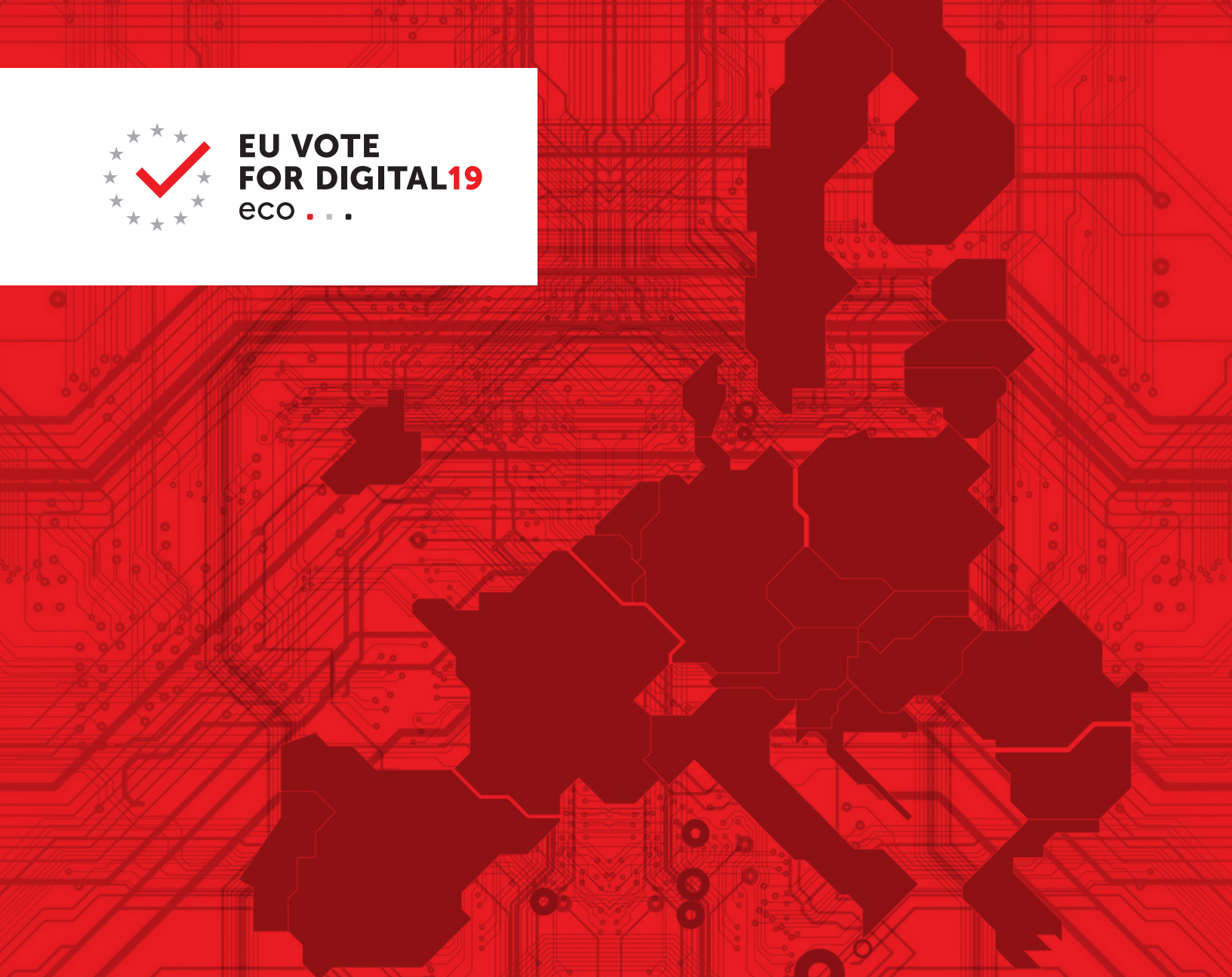
EU VOTE
FOR DIGITAL19
eco



EU AGENDA for modern digital policy-making

eco's 19 Core Demands for the 2019 European Elections

eco
ASSOCIATION OF THE INTERNET INDUSTRY

Contents

EU AGENDA for modern digital policy-making

It is no longer possible to imagine everyday life without digitalization and the Internet. Whether it's the mobile phone, smart TV, home lighting, or the car – almost everything can now be connected through the Internet and supplied with the latest information, video streams, and updates, or can be opened or controlled via the Internet. Digitalization is also making significant advances in the economy. Developments such as the connected car, the Internet of Things, artificial intelligence, or the 5G mobile communications standard offer just a few examples of where we are heading.

