WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

eco

GUIDELINES AND RECOMMENDATIONS: DIGITAL POLICY IN A GLOBAL CONTEXT

Berlin, 12. April 2023

The Internet has brought the world closer together. People across continents are able to communicate and share information with each other seamlessly. The Internet has proven to be a cornerstone of civilization supporting the advances in technological and societal progress throughout the global COVID-19 pandemic. As an infrastructure, it has become invaluable for governments and companies alike. Challenges towards its critical function as an information and communication hub arise from different angles and should be addressed by policymakers, companies and civil society in a joint effort to maintain the open and free nature of the Internet.

eco – Association of the Internet industry is committed to maintaining and expanding this infrastructure. Its aim is to contribute to the discussion and to forward recommendations for an open, sustainable and resilient digital economy and society.

The Internet industry has identified four fields of activity which should be covered by international institutions and governments engaging in global digital policy.

1. Strengthen global interconnectivity

The Internet is a global network which is composed of a multitude of different networks – both national and cross-border – and, per definition, is an international network. It derives its strength and success from being an open, interoperable agglomeration of networks. A segmentation of the Internet would not only be contradictory to the global structure and the interoperability of the networks and could endanger the Internet technically, organisationally, competitively and economically, but would also negatively affect the innovative capacity, the competition, the development of new business models and the diversity. Hence, allowing this interconnectivity to remain intact must be the primary objective of any government or international organisation engaging in Internet policy.

There is major concern about emerging trends and pursuits that could lead to segmentation and fragmentation of the Internet. Fragmentation of the Internet could endanger its technical and organisational functioning, while segmentation could undermine the accessibility of networks to citizens across the globe and adversely affect the way they interact with the World Wide Web.

The main focus must be to ensure that the free, open, technology-neutral and decentralised structure of the Internet is maintained and further advanced. A common European and internationally coordinated approach and the avoidance of nation-centred approaches in the area of global digital governance must be strived for.

The Internet can only function if it is managed collectively in line with multi-stakeholder principles and cannot be dominated by individual actors or governments. In the course of the IANA Stewardship Transition, many Western governments have explicitly committed themselves to the multi-stakeholder principle. It is important that these governments reflect this commitment in their actions and take a supportive role in fostering the multi-stakeholder approach for Internet governance. Since the open multi-stakeholder governance system has come under strain due to the increasing activities of national governments, it is ever more urgent to adopt a supportive role for open organisations as well as standardisation bodies and to coordinate with like-minded governments and actors.

When it comes to debating issues relating to the future design of the Internet, technical standards and interoperability, the necessary institutional framework is provided by bodies such as ICANN, IETF, RIPE, W3 Consortium, other international and European standardisation organisations, and groups and forums such as the Internet Governance Forum. These should be the relevant bodies deciding on the governance of the web. For the technical and organisational functioning of the Internet, the security and stability of the Domain Name System (DNS), the operation of the top-level domains and the allocation of IP addresses are essential.

In the case of international treaties that do not explicitly deal with the self-governance of the Internet, it must be ensured that the Internet's basic principles are maintained. Special sensitivity should be shown when addressing global governing bodies which might impact the structure and functioning of the Internet. Special attention has to be paid to the activities taking place in the ITU, since its decisions can greatly impact the work of the Internet's governing bodies.

Access to multi-gigabit-capable telecommunication networks and infrastructure is indispensable and of outstanding importance for all economies and societies. Therefore, it is of central importance that gigabit infrastructure as well as state-of-the-art mobile networks are rolled out and available worldwide.

The expansion and availability of high-performance digital infrastructure must be a priority. Efficient digital infrastructure forms the backbone of digitalisation. A functioning ecosystem of digital infrastructure also includes high-performance data centres, Internet exchanges, cloud infrastructure as well as co-location services and should not be limited to mere cable connections.

Governments and corporations sometimes take decisions which have unintended consequences on the Internet. It is important to conduct impact assessments to ensure that a policy proposal is fit for purpose without hampering the properties that make the Internet a robust, resilient, global infrastructure that brings economic development and opportunity to everyone.

2. A value-based approach for an interconnected world

Discussions on global Internet policy are often conducted against the background of different ethical assumptions and values. While these varieties in digital ethics may

appear to be marginal in domestic or European political debates, they become a major challenge when discussing the standards, the requirements, the aspects for proliferation and the design of digital networks, infrastructure and technologies.

Navigating these divergent, sometimes conflicting approaches to fundamental and civil rights remains a paramount field of conflict for companies, organisations and lawmakers. It will often prove difficult to reconcile these values and legal systems and to reach a common set of values leading to a basic consensus in order to safeguard and secure fundamental rights and freedoms. Challenges to values and fundamental rights should be addressed jointly by the Federal Republic of Germany, the European Union and the governments of other like-minded states through multilateral agreements and arrangements.

