December 2025

Emerging Digital Technologies and Their Impact on Policy and Regulation in the Middle East and North Africa

Authors: Michael Kende and Riyadh Al-Balushi

Commissioned by the Internet Society

Internet Society

Table of Contents

Acknowledgments: We would like to thank Nermine El Saadany for her leadership and Hana Sabbagh and Hanna Kreitem for their support in the region, and Dr. Joseph Lorenzo Hall, Natalie Campbell, Carl Gahnberg, Olaf Kolkman, John Morris, Christine Runnegar, and Robin Wilton for their input on this report. Policymakers from the countries and participants in workshops in Oman and Bahrain also provided input on country characteristics.

Disclaimer: The Internet Society's Internet Impact Assessment Toolkit[1] (the Toolkit) checks the impact of regulations on the Internet to ensure that they promote the Internet Way of Networking, by providing a framework for the analysis of proposed changes in policies, legislation, regulations, and other aspects impacting the Internet. The authors of this report have used the Toolkit as the lens through which to conduct this comparative analysis of regional policies, and while the lens was designed by Internet Society, the view through it is ours, as are the resulting conclusions.

Executive Summary

Context

This report, commissioned by the Internet Society, analyzes the impact of current and proposed policy and regulations on emerging technologies in the Middle East and North Africa (MENA). The study uses the Internet Society's Internet Impact Assessment Toolkit (the Toolkit), showing its usefulness in assessing complex regulatory landscapes and fostering an Internet Way of Networking.

The Internet Society, as a global advocate for an open, secure, and trustworthy Internet, developed the Toolkit to evaluate policy and regulatory proposals. A central aim of this study is to illustrate how the Toolkit can guide MENA policymakers in developing regulations that support innovation and mitigate risks without negatively impacting the Internet Way of Networking, thereby fostering innovation while safeguarding citizens' rights and not undermining the foundational principles of the Internet.

The report assesses several Internet regulations, reflecting on the opportunities and challenges that they pose for two crucial emerging technologies - artificial intelligence and cloud and edge computing. The project assesses key regulations across six MENA countries - Bahrain, Egypt, Jordan, Oman, Saudi Arabia, and the UAE, focusing on four key areas:

- **Data Governance** – Regulations governing data storage, access, and cross-border transfers.
- **Privacy Protection** – Regulations ensuring user privacy, including protections against automated profiling.

[1] https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/

- **Intermediary Liability** – The extent to which online platforms and service providers are held accountable for third-party content.
- **Encryption Regulation** – The legal frameworks affecting the use and availability of encryption technologies.

These regulations can overlap and have the potential to impact the open, global, and interoperable nature of the Internet, potentially leading to fragmentation.

To ensure a comprehensive assessment, the research incorporated input from policymakers in each of the six focus countries, as well as contributions from Internet Society experts. Key findings and preliminary recommendations were presented and refined through a workshop in Oman in July and a conference in Bahrain in December, where further stakeholder feedback was gathered. The stakeholders were introduced to the Toolkit, which was used throughout to evaluate how existing and proposed regulations align with global best practices and the core principles of the Internet.

Findings and Results

The study provided a comprehensive and current review of actual and proposed legislation in each of the six countries, to come to the following conclusions about their impact on emerging technologies and the broader Internet.

- **Data Governance:** Data localization requirements in several MENA countries may limit access to cloud services, hindering digital transformation. These regulations may also impact the availability and efficiency of AI applications, particularly in healthcare and financial services.
- **Privacy:** While many MENA countries have introduced data protection laws, restrictions on cross-border data transfers and gaps in protections against AI-driven profiling remain key issues.
- **Intermediary Liability:** The absence of clear legal protections for online platforms in most MENA countries increases legal risks, stifles local innovation, and might discourage investment in digital services.
- **Encryption:** Restrictions in some MENA countries) threaten cybersecurity, privacy, and trust in digital services.

Conclusion

Governments in MENA are at a critical juncture in shaping digital policies that will influence innovation, investment, and the Internet's openness. By adopting regulatory frameworks that support the Internet Way of Networking, critically assessed using the Toolkit, they can unlock the full potential of emerging technologies while preserving the fundamental benefits of a globally connected, secure, and trustworthy Internet. This analysis serves as both a specific assessment for the MENA region and a

broader example of how the Toolkit can be employed by diverse stakeholders to promote an open, globally connected, secure, and trustworthy Internet.

Introduction

Emerging digital technologies are reshaping the traditional way of living, the nature of economies, and how we use the Internet. This report, commissioned by the Internet Society, provides a timely analysis of how these technologies are impacting policy and regulation in the Middle East and North Africa (MENA). Crucially, it employs the Internet Society's Internet Impact Assessment Toolkit (the Toolkit) as its primary analytical lens, demonstrating the toolkit's utility for assessing complex regulatory landscapes and fostering an Internet Way of Networking.

While the emergence of artificial intelligence (AI) has received significant attention recently, AI is not the only emerging digital technology with impacts on governments and regulators. Cloud computing is fundamentally changing access to, and the location of, data, content, and services. Digital transformation driven by these and other technologies is a pressing issue, including in the Middle East and North Africa (MENA) region. Consequently, governments are increasingly reviewing existing policies and examining new ones to foster innovation, investment, and the use of new technologies, while also aiming to protect citizens from potential harm. However, it is vital that these regulations must be as smart as the technologies they address to avoid unintended or unanticipated impacts on the Internet.

The advocacy role of the Internet Society as a thought leader on protecting and promoting the Internet is increasingly important. As governments consider altering existing regulations or imposing new ones for emerging technologies, the Internet Society promotes the Internet Way of Networking (IWN) as the essential foundation for the Internet and has developed the Toolkit to guide such decisions and ensure the Internet continues to thrive. Policymakers, academic institutions, and like-minded partners and allies can turn to the Internet Society and resources like the Toolkit when considering their policies and regulations, especially considering that government actions that undermine the open, globally connected, secure, and trustworthy nature of the Internet can also fragment it and reduce its benefits.

This report's primary objective is to assess key Internet regulations for emerging technologies by demonstrating the practical application and value of the Internet Society's Internet Impact Assessment Toolkit. A central aim is to illustrate how the Toolkit can guide MENA policymakers in developing regulations that support innovation and mitigate risks without negatively impacting the Internet Way of Networking. The report assesses several Internet regulations, reflecting on the opportunities and challenges that they pose for new technologies. The two emerging technologies examined here are artificial intelligence and cloud and edge computing. The government policy and regulations reviewed are data governance, privacy protection, intermediary liability protection, and encryption regulation.

These regulations can overlap and have the potential to impact the open, global, and interoperable nature of the Internet, potentially leading to fragmentation.