Digitalization represents a significant challenge for us all. International corporations as well as small and medium-sized enterprises (SMEs) have to adapt, and politicians are also confronted with a multitude of new questions. The structural change is affecting almost all areas of the economy and is exerting an impact on existing and future business models. While all of this opens up many opportunities and possibilities, it also presents us with numerous new challenges.

In order to maintain Europe's competitiveness in the global market in the future, a strong digital single market is needed, and for digital change to succeed in all sectors of the economy, the appropriate framework conditions for digitalization need to be established. A unified legal framework for the digital markets and the operators of digital technologies and services would facilitate the innovative strength of existing industries and economic players, would enable new value chains and business models, and lastly – and importantly – would strengthen new companies and start-ups.

During the 2014-2019 legislative term, a large number of proposals were presented by the EU Commission with the aim of adapting or replacing existing regulations. The spectrum of topics addressed ranged from IT security to copyright law. Despite the multiplicity of initiatives, the development of the digital single market is far from complete. On the contrary, it is a project that is constantly evolving. The next step is to be the transition of the specific digital single market to become a part of the general European single market.

From eco's point of view, many political plans and projects suffered from a lack of understanding of digital technologies, not just in terms of their opportunities and challenges, but also in terms of their practical limitations. Regrettably, the discussion about advancing digitalization is conducted with an underpinning mindset that is skeptical of technology and the Internet and that is strongly influenced by the interests of established industries. An imbalance has emerged. Moreover, the bodies involved in the Commission, the committees in Parliament and the Council and ministries in the EU Member States have sometimes failed to adopt a common idea or a common goal. Here eco sees potential for optimization in the future.

But the EU also needs to further develop in a number of specific areas. eco would like to highlight particular priorities, areas of activity and action, as follows.

eco's 19 Core Demands for the 2019 European Elections

IT Security, State Surveillance, and Law Enforcement

1 The EU must ensure a pan-European approach to the fight against cyber threats, prevent Member States from taking national unilateral action, and also ensure the involvement of citizens.

2 The EU needs to prohibit blanket and government surveillance without specific cause of the European population in all Member States and instead do more to promote encryption and secure services.

3 The EU must adopt a standard approach to the prosecution of cyber crime and establish fair rules and standards – with regard to small and medium-sized enterprises – for cross-border data access in investigative proceedings.

Data Protection and Privacy Online

4 The EU must ensure that Member States implement and apply the General Data Protection Regulation in a uniform and consistent manner

5 The European Data Protection Board must involve the Internet industry more closely in its work.

6 The EU Commission and Parliament must engage in an open dialog with industry in discussing plans for the ePrivacy Regulation in order to avoid a fragmentation of the European data protection framework.

7 The EU Member States must speak out categorically against blanket data retention without specific cause.

Violations of Law and Liability on the Internet

8 The EU must not further weaken the solid and tried-and-tested regulatory framework for the provision of digital services in Europe through inconsistent changes to the e-Commerce Directive and the "Notice and Action" principle.

Continued: eco's 19 Core Demands for the 2019 European Elections

9 The EU must develop a cooperative and socially inclusive approach to dealing with hate speech and fake news, one which involves industry and the public and which does not rely solely on technical solutions.

10 To combat online crime, the EU must strengthen and expand law enforcement and the work of globally networked hotlines.

11 The European Commission and Parliament must develop a modern European copyright law that reconciles the legitimate interests of authors and creators, distributors, the Internet industry, and users.

Infrastructure and Networks

12 The EU must develop a consistent strategy – incorporating elements such as research, education, training, and energy costs – to ensure digital self-determination on the basis of high-performance digital infrastructures.