Internet companies and organisations are aware of their responsibility in this environment. However, the companies and organisations that provide and manage the core Internet infrastructure and network architecture at the technical and administrative level are facing a particular challenge. The free, open and decentralised structure of the Internet is a prerequisite for the equal, equitable and democratic participation of all actors across the Internet, be they governments, civil society or the industry. A segmentation or fragmentation of the Internet could jeopardise the worldwide accessibility and interoperability of networks, thus degrading the technical, organisational and economic viability of the Internet. The principle of interconnectivity on an ‘any-to-any’ basis must be preserved.

Free access to the Internet and to information is essential, especially when repressive regimes spread disinformation. We must protect communication. Access to information and independent reporting enables political discourse, especially in countries with repressive regimes which restrict access to information, limit independent reporting, and attempt to criminalise and censor undesirable media coverage. Broad and unhindered access to the Internet enables citizens to obtain reliable information and a diversity of viewpoints. Restricting access to parts of the Internet would undermine confidence in the multi-stakeholder model and in policies that aim to maintain global Internet interoperability. Regulation via technology is critical and must therefore be rejected. Maintaining core technical infrastructure functionality and neutrality must be preserved. There should be no regulation of traffic or forced routing of Internet data.

The cross-border dimension of the Internet also poses challenges that are not Internet-specific. More to the point, societal and political problems manifest themselves in global communication networks such as the Internet. Disinformation campaigns and manipulation can destabilise states and endanger international peace and societal coexistence. Access to the Internet and to reliable information as well as a free and independent media have an important function for resilient democratic states, especially when repressive regimes spread disinformation and fake news. Therefore, it is imperative that opinion-forming processes are protected from falsification and distortion, that hate speech is combatted, and that freedom of information and expression is secured. One of the central challenges of digitalisation and global connectivity is rooted in harmonising divergent value and

legal systems and working towards a common set of values and a basic consensus. To this end, clear rules and responsibilities are needed, especially in a cross-border context at the international level, so that decisive action is taken against disinformation, hate speech and violence on the Internet. This also includes improving information integrity in order to help citizens to better recognise disinformation and conspiracy ideologies as well as to develop the necessary media skills. Article 19 of the Universal Declaration of Human Rights and Article 11 of the EU's Charter of Fundamental Rights provide the basis and foundation for this.

Maintaining net neutrality and access to information and access to the Internet is a basic prerequisite. Especially in times of crisis, the maintenance of communication infrastructure is essential to guarantee free and independent information flows, particularly in countries with repressive regimes that restrict access to information, limit independent reporting, or suppress unpopular media coverage.

For Western democracies, privacy remains one of the more pressing topics when it comes to discussing global digital politics. With the General Data Protection Regulation (GDPR), the European Union has set the benchmark for protecting the privacy and personal data of citizens. Conveying this standard to other regions of the world, however, has proven difficult, with different understandings of privacy and other interests of governments and societies hampering the dissemination of this standard. In order to avoid a fragmentation of societies in the digital sphere, it is important to foster dialogue and mutual understanding of data protection practices and their respective impacts on civil rights. These efforts have to be furthered against the background of ongoing debates on the future shape of the transatlantic exchange of personal data as well as concerns about the functioning of the Domain Name System (DNS).

While data protection is often regarded as paramount when discussing civil and fundamental rights on the Internet, encryption is very often regarded as secondary. In recent years, several attempts have been made to establish a systematic weakening of encryption through different regulatory and legislative means; mostly without success. The right of individuals and companies to encrypt their data and communication is an important facilitator for ensuring privacy as well as increasing security and trust throughout the Internet. As such, it should be preserved by national legislators and respected in international agreements. Requirements from agencies combatting (serious) crime as well as signal intelligence often challenge this right to encryption, creating dangerous spillover effects that may well reach beyond the intended use of these requirements, as well as chilling effects for users and citizens of digital technologies. There is a broad consensus among the Internet governance community about the need to safeguard encryption.

3. Addressing global challenges

The Internet experienced its rise to becoming a substantial factor for society and the economy during a time when several challenges for the planet were emerging. The questions of how the earth's climates will develop in the coming years and

decades, as well as on how the growing population of the planet can be sufficiently supplied with services and commodities, are also of concern for actors on the web and the Internet industry.

The functioning of the Internet, and of digital technologies in general, requires a permanent supply of electricity. This makes operators of digital infrastructure dependent on affordable energy prices. Policymakers should therefore consider this circumstance when shaping energy policy and energy efficiency policy. Geopolitical events, like the ongoing invasion of Ukraine, have shown that the supply of fossil resources for electricity production has further major disadvantages in addition to its negative contribution to climate development. Securing a stable, reliable and affordable electricity supply for digital infrastructure through renewable energy, energy storage and other means should be jointly addressed by policymaking communities.

The challenges of global climate change and the realisation of the ambitious goals of the Paris Climate Agreement can only be resolved through international cooperation and the rigorous use of digital technologies. If digital technologies and applications are to continue to have a positive impact on the climate balance in the future, accelerated digitalisation in all areas of life and the economy is indispensable. Digital technologies will make a significant contribution to achieving the climate goals if existing innovation potential is rigorously harnessed. The potential to cut back on CO2 arises in a range of fields such as the mobility turnaround, efficiency increases through smart manufacturing, smart cities and other application scenarios.