This report uniquely addresses a need by showcasing how a structured framework—the Toolkit—can be used to enhance decision-making regarding Internet policy. We examine relevant existing and proposed regulations for the new technologies internationally and compare them with those in six MENA countries: Bahrain, Egypt, Jordan, Oman, Saudi Arabia, and the United Arab Emirates, to identify any gaps.

Although the issues addressed by these regulations have been relevant to Internet policy for years, the advent of new technologies may prompt the introduction of new regulations or alterations to existing ones, such as those concerning privacy, intermediary liability, or data localization. This project, therefore, seeks to identify relevant gaps in regulation or proposed changes that would benefit from the application of the Toolkit to ensure consistency with the Internet Way of Networking. This analysis serves as both a specific assessment for the MENA region and a broader example of how the Toolkit can be employed by diverse stakeholders to promote an open, globally connected, secure, and trustworthy Internet.

Key Issues for Project

This section defines the policies and regulations considered in this report, as well as the emerging technologies and the Toolkit for assessing the relevant regulations. The specific policies and regulations in each of the MENA countries are examined below in Section 3.

Policies and Regulations

As the use of the Internet increases in breadth and depth, increasingly covering all aspects of the lives of individuals, the operations of businesses, and the functioning of governments, the amount of data is increasing as its nature evolves to reflect all the online activities. As a result, governments have sought to transpose relevant offline regulations online and develop new regulations as needed. Such regulations can increase the ability and incentive of businesses to innovate and invest in new services, and for individuals to trust in those services. In this report we examine four such sets of regulations, and how they can help to ensure an open and trustworthy Internet.

Data Governance

Data governance is a government policy that can define categories of data and direct how organizations manage each category of data. Examples of categories include personal data, company data, research data, and public data. In some countries financial data or health data is treated apart from the other categories. Among other aspects, policies can cover governance of particular categories of data within a country (at rest) as well as cross-border transfers (in transit).

Data governance policies must balance several important elements of an open, globally connected, secure and trustworthy Internet. Specifically, the open Internet is built on free flows of data, so efforts to restrict cross-border transfers can result in fragmentation of the Internet.[2] At the same time, without restrictions on the treatment of data at rest in the country, or similar assurances outside the country, the Internet would become less trustworthy.

There is some overlap with the other categories of policies below. Privacy policies cover the specific governance of personal data, while some countries' data governance policies address encryption of data. Here we cover general aspects of data governance, and in the sections below aspects specific to privacy protection and encryption.

Privacy Protection

Privacy regulations establish individuals' rights to privacy and protection of their personal data. In this context, personal data is defined as any information related to an identified or identifiable person, including name, contact information, credit card number and other such information. The European Union has a further classification of sensitive data, which includes racial or ethnic orientation, health and genetic data, political beliefs and sexual orientation.

Privacy regulations dictate how such data should be collected, used, stored, protected and shared. This includes how it is used for automatic profiling or decision-making, which is increasingly relevant with the increased introduction of artificial intelligence to business and government processes.

Privacy protection is a subset of data governance relevant to specific data, which can include specific requirements on its treatment at rest or in transit, including across borders. A lack of sufficient privacy protection can have a significant impact on individuals whose data is leaked and misused, particularly if the data are sensitive, and can lower trust in the Internet among all users, not just those directly affected.

Intermediary Liability Protection

Intermediaries are entities that enable or support the communication of content on the Internet by users (businesses, governments, individuals, and organization). They handle content created by those users but are not legally responsible for that content. Intermediaries include content delivery networks (CDNs), cloud providers, web hosts, search engines, social media platforms, and Internet service providers (ISPs). Without intermediaries, individuals would not be able to engage in online discussions of football, make videos or other creative content available online, or more broadly participate in global online dialogue.

---

[2] For an Internet Way of Networking Use Case on the impact of data localization, see https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/

As an example, a user may create a video and use an ISP to upload it to a social media platform. This platform may deliver it to a CDN which distributes the video to caches located near the platform's main userbases, and end-users access the video from a nearby cache. None of the companies hosting and delivering the video have any editorial responsibility over the content that is in the video. However, if the content infringes copyright protections, or is harmful or illegal, in some jurisdictions, a court may order an intermediary to take down or block access to the video.

Intermediary liability protection shields these intermediaries from liability for the content that they carry or host.[3] Furthermore, companies can take a decision to remove objectionable content, with no liability for doing so. Intermediary liability protections have enabled a wide range of intermediaries to experiment and start new and innovate online services. A lack or limit on intermediary protections would likely discourage companies from offering those services or to so severely limit access to their services and the type of content that can be communicated that individuals may be prevented or discouraged from participating on the Internet.

Encryption

Encryption protects online data so that it can only be used by those intended to have access.[4] For instance, it is now often used by messaging services to protect messages end-to-end, so that even the provider cannot read them. It is also used to protect information transmitted through the World Wide Web, such as by e-commerce sites to protect their customers credit card purchases. More generally, it can be used to protect data at rest (in a data center) or in transit (through ISPs).

Encryption is important in protecting privacy and sensitive data, preventing cybercrime, and unlawful interception. The result is that the Internet is more secure and trustworthy. Legal limits on the use of encryption can harm individuals, companies, and other organizations including governments whose data is exposed to cybercrime or unlawful interception. This would limit investments by companies who would otherwise rely on encryption protections, and limit usage by individuals involving personal data, as the Internet would be less secure or trustworthy.

Emerging Technologies

This report examines policy and regulatory responses to two emerging technologies – artificial intelligence and cloud and edge computing. These technologies have been emerging for a number of years but have not been deployed at scale in all countries and are undergoing continual changes. While AI is not a new technology, generative AI gained widespread awareness just two years ago in

[3] For an Internet Way of Networking Use Case on Intermediary Liability Protection, see https://www.internetsociety.org/resources/doc/2024/a-policy-framework-for-internet-intermediaries-and-content/

[4] For a description of encryption, see https://www.internetsociety.org/issues/encryption/what-is/

November 2022, with the introduction of ChatGPT to the public. Likewise, cloud computing is an established form of hosting and delivering content and services but is not present in all countries today; on the other hand, the emergence of edge computing requires local access.

The adoption and usage of these technologies is impactful, and in turn impacted by relevant policies and regulations, or a lack thereof. At the same time, governments may seek to balance a need to address the potential impact of the technologies on the one hand, while seeking to promote investment and innovation on the other hand. An assessment using the Toolkit can help to achieve both goals. The two technologies are introduced here, and the Toolkit is introduced in the next section.

Artificial Intelligence

While AI has a wide and spreading impact across organizations and society, here we focus on two broad types of AI – expert systems and generative AI – where the relevant regulations are most likely to have an impact.

