identity, traffic through the Internet consists of unverified data blobs moving from one machine to another with the final destination performing widely disparate degrees of verification. These data packets, which can contain anything from web pages and emails to video streams and file transfers, are often encrypted for security, making it difficult to verify their content at every hop. As a result, internet service providers (ISPs) and other intermediaries can collect and analyze this traffic, but the actual content and its legitimacy

remain largely unverified until it reaches its final destination. This lack of verification can lead to privacy concerns and potential misuse of data.

We need to strive to ensure that all Internet traffic is "authentic." In the context of Internet data, "authentic" refers to data that can be verified as genuine, accurate, and trustworthy. Authentic data has not been tampered with or altered in any unauthorized way, and its origin and integrity can be confirmed. This involves ensuring that the data is generated by a legitimate source, has not been corrupted or falsified, and remains consistent throughout its lifecycle. Authentication mechanisms, such as digital signatures, cryptographic hashes, and secure channels, are often used to verify the authenticity of data on the Internet.

To ensure only authentic data passes through the Internet, Internet leaders need to implement robust data validation and verification processes, enforce strict access controls, use strong encryption methods, maintain regular backups and recovery plans, implement data versioning and timestamps, keep detailed audit trails and logs, and establish effective error handling mechanisms. These steps help maintain data integrity, prevent unauthorized access, and ensure data remains accurate and reliable throughout its lifecycle.

The **Coalition for Content Provenance and Authenticity (C2PA)** aims to combat the spread of misleading information online by developing technical standards for certifying the source and history (or provenance) of media content. Their mission is to provide publishers, creators, and consumers with the ability to trace the origin of diverse types of media, ensuring transparency and authenticity . By creating a digital fingerprint for content, C2PA helps verify its authenticity and track any changes made, thereby fostering trust in digital media. The work of the C2PA is a model for private sector collaboration and is arising as the leading effort to thwart deep fakes and misinformation generated by artificial intelligent agents.

EMPOWERING INTERNET USERS WITH SMART WALLETS

For years we have seen the transformation of the Internet portal from the computer browser to the smartphone. This transformation cannot be complete until we have a secure place to store our most sensitive information, similar to the physical wallets we've used for thousands of years (dating back to ancient civilizations like Egypt and Mesopotamia).

To establish an interoperable and secure wallet for cryptocurrency and verifiable credentials, we need to prioritize multi-factor authentication (MFA) for enhanced security. Implement open standards like OpenID for Verifiable Credentials to ensure cross-platform interoperability. Furthermore, we need to encrypt all stored data to protect against unauthorized access and conduct regular security audits to address vulnerabilities. Finally, we need to educate users on the best security practices and ensure compliance with relevant regulations and standards for data protection and privacy. By following these steps, we can create a reliable, secure, and interoperable wallet for managing digital assets and credentials.

The **European Union (EU)** efforts on **eIDAS 2.0** and **The OpenWallet Foundation** focus on creating a secure and interoperable digital wallet for European citizens. eIDAS 2.0, an updated

European regulation, mandates that all EU member states provide conformant digital wallets by early 2027 . These wallets will enable users to securely identify themselves, store, and manage various documents like driving licenses and verifiable credentials. The OpenWallet Foundation supports this initiative by promoting open standards, ensuring high security, and facilitating cross-border interoperability. The goal is to create a user-friendly, secure, and free-of-charge digital identity solution that respects privacy and enhances trust in digital transactions.

While this effort is ambitious and under attack for its heavy-handed approach, the result of enacting law within twenty-seven member states (and growing) is feverishly bringing collaboration of private and governmental factions together. This should lead to global standards in this area.

THE NETWORK OF NETWORKS

With the approaching hybrid of authentic and anonymous data and sources traversing the Internet, how do users know they are interacting with bona fide actors? One answer is trust registries.

Trust registries address several critical issues on the Internet by ensuring the authenticity of digital documents, thereby simplifying the verification of e-health credentials, educational certificates, and professional licenses. They help prevent identity theft and document forgery by validating data sources and authenticity. Trust registries also provide a standardized framework for interoperability, allowing different systems to recognize and verify credentials seamlessly across borders. Additionally, they enhance transparency and security in digital transactions by fostering trust among users and service providers through cryptographic methods and decentralized verification processes. Overall, trust registries create a secure foundation for digital interactions on the Internet.