In order to harness the sustainability potential of digital technologies, a holistic approach that combines digital infrastructure and technologies into an ecosystem is required. The prerequisite for this is a functioning digital ecosystem of energy-efficient data centres, cloud-based applications, high-performance gigabit infrastructure, 5G networks and software programmed for energy efficiency.

Moon-shot innovations shape the way digital technologies are deployed and have an impact on economic and social development in general. Cross-sectional technologies like Artificial Intelligence (AI) are currently difficult to assess and their potential impacts in many fields are not yet properly determined. It is thus imperative to exchange and discuss with other actors and governments the potential impacts of cross-sectional technologies, how to properly address these impacts, and how to handle any side effects these new technologies may bring. The Internet industry is convinced that innovations like AI cannot be curtailed but need to be embedded in a proper governance scheme which includes regulation, but is not limited to it. Thus, issues like access to respective technologies and the ability to employ them can be addressed. It is also important to create governance structures to address undesirable side effects, such as discrimination by AI through training with regiocentric datasets, in order to enable global acceptance of and participation in new technological developments. These exchanges should also include the question of where the use of respective innovations should be discouraged, i.e. on detrimental social engineering or weaponisation. The Internet

industry believes that digital technologies can provide a meaningful contribution to meeting global challenges and positively impact society.

4. Shaping markets in an interconnected world

Increased digital interconnection has fostered cross-border entrepreneurial activity on a continental scale. This has led to supply chains now stretching across the globe and products being transferred across the planet. This development has given rise to questions on how to shape and govern digital trade and the transfer of data. Moreover, increased globalisation has given rise to discussions on supply chains, their criticality, and questions over dependency on resources, products and technologies, which are not readily available through domestic exploitation or production. Digital Sovereignty has become the keyword which subsumes these discussions and is the factor that has gained prominence against the background of ongoing geopolitical developments.

International connectivity, data traffic and transfer of personal and non-personal data within and outside the EU are a foundation for the global connectivity of the economy, the society and science. This is underlined by the intensified international awareness and significance of data protection within and beyond European borders since the adoption of the European GDPR. Especially in view of the legal uncertainties following the Schrems II ruling of the European Court of Justice in 2020 (C-311/18), it is necessary to resolve the related issues of international data transfer. It is high time for a fundamental and sustainable long-term approach that enables legal cross-border and international data flows.

The increasingly important role that digital infrastructure, including data centres, plays for the economy, society and the state has further highlighted the questions revolving around their functioning, availability and supply chains. As connectivity and digitalisation increase, the threats to companies, states and citizens are changing. With the growth in importance and reliance on the functionality and integrity of digital technologies, services and infrastructure, these elements are increasingly exposed to targeted attacks. Current developments make it clear that global conflicts also pose a threat to IT security and that cyber threats and attacks are in general on the rise.

Strengthening IT security and the resilience of digital infrastructure is of great importance and must be perceived as a shared responsibility. Therefore, it is important that suitable approaches to improving Internet security are discussed at the European and international level and that responsible state behaviour in cyberspace is promoted. The Internet, as it stands, is a civilian infrastructure which should not be misused as a means to disrupt essential and vital services and institutions of society, or even be weaponised against them.

5. Guidelines

Subsuming the aspects above, eco – Association of the Internet industry puts forward the following guidelines for policymakers' consideration when shaping digital policy in a global context:

- Respect and foster the open multi-stakeholder approach applied to Internet governance through the established mechanisms and institutions, while curtailing negative political influence through selected nation-state governments exploiting this approach to further their political agenda.
- Respect and foster open, technology-neutral, accessible networks based on open, community-driven and developed standards.
- Uphold the principle of interconnectivity on an 'any-to-any' basis and avoid segmentation and fragmentation of the Internet through technological, legal-political or societal measures.
- Conduct impact assessments on policies or decisions that might affect the Internet, in order to avoid unwanted consequences on the properties which make the Internet resilient, grow and thrive.
- Foster and secure free access to the Internet for citizens across the globe while mitigating uncertainties arising from different legal systems.
- Acknowledge privacy and encryption as important factors for citizens to conduct safe and confidential communication and to build trust in digital technologies.
- Ensure that digital infrastructure is provided with reliable and economical access to electricity.
- Understand digitalisation as a driving force and a prerequisite for climate-friendly transformation in manufacturing, logistics and living.
- Foster and support development in cross-sectional technologies that bear great innovative potential and ensure access and understanding of said technologies.
- Establish sustainable foundations for the legal exchange of data across borders.
- Understand cybersecurity as a means to strengthen trust in and reliance on digital solutions and guard reliability for political actors to be able to maintain operations in networks while harnessing the understanding of technologies and their functions and shortcomings, in order to remain technologically sovereign.