AI expert systems assist or automate human decision-making in a specific domain. For instance, they can help doctors diagnose specific types of cancers from images and assist in devising treatments. The systems are trained using existing images that have been labeled with relevant patient information about the course of the cancer and with input from experts providing a knowledge base. These AI systems can provide valuable assistance to professionals making difficult decisions – however, their value depends on the quality of the training data.

Regulations that localize data needed to train AI expert systems, such as health data, can limit the value of expert systems for citizens of those countries. In particular, medical diagnostic systems could provide incorrect diagnoses or ineffective treatment plans, if there is a disease endemic to a country or region from which the relevant data is not made available. Another result could be that the medical expert system is not made available or used in those countries. This is a representation of the impact of fragmenting the Internet which could have tangible impacts on citizens who would otherwise benefit from the expert systems.

Other expert systems may use personal information for profiling users or in decision-making systems, including for recommendations and financial decisions. If this is done without the knowledge or consent of the users, it would violate their privacy rights and, once understood, would undermine trust in using the Internet. Privacy regulations can address this by requiring consent to use personal data in such systems or enabling users to opt-out of having their data included in the systems.

Generative AI models learn from input training data and then generate new content, which can include text, voice, images, video, and computer code. A subset of generative AI models known as large language models produce text and can be trained on existing text that does not need to be labeled, a methodology also known as unsupervised learning. As such, all available text on the Internet can be

used as training data, along with books and other texts. Other forms of generative AI may require labeled data, such as for image recognition.

Among the rapid increase in the use of generative AI systems, and the race to update existing ones and introduce new ones, a number of concerns have arisen. These include that the systems may be infringing copyright material in their training data; that they can create deep fake images or videos for misinformation and disinformation; that they can be used to create spam emails with malware to infect devices; and that they can "hallucinate" false results with seeming, and unwarranted, confidence.

These risks are leading governments to consider regulations or guide rails for relevant AI systems. The EU AI Act has already taken an approach to match the level of regulations to the risks of AI, as described below. Some regulatory issues are still open, such as whether to consider protections like intermediary liability protections, and if so, what the nature of these protections should be and the corresponding responsibilities of AI providers. Governments should be guided by the Internet Society Toolkit in assessing the possible impact of proposed regulations on the Internet.

Cloud and Edge Computing

Cloud services enable organizations to access infrastructure, platforms, or software through third-party providers and make content available to users through the Internet. This reduces the need for organizations to host software, content and services in their own infrastructure, lowering their investment costs and need for extensive equipment and staff, while also often providing state of the art cybersecurity protection. Cloud providers may aggregate data in one or several locations for processing and/or storage within a region, and thus it may not be hosted in the country from which the data is sourced and used.

There are two extensions of cloud computing that can move content or services into countries in order to be accessible closer to the users. Content delivery networks (CDNs) enable providers to cache popular content near or inside ISPs' networks to reduce the cost and latency of delivering it to users. Cloud companies may develop their own CDNs or use third party CDNs to deliver content. Edge computing moves access to relevant services closer to users, particularly for low latency services such as factory automation or autonomous vehicles. CDNs store data, while edge computing processes data – both use the Internet to bring in the relevant data and then deliver it to the end-users when needed.

Regulations may prevent users from fully benefiting from cloud services and content. Data governance or privacy regulations requiring data to be localized in a country may prevent data from being aggregated by cloud companies in regional hubs and may prevent them from investing in the country. Restrictions on content may prevent data from flowing into a country, while a lack of intermediary liability protection may prevent cloud companies from hosting content as intermediaries in the country. Finally, limits on the use of encryption in the country may impact the availability or usage of cloud services, given the difficulty of privacy protection and exposure to cybercrime.

Regulatory restrictions on cloud companies, and corresponding use of CDNs or edge computing, can leave the Internet in that country less open, globally connected, secure, or trustworthy. The restrictions should be assessed using the Toolkit presented in the following section.

Internet Society Assessment Toolkit

The analytical framework underpinning the findings and recommendations in this report is the Internet Society's Internet Impact Assessment Toolkit. Understanding its components is key to appreciating the systematic approach taken to evaluate the impact of policies on the Internet.

The Internet Society promotes the Internet Way of Networking as the foundation of a strong Internet, to enable advocacy on issues that help the Internet be more open, globally connected, secure and trustworthy. The Internet Society's Internet Impact Assessment Toolkit checks the impact of regulations on the Internet to ensure that they promote the Internet Way of Networking, by providing a framework for the analysis of proposed changes in policies, legislation, regulations and other aspects impacting the Internet.

The Internet Way of Networking identifies five critical properties of the Internet, along with a number of enablers to help the Internet to achieve a set of goals. The critical properties describe the foundations the Internet needs to *exist*, while the enablers describe the conditions that help the Internet to *thrive*.

By way of analogy, think of a city. There is a set of infrastructure that defines a city and enables it to exist: roads, public transportation, sewage, airports, a business district, housing, arenas, and so on. What makes a city thrive, however, are shops, restaurants, offices, arts, games, and concerts, which fill the infrastructure with activities and people. Going back a few years to the lockdowns during the pandemic, while cities continued to exist, the closures and cancellations meant they could no longer thrive. It was, in fact, the Internet that took the place of all that had been taken away, that provided some means for people to thrive. In turn, the critical properties ensured the continued existence of the Internet, and the enablers helped the Internet to thrive.

The Critical Properties that underpin the Internet make it unique and are necessary for the healthy evolution of the Internet and deliver benefits, as shown in Table 1.

Table 1: Critical Properties of the Internet (Source: Internet Society[5])

Critical Properties	Benefits
1. An Accessible Infrastructure with a Common Protocol that is open and has low barriers to entry	Unrestricted access and common protocols deliver global connectivity and encourage the network to grow. As more and more participants connect, the value of the Internet increases for everyone.
2. Open Architecture of Interoperable and Reusable Building Blocks based on open standards development processes voluntarily adopted by a user community	Open architecture creates common interoperable services, which deliver fast and permissionless innovation everywhere. The inclusive standardization process and demand-driven adoption ensures that useful changes are adopted, while unnecessary ones disappear.
3. Decentralized Management and a Single Distributed Routing System which is scalable and agile	Distributed routing delivers a resilient and adaptable network of autonomous networks, allowing for local optimizations while maintaining worldwide connectivity.
4. Common Global Identifiers which are unambiguous and universal	A common identifier set delivers consistent addressability and a coherent view of the entire network, without fragmentation or fractures.
5. A Technology Neutral, General-Purpose Network which is simple and adaptable	Generality delivers flexibility. The Internet continuously serves a diverse and constantly evolving community of users and applications. It does not require significant changes to support this dynamic environment.