13 The EU needs to maintain and further develop its well-balanced regulatory approach to safeguarding the free Internet and being innovation-friendly.

Services and Competition

14 Within the scope of media convergence, the EU must establish a consistent regulatory framework which subjects similar services and products to the same rules.

15 The EU must take a firm stand against protectionist tendencies that penalize digital services and business models, both in individual Member States and at European level.

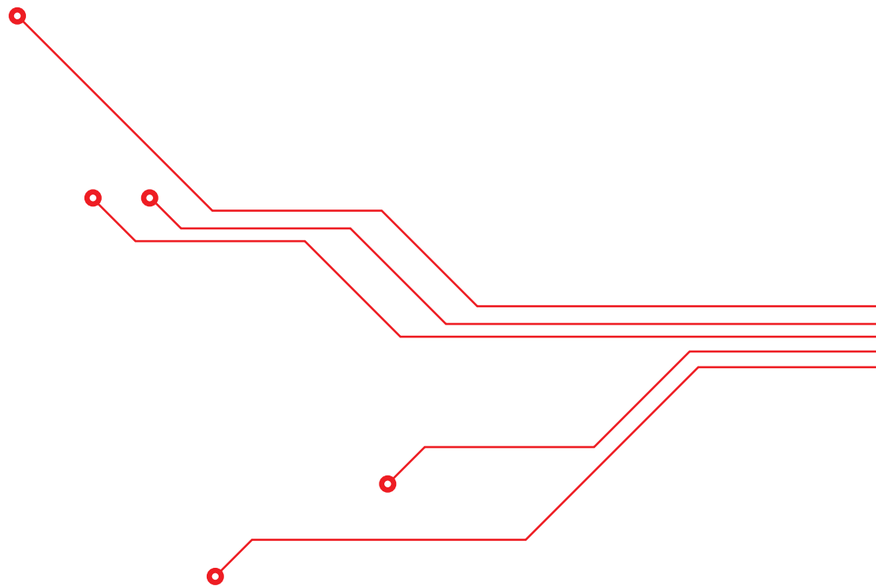
16 The EU must take greater account of start-ups and small and medium-sized enterprises in legislative proposals and establish appropriate and equitable market and competitive conditions.

Digital Industry and Digitalization

17 The Council of the European Union should pull back from its plans for a digital tax and instead work towards a single taxation system that taxes all companies according to the same principles.

18 EU Member States must abolish internal virtual borders and guarantee free movement of data within the EU.

19 The EU must develop a coherent European strategy to strengthen the development and deployment of artificial intelligence and blockchain technologies.



IT Security, State Surveillance, and Law Enforcement

1 The EU must ensure a pan-European approach to the fight against cyber threats, prevent Member States from taking national unilateral action, and also ensure the involvement of citizens.

With increasing connectivity and digitalization, threats for companies, states and citizens are changing. Aside from conventional criminals, states or their proxies are increasingly being regarded as initiators of attacks. It is not only citizens, companies, and Member States that have to cope with this increasing danger and these challenges; the EU also has a special responsibility here and must provide targeted support to Member States. However, it must not disregard its central role of protecting fundamental rights.

The cooperation between European security institutions – such as ENISA and Europol – and the Internet industry must be further intensified in order to tackle challenges efficiently and effectively. Fundamental rights, security, and economic feasibility must be brought into harmony with one another. In tackling shared dangers and threats, it is important to refrain from excessive regulations and impetuous regulatory measures. Sufficient operational capacity must also be put in place at EU and Member State level. IT security must be understood as a common challenge that government institutions, companies, and users can address together responsibly and efficiently.

The Cybersecurity Act constitutes a central building block for countering dangers in the Internet and technology sectors. It is intended to put into effect the mandate for the European IT security agency ENISA – an important step for IT security that eco is fully in favor of. ENISA's first central task should be to coordinate and monitor the consistent and stringent implementation of the NIS Directive in all EU Member States. The guidelines of the EU Commission provide a sensible basis and starting point for this.