The **Global Acceptance Network (GAN)** aims to establish a new trust layer for the Internet by creating standards for the interoperability of trust registries. GAN seeks to address the lack of trust in digital interactions by developing a neutral governance system that ensures secure and seamless digital credential exchanges. By implementing protocols like the Trust Registry Query Protocol and governance frameworks, GAN facilitates the validation and recognition of digital credentials across different ecosystems, enhancing trust and transparency in online transactions.

The GAN is just being established so it is unclear whether it will achieve its objectives. It has already signed up major companies, credential ecosystems and governments such as the Bhutan NDI. The GAN fills a needed gap in Internet governance as it focuses on the interoperability of trusted information rather than solely the message traffic and the Internet server backbone.

TRAVERSING CROSS-BORDER REGULATION AND RECOGNITION

Efforts in cross-border regulation and cooperation for the Internet, focus on harmonizing policies to address the challenges of digital trade, data privacy, and cybersecurity. International organizations like the **World Trade Organization (WTO)** and the **Organization for Economic**

Cooperation and Development (OECD) are working to create frameworks that facilitate regulatory cooperation and ensure that digital services can operate seamlessly across borders. These efforts aim to balance national concerns such as privacy and security with the global nature of the Internet, promoting stability and trust in digital interactions.

The Canadian **Digital Governance Council's (DGC)** conformance program assists in cross-border regulation and recognition by providing a standardized framework for assessing and certifying digital governance practices. This program ensures that organizations adhere to best practices in data integrity, security, and privacy, enabling them to demonstrate their commitment to digital trustworthiness leading to cross-border recognition. By obtaining DGC certification, organizations can gain recognition and trust across borders, facilitating smoother digital interactions and compliance with international regulations.

Future Internet trust is dependent on governments holding their digital practices accountable through conformance programs like the DGC.

CREATING DIGITAL UNITY

Efforts to address the digital divide focus on improving accessibility, affordability, and digital literacy. Initiatives include expanding broadband infrastructure to underserved areas, implementing public-private partnerships to fund and deploy technology, and providing digital skills training to help individuals fully participate in the digital economy. Programs like the **Digital Inclusion Navigator** through the **EDISON Alliance** are working to bridge these gaps globally, ensuring that more people can access and benefit from digital tools and resources.

The **United Nations** is actively working to address the digital divide through initiatives aimed at increasing connectivity, promoting digital literacy, and ensuring equitable access to technology. The **United Nations Development Programme (UNDP)** is actively promoting **Digital Public Infrastructure (DPI)** to support digital transformation and achieve the **Sustainable Development Goals (SDGs)**. DPI encompasses open technology standards, enabling governance, and a community of innovative market players. UNDP's efforts include the 50-in-5 campaign, aiming to help fifty countries design, launch, and scale DPI components by 2028, and the High Impact Initiative on Digital Public Infrastructure, targeting support for 100 countries by 2030. These initiatives focus on improving public service delivery, fostering digital inclusion, and ensuring secure and transparent digital interactions. Additionally, the UN is developing a **Global Digital Compact** to promote an open, free, inclusive, and secure digital future, with input from various stakeholders including governments, tech companies, civil society, and academia**.**

The **Global DPI Conference**, held in Cairo, Egypt from October 1-3, 2024, brought together over one hundred countries to discuss the transformative impact of Digital Public Infrastructure (DPI) on achieving the Sustainable Development Goals (SDGs). The conference highlighted the progress made in adopting and implementing DPI, showcasing diverse technology solutions, policy frameworks, and implementation models. The outcome statement emphasized the need for knowledge sharing, stakeholder engagement, universal safeguards, inclusive innovation,

and thriving local digital ecosystems to accelerate DPI implementation and ensure it benefits everyone.

The vision of a truly global and inclusive Internet cannot be realized unless the Internet is governed with principles of equitability and inclusion for all.

FINAL THOUGHTS

The governance of the Internet continues to evolve, necessitating adaptive frameworks that consider technological advancements, societal needs, and security challenges. An inclusive, multi-stakeholder approach that emphasizes collaboration, transparency, and education will be crucial in ensuring that the Internet remains a resource for all, facilitating global communication and innovation.

CALL TO ACTION

If you would like to learn more about how the Digital Governance Institute may help in Internet governance, please contact us at info@digitalgovernanceinstitute.com.

Scott Perry is the Founder and CEO of the Digital Governance Institute where he provides a variety of governance solutions in the emerging space of governance of digital assets. Scott is a recognized global leader in digital identity, blockchain, and verifiable credential governance and accreditation. He has worked with the world's most respected SSL-certificate issuers, aerospace and defense companies, and government agencies such as the US Senate Sergeant at Arms and Federal Aviation Administration.