Furthermore, the enablers can help the Internet to achieve a set of goals, as follows.

[5] For more details, see https://www.internetsociety.org/resources/internet-impact-assessment-toolkit/the-internets-five-critical-properties/

Table 2: Enablers of an Open, Globally Connected, Secure and Trustworthy Internet (Source: Internet Society)[6]

Goals	Enablers
An **Open Internet** that allows everyone to participate with a minimum of barriers, to use it, to innovate, and to grow and sustain the Internet as a force for good	• Easy and unrestricted access, for networks and users; • Unrestricted use and deployment of Internet technologies and standards; • Collaborative development, management, and governance of Internet technologies and standards
A **Globally Connected Internet** that is inclusive, allowing everyone to interconnect without geographical restrictions and use the full power of the network.	• Unrestricted reachability, for users to access to all resources and technologies made available on the Internet; • Available capacity, sufficient to meet user demand, including ports, bandwidth, and services
A **Secure Internet** that survives attacks, that supports everyone in maintaining integrity and confidentiality of the data. A secure Internet also means that its use does not create insecurity, such as botnets that are used in phishing scams.	• Data confidentiality of information, devices, and applications, usually accomplished with encryption, to protect data in transit and at rest; • Integrity of information, applications, and services, so that data is not modified in transit or at rest, and services cannot be manipulated
A **Trustworthy Internet** that people can depend on to be there, so that the Internet can be a base for worldwide services, everything from recreation to commerce to information.	• Reliability, resilience, and availability, to deliver services as promised, even in the fact of challenges; • Accountability, giving users the assurance that entities are acting in a transparent and fair way; • Privacy, giving individuals and groups the ability to understand and control what information about them is being collected and to control how it is used

[6] For more details, see https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/

The Internet Impact Assessment Toolkit checks the impacts of regulations on the Internet in two ways: mapping the effects of regulations on the critical properties of the Internet Way of Networking aims to preserve the unique value of the Internet; and analysing the impact of regulations on the enablers helps understand the implications for an open, globally connected, secure and trustworthy Internet. The overall goal is to help Internet stakeholders identify the possible effects, both positive and negative, of policies and regulations, to be able to make more informed decisions.

The next sections provide international examples of the relevant regulations of artificial intelligence and cloud and edge computing globally and identifies proposed or actual regulations in the six MENA countries, and uses the Toolkit to assess those regulations and make recommendations.

Policies and Regulations

This section explores some of the most prominent international examples of policies and regulations considered in this report before examining the laws of each of the focus countries.

International Examples

Data Governance

One significant focus of data governance relates to the transfer of data outside the country. This is understandable, as such transfers are increasingly common, resulting from increases in cross-border interactions between and among individuals and organizations, and as cloud companies aggregate data for processing and/or storage. While some countries still have no regulations on such transfers, enabling a free flow of data across borders, others have imposed data localization laws on categories of data that do not allow such transfers. In between, many laws around the world impose restrictions on the ability to carry out cross-border data transfers to ensure that the protection of data in the destination country meets the legal requirements imposed by their domestic law.

For example, the European Union General Data Protection Regulation (GDPR) conditions the transfer of data outside the European Economic Area (EEA) on sufficient safeguards. An interesting international example resulting from the GDPR that attempts to strike a balance between the need to control cross-border data transfers and the need to facilitate the transfer of data for businesses to be able to deliver cross-border services is the Data Privacy Framework Program of the US, the EU, the UK, and Switzerland. This program aims to facilitate data transfers from Europe to the United States while complying with data protection principles of the EU, the UK, and Switzerland using a self-certification system that allows businesses to transfer data to the US if they comply with the principles of the framework.

Privacy

Over the past few years, the MENA region has had significant developments in privacy regulation as many countries issued their first ever personal data protection laws or have had them enter into force. In addition to protecting data at rest, and alongside any restrictions on transfers of data, these laws provide a much needed protection against the misuse of the personal data of Internet users by requiring consent before any data is processed.

However, some laws have gaps when it comes to the use of personal data regarding new practices such as automated profiling. A good international example that attempts to address this gap is again the GDPR, which regulates automated profiling and requires transparency about how profiling is used to evaluate and predict a person's behavior. While not banned outright, the GDPR restricts the use of profiling for automated decisions that significantly impact individuals and grants individuals the right to object to such processing of data.

Intermediary Liability

In the early days of the commercial Internet, US courts issued two separate rulings on defamatory content posted by users on different online bulletin boards, which were early forms of intermediary platforms. The rulings held that bulletin boards that did not filter postings would not deemed liable for the defamatory content, while the bulletin boards that did filter postings would be deemed liable for all content on their service. Seeing that this led to the perverse incentive not to have any filters in order to avoid liability, the US Congress adopted laws with provisions protecting intermediary liability that led to the growth and variety of platforms seen today.

To enable online speech by individuals, the US Congress chose to protect online intermediaries regarding third party content. This shift is achieved through what is known as “Section 230” of the US Communications Act and, for copyright, Section 512 of the Digital Millennium Copyright Act. Section 230 of the Communications Decency Act shields platforms from liability for most content, including certain criminal content, unless the intermediary created the content. Section 230 does not impose any obligation to remove challenged content. The Digital Millennium Copyright Act (DMCA) offers a similar "safe harbor" (Section 512) for copyright infringement. Platforms following DMCA procedures to remove infringing content and address repeat offenders can avoid liability for their users’ copyright violations. These laws enable platforms to function and flourish without constant legal challenges or the risk of potentially crushing financial liability.

Encryption

Most countries around the world generally do not restrict the ability to use encryption technologies. However, some regulations may exist, such as controls on exported encryption strength or requirements for companies to assist law enforcement with decryption. This balance is often struck due to the importance of the Internet safety benefits obtained through encryption in promoting an Internet that is trustworthy and secure.

In addition to the four policy categories above, which impact emerging technologies, countries are beginning to develop regulations focusing on AI as a technology directly. For instance, as shown in the box below, the European Union recently adopted a relevant act.

Regulation of Artificial Intelligence

In 2024, the EU formally adopted the EU AI Act, which employs a risk-based approach regulating AI from a product safety perspective. Using this approach, AI technologies posing unacceptable risks are strictly prohibited, minimal-risk technologies remain unregulated, while high-risk and limited-risk technologies are subject to a tailored regulatory framework based on their level of risk. The primary focus of these regulations is on AI system providers, who are obligated to ensure quality, transparency, human oversight, and safety. In specific cases, a fundamental rights impact assessment may be required. The EU AI Act imposes significant fines that can amount up to 35 million Euros. The EU AI Act will fully enter into force after two years, and it will take time to assess the extent to which it succeeds at protecting users of AI technology.