One challenge will continue to be the certification framework envisaged by the Cybersecurity Act. On the one hand, this specifies transparent and comprehensible security requirements. On the other hand, due consideration must be given to the special requirements of modern information technology and open platforms and to the need for implementation which is geographically as widespread as possible. This balancing act between the necessary abstraction and the concrete need for security can, for example, be managed through standardization processes and only in cooperation with the Internet industry.

The EU and ENISA must ensure that Member States do not take national unilateral action and that a necessary pan-European approach is taken. Otherwise, this will have negative consequences for the European (digital) single market as a whole, as well as for individual Member States and their companies.

2 The EU needs to prohibit blanket and government surveillance without specific cause of the European population in all Member States and instead do more to promote encryption and secure services.

However, it is not only companies and European authorities that need to make a contribution to improving security in networks. The EU Member States must also critically review any efforts to introduce built-in back doors for authorities or central encryption systems with "master keys" for investigating authorities. The compilation and non-disclosure of vulnerabilities in services, products, and equipment (so-called zero day exploits) are not conducive to the general improvement of IT security. Corresponding measures also undermine the confidence of users in services and products as well as in the use of the Internet in general.

In addition, nationwide and state measures undertaken without specific cause for the surveillance of the European population, such as the repeatedly re-emerging measure of blanket data retention, must be prevented in all Member States. The European Court of Justice has presented clear case law to this effect. The EU Parliament and the EU Commission must also make a commitment to this legal position.

The loss of reputation caused by the measures described, whose added value for actual police work and investigations can only be classified as questionable, is unacceptable to the Internet industry.

A commitment to strong encryption, support for the development and deployment of easy-to-use encryption, and the express rejection of any form of weakening or undermining of encryption techniques would strengthen overall confidence in networks and services, promote confidence in digitalization, and strengthen Europe as a single digital market.

3 The EU must adopt a standard approach to the prosecution of cyber crime and establish fair rules and standards – with regard to small and medium-sized enterprises – for cross-border data access in investigative proceedings.

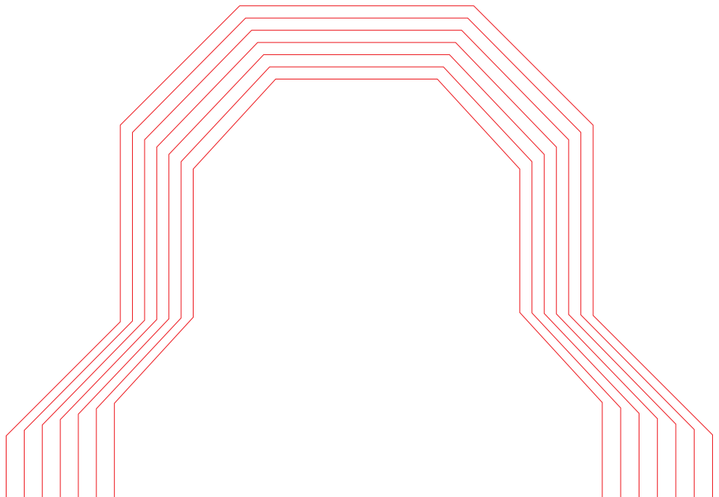
An increasingly connected world regrettably also gives rise to cyber crime in a wide variety of guises and forms, which also poses challenges to law enforcement authorities in the Member States. Here it is necessary to find a common approach within the EU and to establish and guarantee rules and standards for rapid cross-border data access for the investigation and prosecution of cyber crime.

Not long after having adopted the European Investigation Order in 2014, the EU presented a new, additional proposal in the form of the

Continued: IT Security, State Surveillance, and Law Enforcement

e-Evidence Regulation. Here the thinking is to maintain the high protection and security standards which prevail in some individual Member States, or to adapt and adopt these to ensure compliance at this high level throughout the EU. In addition, it is intended to minimize the risk of abuse and to eliminate the liability risks for Internet service providers.

Greater efficiency in the exchange of data with law enforcement is generally to be welcomed, but must not be at the expense of SMEs or the citizens concerned, especially in terms of unrealistic response times and impractical verification measures. The fulfilment and responsibility of sovereign tasks must not be transferred to the private sector.



Data Protection and Privacy Online

4 The EU must ensure that Member States implement and apply the General Data Protection Regulation in a uniform and consistent manner.