He is a Co-Chair the Trust Over IP Foundation's Governance Stack Working Group where he has authored and contributed to most of its governance and assurance publications driven to create standards and accountability in decentralized identity and verifiable credential networks.

As a hands-on governance and cybersecurity consultant and auditor, Scott provides deep and impactful advice that you would expect from a leader in the field.

REFERENCES

To maintain the integrity and credibility of this paper, a comprehensive reference list of academic articles, reports from governance bodies, and other relevant literature are included below:

ACADEMIC ARTICLES

1. Barlow, J. P. (1996). "A Declaration of the Independence of Cyberspace." Retrieved from: https://www.eff.org/cyberspace-independence
2. DeNardis, L. (2014). "The Globalization of Internet Governance: The Emerging Role of Multistakeholderism." *Internet Policy Review*, 3(3). doi:10.14763/2014.3.309
3. Mueller, M. (2009). "Ruling the Root: Internet Governance and the Taming of Cyberspace." *The MIT Press*.
4. Zittrain, J. (2008). "The Future of the Internet and How to Stop It." *Yale University Press*.

BOOKS

5. Kurbalija, J. (2016). "An Introduction to Internet Governance." DiploFoundation.
6. Ray, S. (2020). "Internet Governance: The New IGC Framework." Cadmus Journal, 5(1), 6-30.

REPORTS FROM GOVERNANCE BODIES

7. Internet Corporation for Assigned Names and Numbers (ICANN). (2019). "ICANN's Multi-Stakeholder Model: The Next Era of Governance." Retrieved from: https://www.icann.org
8. United Nations. (2019). "Report of the Secretary-General's High-Level Panel on Digital Cooperation." Retrieved from: https://digitalcooperation.org
9. World Economic Forum. (2020). "The Future of Digital Cooperation: Reflections on the UN Secretary-General's High-Level Panel on Digital Cooperation." Retrieved from: https://www.weforum.org

INDUSTRY REPORTS

10. Internet Society (ISOC). (2021). "Internet Governance: An Enduring Challenge." Retrieved from: https://www.internetsociety.org
11. Pew Research Center. (2021). "The State of Online Harassment." Retrieved from: https://www.pewresearch.org

International Guidelines

12. Council of Europe. (2020). "Internet Governance and Human Rights." Retrieved from: https://www.coe.int/en/web/freedom-expression/internet-governance

13. Organization for Economic Cooperation and Development (OECD). (2021). "Going Digital: Shaping Policies, Improving Lives." Retrieved from: https://www.oecd.org

Relevant Online Resources

14. Internet Governance Forum (IGF). (2022). "About the IGF." Retrieved from: https://www.intgovforum.org

15. W3C (World Wide Web Consortium). (2021). "About W3C." Retrieved from: https://www.w3.org

16. Where Wizards Stay Up Late by Katie Hafner and Matthew Lyon – A great read on the origins of the Internet.

17. **RFC 801** – "Planning and Control of Resources for the ARPANET".

18. **"A Brief History of the Internet"** – Available on the Internet Society's website.

19. **"Where Wizards Stay Up Late** by Katie Hafner and Matthew Lyon – A great read on the origins of the Internet.

20. **RFC 801** – "Planning and Control of Resources for the ARPANET".

21. **"A Brief History of the Internet"** – Available on the Internet Society's website.

22. "**Bhutan NDI**" https://www.bhutanndi.com/

23. " **Coalition for Content Provenance and Authenticity,"** https://c2pa.org/

24. "**eIDAS 2.0,**" https://www.european-digital-identity-regulation.com/

25. "**The OpenWallet Foundation,**" https://openwallet.foundation/

26. "**Global Acceptance Network,**" https://gan.foundation/

27. "**World Trade Organization**", https://www.wto.org/english/res_e/publications_e/digital_trade_2023_e.htm

28. "**Organization for Economic Cooperation and Development,"** https://www.oecd.org/en.html

29. "**Digital Governance Council,"** https://dgc-cgn.org/dtp/

30. "**EDISON Alliance,"** https://www.edisonalliance.org/home

31. "**United Nations Development Programme,"** https://www.undp.org/

32. "**Global DPI Conference,"** https://www.globaldpisummit.org/

This reference list is a mix of foundational texts, current reports, and institutional resources crucial for understanding the evolution of Internet governance. It can serve as a valuable resource for further study and engagement in this dynamic field.