Regulations in Focus Countries

This section looks in more detail at the laws and regulations of the six countries covered by the report, namely, Bahrain, Egypt, Jordan, Oman, Saudi, and the UAE and how these countries attempt to regulate data governance, privacy, intermediary liability, and encryption with respect to the emerging technologies.

Bahrain

In the area of **data governance**, Bahrain has an elaborate framework that regulates the use of data through the Personal Data Protection of Law 2018 along with a number of decisions issued by the Ministry of Justice, Religious Affairs, and Awqaf covering matters such as data subject rights, rules for processing sensitive data, complaint mechanisms, and the rules for the transfer of personal data outside Bahrain. These legal instruments attempt to draw a balance between the free flow of data on one side and ensuring that this data is adequately protected on the other side.

One of the ways in which the Bahrain law attempts to draw this balance is through the restrictions on the transfer of personal data outside Bahrain under article 12 of the Personal Data Protection Law of 2018. Under this article, it is prohibited to transfer personal data outside Bahrain, except under one of the two following cases:

> *"1. The transfer is to a country or territory that is listed in a record compiled and updated by the Authority, comprising of countries and territories that, upon the Authority's discretion, provide adequate legislative and regulatory protection for personal data. Such record shall be published in the Official Gazette.*

2. A transfer occurs upon the Authority's authorization on a case-by-case basis provided that the data will be subject to an adequate level of protection. The adequacy of such level of protection shall be assessed in the light of all the circumstances surrounding the data transfer operation, which shall include in particular the following:

i. the nature of the data to be transferred, purpose and duration of processing;

ii. the country or territory of origin of the data, its final destination, and available measures, in such countries and territories, to protect personal data; and

iii. Relevant international agreements and legislations that are in force in the country or territory, which the data shall be transferred to.

The aforementioned authorisation may be conditional or for a certain timeframe."

This approach permits Bahraini personal data to be transferred outside the country if the data is transferred to a country on the "white list" created pursuant to article 12(1) above, or if the data is transferred to a country authorised by the Bahraini authorities on a case by case basis. While this approach might seem reasonable, it still imposes restrictions on the free flow of data across borders, especially regarding cases where the country in question is not on the white list and requires specific approval from the Bahraini authorities. There is no public record of the number of requests made to obtain such authorisations or the outcomes of such requests. It is recommended for Bahrain to reconsider the data location rules found in the Bahraini Data Protection Law in a manner that allows data to flow freely between Bahrain and other countries that have suitable levels of data protection.

Bahrain has a sophisticated **privacy** framework through the Personal Data Protection Law and its implementation decisions issued by the Ministry of Justice, Religious Affairs, and Awqaf. Even though the Bahraini Personal Data Protection Law was one of the earliest data protection laws in the region as it came out in 2018, it already covered provisions to protect individuals from being subject to decisions made through automation tools, as it gives individuals the right under article 22 of the law to object to decisions made using automated processing if the decision relates to matters such as work performance, financial standing, or credit-worthiness of a person, and gives that person the right to have the decision reconsidered using means that are not completely automated.

When it comes to **intermediary liability**, the current legal framework in Bahrain can be seen as one of the most sophisticated in the region due to the presence of specific provisions in the Bahraini Copyright Law of 2006 that provide protection to service providers against liability for civil actions for copyright infringement by their users, if the intermediary meets certain conditions depending on the role of the intermediary in the processing of the infringing material, for example, that the transmission of the infringing content was not at the initiative or under the guidance of the intermediary and that the intermediary did not select the content or its recipients. However, Bahrain does not yet provide more comprehensive intermediary protections from liability for third party content. Such provisions

provide legal certainty to hosting service providers, social media platforms, and other intermediaries by providing them protection against civil liability for third party content uploaded to their servers or platforms, which in turn can act as an enabler for Bahrain-based businesses to create local hosting services and platforms and other innovative intermediary services.

Without these protections, domestic innovation and foreign investment would likely be stifled and local users would be deprived from accessing relevant platforms that exit the market, against the principles of a free and open Internet. For hosting service providers and other platforms to be able to operate with legal certainty in Bahrain, it is important for Bahrain to consider introducing a comprehensive framework to protect them against liability for third party content.

The use of **encryption** in Bahrain is not regulated and there do not seem to be restrictions on its use outside the provisions of the Cybercrime Law that prohibit the use of encryption (as an aggravating factor) in order to commit or conceal a crime.

The regulation of privacy and encryption in Bahrain supports the principles of an open, globally connected, secure and trustworthy Internet, while our recommendations address current data governance and intermediary liability statutes.

Egypt

In the area of **data governance**, the Egyptian Personal Data Protection Law of 2020 provides a comprehensive framework for the protection of privacy and the governance of the use of personal data. However, Chapter Seven of this law, which is titled "Cross-border Personal Data Transfers", stipulates in article 14 that "Transfer of Personal Data which is collected or prepared for Processing, to a foreign country, or its storage or sharing may only be undertaken if the level of data protection or security in the foreign country meets (or exceeds) the requirements stipulated under this Law, and *subject to obtaining a relevant License or Permit from the Center*." (italics added)

Such restrictions that require obtaining licenses or permits from the government prior to transferring data abroad are not in line with the best practices found in other laws globally including the laws of other countries in the region. Imposing such restrictions can make it difficult for providers to aggregate their data across different countries, which can in turn lead to a fragmented Internet. Such restrictions can also make it difficult for foreign cloud providers and apps to comply with the law, which in turn limits investment and the ability of users in Egypt to benefit from these services and goes against the core principles of a free and open Internet. It is therefore recommended that Egypt reconsiders the data location rules found in Chapter Seven of the Egyptian Personal Data Protection Law in a manner that allows data to move between Egypt and other countries that have suitable levels of data protection without the need to obtain a license.

As previously mentioned, the Egyptian Personal Data Protection Law provides a comprehensive framework for the protection of **privacy** and provides fundamental rights for data subjects. However,

this law falls short in addressing emerging privacy challenges posed by artificial intelligence and automated decision-making as it lacks specific provisions to protect individuals from algorithmic bias and discrimination, particularly in areas such as employment and creditworthiness. This lack of protection can put the privacy rights of users at risk and lower trust in the Internet.

To ensure robust privacy protections in the digital age, Egypt should adopt measures to safeguard against automated processing and profiling. Such measures would align with international best practices and provide greater transparency and control to individuals over their personal data. It is recommended that Egypt introduces provisions in its Personal Data Protection Law for the protection against automated data processing and profiling to protect privacy and enable users to understand or control how their data is used.