With the introduction of the General Data Protection Regulation (GDPR), the basis was established for standardized data protection in Europe. Its basic principles and requirements now apply in all EU Member States. The institutional framework to be created by the GDPR is also beginning to take concrete shape with the establishment of the European Data Protection Board.

It is now important to ensure that the implementation of the GDPR throughout the EU is consistent and in accordance with the purpose of the regulation.

5 The European Data Protection Board must involve the Internet industry more closely in its work.

However, the resolutions adopted to date by the Article 29 Working Party (which was absorbed into the European Data Protection Board in the wake of the GDPR) cast doubts concerning systematic and appropriate implementation when it comes to ancillary matters (e.g. the transfer of playlists of music services).

For this reason, eco calls for a targeted structuring of the work of the European Data Protection Board and a closer integration of the competence of the Internet industry into its work. This should also considerably accelerate the practical concretization necessary for the application of the GDPR.

Furthermore, it has to be recognized that the Internet does not stop at national borders and that, for example, the consistent implementation and application of the GDPR can pose a challenge to website operators around the world.

The reaction of numerous American news providers – namely, the blocking of European access to their websites – is probably the most prominent example of the worldwide effects of the GDPR and means a restriction of information availability for EU users.

Such developments should be countered by proactive measures on the part of the EU, such as a dialog with website operators in third countries for a better understanding and easier implementation of the new requirements.

On the other hand, in eco's view, the EU-US Privacy Shield provides a basis for structuring data traffic with third countries. Corresponding agreements or the recognition of adequate data protection must also be made with Great Britain and other regions of the world.

Continued: Data Protection and Privacy Online

6 The EU Commission and Parliament must engage in an open dialog with industry in discussing plans for the ePrivacy Regulation in order to avoid a fragmentation of the European data protection framework.

If the plans of the EU Commission and Parliament are to be pursued, the regulation of data protection on the Internet has not yet been completed with the GDPR. The ePrivacy Regulation is another legislative act in the pipeline, and is one which could have far-reaching effects on networks and services – and also on digital business models in Europe.

The GDPR has already led to restrictions for website operators and digital services, and a further tightening of data protection regulations beyond this general measure would be likely to disadvantage Europe as a business location. Such a regulation would ultimately benefit products and services which mainly generate and process user data outside of Europe and which develop their business models on this basis.

Conversely, the inconsistent requirements and specifications of the ePrivacy Regulation would undermine a strengthening of Europe as a digital location and exacerbate the problem of the acceptance and implementation of European data protection initiatives through unclear definitions of terms.

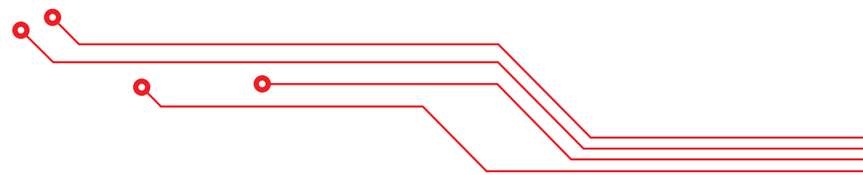
The ePrivacy Regulation should be discussed in an open dialog between policy-makers and industry in order to enable a Europe-wide understanding of the goals to be attained and potential problems which might be encountered.

7 The EU Member States must speak out categorically against blanket data retention without specific cause.

Explaining blanket data retention undertaken without specific cause – and prohibited by the ECJ – to users is a difficult task in its own right, but this is not the only reason for eco to categorically reject it. It is highly unfortunate that, in Germany, the concerned companies in the Internet and telecommunications sectors have already twice had to invest considerable time and expense in terms of personnel and financial resources to implementing what is effectively unlawful blanket data retention. No evidence has been offered to date of benefits of such retention, nor have efforts been made to empirically support their value.

The technical procedures required for blanket data retention, as well as the administrative and personnel costs, place a massive burden on the companies concerned. This constitutes an infringement both of their fundamental rights and of those of data subjects.