In the area of **intermediary liability**, the Egyptian Cybercrime Law has a number of provisions that hold the owner of a platform responsible for content published by a third party, and potentially subject to punishment if the platform owner knew of the existence of the criminal content and failed to report it to the authorities or if he facilitated its occurrence. Similarly, Egypt also has no framework for limiting the civil liability of a website owner for intellectual property infringements uploaded by third parties on their platforms.

As a result, creating and managing platforms in Egypt that allow users to upload and share content is risky for the owners and managers of such platforms as they would be required to monitor each single item uploaded to their platform, or else they would be held liable for it. Maintaining this is practically impossible to achieve, and as a result, it is risky for Egyptians to create alternatives to social media platforms such as Facebook, X, YouTube, or Instagram without putting themselves at serious legal jeopardy and creating a high level of uncertainty for these platforms. This goes against the principles of a free and open Internet. It is recommended for Egypt to consider creating a legal framework for protecting platforms creators and managers from liability for third party content.

Finally, Egypt is one of the few countries in the region that requires obtaining a permit from the government prior to using any **encryption** technology. This is stipulated in article 64 of the Telecommunications Law of 2003 and applies to all users of telecom services including Internet companies:

> "*Telecommunication Services Operators, Providers, their employees and Users of such services shall not use any Telecommunication Services encryption equipment except after obtaining a written consent from each of the National Telecom Regulatory Authority, the Armed Forces and National Security Entities*. […]"

Having such restrictions on the use of technology can put Internet users at risk, as encryption is fundamental to the safe operation of the Internet and is necessary for payment transactions, authentication of users, and generally protecting data in transit and at rest. Lack of encryption

threatens the security, stability, and safety of people. Furthermore, such provisions can also restrict the ability of local companies in Egypt from innovating in the area of cybersecurity due to the difficulty in obtaining the government approval required to use encryption, while also potentially restricting investment of companies, including cloud companies, whose clients require encryption of their personal and sensitive data. It is recommended for Egypt to remove all restrictions on the ability to use encryption so that the law does not impact the security or trustworthiness of the Internet.

Jordan

Jordan has recently issued a new Personal Data Protection Law and its regulation, and this law recognizes many of the commonly recognized **data governance** principles, drawing a balance between the free flow of data on one side and ensuring that this data is adequately protected on the other side. This is in line with international best practice such as the EU GDPR and the law does not appear to impose any serious restrictions on the free flow of data.

When it comes to **privacy**, the Jordanian law includes the right to consent to personal data processing, the right to access one's own personal data, and the right to request to have personal data deleted. The law also addresses the concept of "profiling", which is a practice that imposes new challenges for users in the age of artificial intelligence. However, the scope of the provisions relating to profiling is only limited to the right to object only if profiling goes beyond the objective for which the data was collected or is discriminatory. This falls behind the protections offered by some more progressive laws that give the data subject the right to be notified of the profiling practice and the right to demand that any decision made regarding them based on automated profiling is reconsidered using means that do not involve automated profiling, additions that would help to ensure an Internet that is trustworthy. It is recommended that Jordan reconsiders the provisions relating to profiling to notify the data subject of the profiling, to allow the data subject to object to the decisions made through profiling, and to impose additional measures to rectify such decisions.

In the area of **intermediary liability**, the Jordanian Cybercrime Law imposes strict liability against the person responsible for a website or a social media platform for content published on such website or platform, even if that content was published or created by a third party. Similarly, Jordan also has no framework for limiting the civil liability of a website or platform owner for copyright infringements uploaded by third parties on their websites or platforms. This makes creating and managing websites or social media platforms in Jordan that allow users to upload and share content risky for the owners and managers of such websites or platforms as they will be required to monitor every single item uploaded to their platform, or else they would be held liable for it. Maintaining this is difficult and costly, and as a result, it is impossible for Jordanians to create alternatives to social media platforms such as Facebook, X, YouTube, or Instagram without putting themselves at serious legal risk. This goes against the principles of a free and open Internet. It is recommended that Jordan considers creating a legal framework for protecting intermediaries from liability for third party content.

The use of **encryption** in Jordan is not regulated and there do not seem to be restrictions on its use.

The regulation of data governance and encryption in Jordan support the principles of an open, globally connected, secure and trustworthy Internet, while our recommendations address current privacy and intermediary liability statutes.

Oman

In the area of **data governance**, the recently issued Omani Personal Data Protection Law does not impose any serious restrictions on the ability to transfer personal data outside the country. It simply requires that the data controller ensure that the country to which the data is transferred provides a level of protection like that offered by Omani law.

On the other hand, Oman has several sectoral regulations with data localization requirements that mandate that the data is stored locally in the country. For example, the Regulation Governing the Provision of Voice or Video Telecommunications Service over Internet Protocol issued by the Telecommunications Regulatory Authority in 2022 requires in article 12 that the "data centers for the personal data of the beneficiary are located and kept within the geographical boundaries of the Sultanate of Oman", which means that providers of voice and video calling applications, such as Zoom, are required to physically store their data in Oman in order to be permitted to provide their services in Oman. Similarly, Oman's Executive Regulation of the Law of Carriage by Land which was issued by the Ministry of Transport and Communications in 2018 has a chapter dedicated to the governance of transportation apps and requires the data used by these apps to be located in the country.

Such regulations make it extremely difficult for some of the most popular apps in the world, such as FaceTime, WhatsApp, and Uber, to comply with Omani law, so as a result, these apps are effectively banned in Oman. This limits the ability of users in Oman to benefit from these apps and goes against the core principles of a free and open Internet. Oman should consider applying the general data protection law to VoIP and transportation data so that the data can be transferred abroad under suitable conditions, to enable full access to the respective apps and meet the goal of a globally connected Internet.

In the area of **privacy**, the Personal Data Protection Law and its regulation recognises basic rights to privacy such as the right to consent to personal data processing, the right to access one's own personal data, and the right to request to have personal data deleted. This is in line with international best practices such as the EU GDPR. However, this new law does not recognise some of the new challenges facing users in the age of artificial intelligence, and does not provide any special provisions for the automated processing of personal data using AI or the right to be informed of the use of profiling technologies in areas such as employment and education. The lack of protection regarding such new uses of personal data can put the privacy rights of users at risk, and is not in line with best international practices in this field, including laws in some other countries in the region. It is recommended that Oman introduces provisions for the protection against automated data processing and profiling to protect privacy and enable users to understand or control how their data is used.

When it comes to **intermediary liability**, Oman, along with Bahrain, is one of few countries in the region that have specific rules that address intermediary liability regarding intellectual property protection that provides protection for platforms, such as YouTube and others, in regard to third party content. This rule was issued by virtue of Telecommunications Regulatory Authority Decision 151/2008 regarding the Limitation of Liability for the Service Provider for Online Material on the Internet. According to this decision, intermediaries can be shielded from liability for intellectual property infringing content as long as the content is uploaded by a third party, not modified by the intermediary, and taken down by the intermediary upon its notification of the presence of the infringing content by the rights-holder.

However, Oman does not have clear legal provisions that limit the liability of intermediaries for content such as defamation and other illegal content outside intellectual property infringement. The lack of these rules means that platforms can face serious risks if they are held liable for content uploaded to their platforms by a third party. This can stifle domestic innovation and foreign investment and deprive local users of platforms, against the principles of a free and open Internet. It is recommended that Oman extends the protection from liability of intermediaries beyond intellectual property protection to include all third party content, in order to ensure an open Internet that is globally connected.

Finally, regarding **encryption**, the Omani Telecommunications Law of 2002 is one of the few pieces of legislation in the region that requires obtaining a license from the government prior to using any encryption technology. This is stipulated in article 48 of the law:

> *"It is not permitted, without a licence from the minister, to use encryption in telecommunications or computer networks. The licence shall specify the persons who may operate, its conditions, the fees imposed for issuing the licence, and the controls relating to the preservation of the encryption key, as specified by the executive regulation of the law."*

According to public announcements made by the government on social media, only one company has ever obtained this license since the issuance of this law more than 20 years ago. Having such restrictions on the use of technology can put Internet users at risk, as encryption is fundamental to the safe operation of the Internet and is necessary for payment transactions, authentication of users, and generally protecting data in transit and at rest, and the lack of encryption threatens the security, stability, and safety of people. Provisions such as article 48 of the Omani Telecommunications Law can also restrict the ability of local companies in Oman to innovate around cybersecurity due to the difficulty in obtaining the government approval required to use encryption, while also potentially restricting investment of companies, including cloud companies, whose clients require encryption of their personal and sensitive data. It is recommended for Oman to remove this provision to allow data to flow freely outside the country as long as the destination country provides an adequate level of protection. Further, it is recommended that Oman remove the requirement to obtain a license to use encryption technologies.

Saudi Arabia

Like other countries in the region, Saudi has recently issued a Personal Data Protection Law that provides a **data governance** framework for the use of personal data and guarantees a number of data subject rights. However, this law sets a complicated criteria for permitting data to be transferred outside Saudi as it states that the data can be transferred outside the country on the condition that the protection offered by the destination country is at least equivalent to the standard of protection guaranteed by Saudi law based on a criterion determined by the Saudi government. This criterion has been translated into a "white list" system under which data can be freely transferred to a designated list of countries only. The concept of the white list was introduced in September 2024 and at the time of writing, this list is not yet published.

In addition, Saudi law permits the transfer of data outside the white list if several conditions are met, including a certification requirement for the data controller. Given that this is still very new, how this will play out in practice is unclear as there is no white list and certification providers have not been identified. While this might seem at first glance reasonable, to ensure the protection of the rights of users, having a narrow white list and imposing stringent authorization requirements can put serious restrictions on the ability of domestic and foreign cloud providers and apps to comply with the law, which in turn limits innovation and investment and the ability of users in Saudi to benefit from these services, and goes against the core principles of a free and open Internet. It is recommended that Saudi reconsiders its data localization rules found in the Saudi Personal Data Protection Law in a manner that allows data to move between Saudi and other countries that have suitable levels of data protection.

As stated above, Saudi's Personal Data Protection Law and its regulation recognizes basic rights to **privacy** such as the right to consent to personal data processing, the right to access one's own personal data, and the right to request to have personal data deleted, all of which is in line with international best practice such as the EU GDPR. However, this law does not recognize some of the new challenges facing users in the age of artificial intelligence, and does not provide any special provisions for the automated processing of personal data using AI or the right to be informed of the use of profiling technologies in areas such as employment and education.

The lack of protection regarding such new uses of personal data is not in line with best international practices in this field as many laws, including laws in some other countries in the region, offer protection against automated processing and profiling. This lack of protection can put the privacy rights of users at risk and lower trust in the Internet. It is recommended that Saudi Arabia introduces provisions for the protection against automated data processing and profiling to protect privacy and enable users to understand or control how their data is used.

When it comes to **intermediary liability**, Saudi law does not provide specific provisions for limiting the liability of the platform for content published by third parties. The GCC Model Cybercrime Law, which was adopted by Saudi Arabia, stipulates that the court *may* exempt a website owner or manager from liability only if the content is immediately removed upon the request of the authority. This uncertainty

makes creating and managing web platforms in Saudi that allow users to upload and share content risky for the owners and managers of such platforms as they will be required to monitor every single item uploaded to their platform, or else they could be held liable for it. This is practically impossible to achieve, and as a result, it is impossible for Saudis to create alternatives to social media platforms such as Facebook, X, YouTube, or Instagram without putting themselves at serious legal risk, creating a high level of uncertainty for these platforms. This goes against the principles of a free and open Internet, and can stifle domestic innovation and foreign investment and deprive local users of platforms, against the principles of a free and open Internet. It is recommended that Saudi considers creating a legal framework for protecting website creators and managers for liability for third party content.

The use of **encryption** in Saudi is not regulated and there do not seem to be restrictions on its use. This regulation supports the principles of an open, globally connected, secure and trustworthy Internet.

United Arab Emirates

The UAE has a sophisticated legal framework for **data governance** regarding the protection of personal data under the Personal Data Protection Law, which does not appear to impose any serious restrictions on the flow of data between the UAE and other countries. However, the UAE has sectoral legislation that impose data localization requirements. For example, article 13 of the UAE Healthcare Information Law stipulates:

> *"It is not permissible to store, process, generate or transform the health data and information outside State -which are related to the health services provided inside State- except in the case where a resolution is issued from the Health Authority in coordination with the Ministry."*

While it might seem reasonable at first glance to have such laws in place to protect the privacy rights of patients, having the data within the country does not necessarily mean that the data is more secure or that the privacy of the users is more protected. Such restrictions might also make it difficult for certain healthcare providers to take advantage of the opportunities offered by foreign cloud providers or services, which in turn limits investment and the ability of users in UAE to benefit from these services and goes against the core principles of a free and open Internet. It is recommended for the UAE to reconsider the data localization rules found in the Health Information Law in a manner that allows data to move between the UAE and other countries that have suitable levels of data protection.

When it comes to **privacy** protection in general, as mentioned earlier, the UAE has a Personal Data Protection Law that guarantees the rights of data subjects and includes special provisions relating to automated processing of data under article 18:

> *"1. The Data Subject shall have the right to object to any decisions resulting from automated processing, including profiling, particularly those decisions which have legal impact on or adversely affect the Data Subject.*

2. Notwithstanding Paragraph 1 of this Article, the Data Subject may not object to the decisions resulting from automated processing in the following cases:

a. If the automated processing is agreed upon under the contract made between the Data Subject and the Controller.

b. If the automated processing is required under other legislations which are applicable in the State.

c. If the Data Subject gives prior consent to the automated processing as set out in Article (6) of this Decree by Law.

3. The Controller shall adopt appropriate measures to protect the privacy and confidentiality of the Data Subject's Personal Data in the cases referred to in Paragraph 2 of this article and shall not cause any prejudice to the Data Subject's rights.

4. The Controller shall include the human element in reviewing automated processing decisions at the request of the Data Subject."

This article is one of the most comprehensive provisions found in the region that protect data subjects from the automated processing of their personal data, through profiling and other practices, and also grants the data subject the right to demand that a human review is made in regard to decisions based on automated data processing, which is a progressive right necessary for the protection of data subject rights in the age of AI.

Regarding intermediary liability, the UAE law does not provide specific provisions for limiting the liability of the platform for content published by third parties. Article 53 of the Law on Combatting Rumours and Cybercrimes appears to suggest that a platform would be held liable for any content it makes available or stores even if that content is uploaded by a third party, if the platform fails to remove the content upon request by the government within a specific period of time. This makes creating and managing web platforms in the UAE that allow users to upload and share content risky for the owners and managers of such platforms as they will be forced remove any content the government orders them to remove, or else they would be held liable for it. The law provides a mechanism to appeal such orders in Article 63, but this mechanism does not appear to permit the platform not to fulfil the order, and in all cases, even if an appeal is made, the law deems the appeal rejected if the government does not respond to it within 7 days.

This makes it challenging for Emiratis to create alternatives to social media platforms such as Facebook, X, YouTube, or Instagram without putting themselves at serious legal risk and creates a high level of uncertainty for these platforms. This can stifle domestic innovation and foreign investment and deprive local users of platforms, against the principles of a free and open Internet. It is recommended that the

UAE considers creating a legal framework for protecting website creators and managers from liability for third party content.

The use of **encryption** in the UAE is not regulated and there do not seem to be restrictions on its use.

The regulation of privacy and encryption in the UAE support the principles of an open, globally connected, secure and trustworthy Internet, while our recommendations address current data governance and intermediary liability statutes.

Conclusion

While emerging digital technologies such as AI are introducing new opportunities, and challenges, for individuals, businesses, and governments, it is important to ensure that government responses address the challenges without impacting the core nature of what enables the Internet to exist and thrive. AI is not the only impactful emerging digital technology, as cloud and edge computing fundamentally changes access to, and the location of, data, content, and services. This report has demonstrated the utility of the Internet Society's Internet Impact Assessment Toolkit for this purpose in the context of six MENA countries.

As governments consider gaps or alterations to existing regulations or imposing new ones, in its advocacy role as a thought leader on promoting the Internet, the Internet Society developed the Internet Impact Assessment Toolkit to help guide governments. This Toolkit provides a means to determine if regulations promote the Internet Way of Networking, which considers a number of critical properties that the Internet needs to exist, along with a number of enablers to ensure that it continues to thrive and meets the goals of an open, globally connected, secure and trustworthy Internet delivering benefits for all.

This report uses the Toolkit to assess four Internet regulations, reflecting on the opportunities and challenges that they pose for new technologies. The two emerging technologies examined here are artificial intelligence and cloud and edge computing. The government policy and regulations we examine are data governance; privacy protection; intermediary liability protection; and encryption regulation. These are examined in six MENA countries: Bahrain, Egypt, Jordan, Oman, Saudi Arabia, and the United Arab Emirates.

Overall, we find that all of the countries have relevant regulations, but some may not cover all the existing or emerging issues raised by the new technologies, and in other cases gaps may exist. To ensure that the regulations help ensure an open, globally connected, secure and trustworthy Internet, we make a number of recommendations. In general, these recommendations in the four policy areas are as follows:

- *Data governance.* Data protection laws can be used to govern how different categories of data are managed in the country and the conditions under which data can be transferred to other countries. Most of the countries reviewed have some restrictions on the transfer of data to other countries. While it is important to ensure that data is moved to countries that offer suitable levels of data protection, regulations that prohibit transfers or restrict the movement of data to a select group of countries can act to fragment the Internet and prevent the development of inclusive AI systems and the use of cloud and edge services.

- *Privacy protection.* This is a subset of data governance regulations that aim to establish individuals' privacy rights and protect their personal data, and while it is important to protect those rights when personal data is transferred to other countries, overly restrictive regulations can act to fragment the Internet and restrict the availability of services using personal data. With the advent of AI, personal data may be used for automatic profiling or decision making, and laws should provide users with the right to be informed if they are the subject of profiling technologies. All the countries reviewed have laws addressing privacy of personal data, but most do not have provisions that protect against the use of personal data for profiling or automated decision making.

- *Intermediary Liability Protection.* Intermediaries such as content delivery networks, cloud providers, social media companies and Internet service providers host and deliver Internet traffic between end points but are not responsible for the content of the traffic. Intermediary liability protection shields them from liability for the content that they host, including content that may violate domestic laws or infringe copyright protections. The majority of the countries reviewed do not have any provisions that protect intermediaries from liability at all, and only two countries have provisions that limit the liability of intermediaries for copyright infringement (but not for other illegal content). A lack of such protections can limit domestic innovation and foreign investment in platforms that host content in the country.
- *Encryption regulations.* Encryption protects online information so it can only be read by those intended to have access, such as for messages, web traffic, and personal data in transit or at rest. The majority of countries reviewed do not have restrictions on encryption. Regulations limiting or preventing the use of encryption can limit privacy protection, increase the risks of cybercrime, and limit investment by cloud companies and others relying on encryption protection.

The recommendations provided in this report with regards to the four sets of regulations in each of the countries examined are intended to ensure an Internet that is open and globally connected, not fragmented, and one that is secure and trustworthy, not vulnerable to cybercrime and data leaks. This will enable investments in cloud and edge technologies in the countries to the benefit of individuals

and organizations, and innovation in AI systems that will deliver new services and opportunities for citizens.

The analysis presented effectively illustrates how the Internet Impact Assessment Toolkit can guide the development of 'smart' regulations, responsive to emerging technologies from a consistent and principled framework. The Internet Society commissioned this work in part to provide a concrete example of the toolkit in action, and its staff and members stand ready to help governments and other stakeholders apply the Toolkit to achieve the goal of an open, globally connected, secure, and trustworthy Internet for all.