The result is that, for SMEs in particular, the financial resources required to develop innovative telecommunications services and to set up and expand high-performance telecommunications networks and gigabit infrastructures are diverted to implementing blanket data retention. In addition, legislative proposals that are challenged before the ECJ and the national courts and which are lacking in substance and durability lead to a lack of the essential investment, planning, and legal certainty for the companies concerned.



Violations of Law and Liability on the Internet

8 **The EU must not further weaken the solid and tried-and-tested regulatory framework for the provision of digital services in Europe through inconsistent changes to the e-Commerce Directive and the "Notice and Action" principle.**

For almost 20 years, the e-Commerce Directive has been one of the central cornerstones for the provision of digital services in Europe and has formed the basis of national legal regulations. It has enabled the evolution of the Internet and its many services in the form we know today. At the time of its adoption, obligations and liability rules for Internet service providers were agreed upon. The provider privilege ensured that content was subject to follow-up control and that Internet service providers could become directly liable for infringements by third parties in the absence of consistent follow-up ("Notice and Action" or "Safe Harbour").

Services offered on the Internet and usage habits have changed since then, and for this reason amongst others, there have been increased calls for a change in the e-Commerce Directive and the "Notice and Action" principle. Initially, codes of conduct were used to oblige large providers to take more active action against unwanted content. Measures in the two subject areas of child sexual abuse material (CSAM) and terrorist content lowered the thresholds for further steps and for the extension of measures (e.g. deployment of filter and AI technologies) to other content.

This tendency towards technological solutions constitutes a risk-laden development, in eco's view. The susceptibility of such solutions to errors and technical limits poses a threat to the fundamental rights of users and companies (in particular in the areas of freedom of expression and entrepreneurial freedom). Of paramount concern is the fact that measures are often tailored to the circumstances of the largest players in the market and that SMEs and (the desired European) start-ups are left out of the equation. This development is particularly problematic because the majority of European ICT companies are small to medium-sized enterprises.

9 **The EU must develop a cooperative and socially inclusive approach to dealing with hate speech and fake news, one which involves industry and the public and which does not rely solely on technical solutions.**

Over time, platforms and services have evolved on the Internet that have not only acquired a massive profile, but are also used on a daily basis by the majority of Internet users – above all, these include social media such as Facebook, Twitter, LinkedIn, or Instagram. Users share (personal) information through these platforms and companies (e.g. media companies) use these platforms to draw attention to their content and articles or to make their content directly available.

As a lamentable consequence of the latest US presidential elections, supposedly new phenomena such as filter bubbles and fake news took on a prominent register. Another term in this category is hate speech, a term emerging in particular in the wake of the 2015/16 refugee movements. None of these phenomena are entirely new. However, the digital distribution channel alone is nowadays easier to use and is an inexpensive and uncomplicated means of rapid, broad distribution and anonymized attacks, or attacks using a pseudonym.

However, these developments should not be countered with unreflective measures. The solution can only be arrived at through cooperation between the groups concerned – citizens, companies, and the state. It would be delusional to believe that technology alone would be able to master the challenges facing society as a whole.

10 **To combat online crime, the EU must strengthen and expand law enforcement and the work of globally networked hotlines.**

A similar development – towards more technological solutions and automation – can also be seen in the fight against the dissemination of terrorist and child abuse material on the Internet. It should be noted, however, that the nature and seriousness of crimes in these areas are of a special nature. This is because there is a comparably uniform legal situation worldwide and the relevant content can be identified relatively unambiguously. Relevant technical support may be useful here – within this limited area of application and within certain bounds.

But even here, technological approaches alone cannot prevent everything. The work of specialized and globally networked hotlines, and cooperative initiatives with Internet service providers, offer much more promise of success. In this context, it should not be forgotten that a rigorous investigation of the perpetrators and criminal prosecution are fundamental for combating and prosecuting the spread of terrorist and child abuse material on the Internet.
eco calls for resolute support for this internationally successful and cooperative model. Its success is confirmed by the high take-down rates and presents a clear case for its continuation into the future in its current form, so that the fight against this illegal content can continue to be successful.

.

11 **The European Commission and Parliament must develop a modern European copyright law that reconciles the legitimate interests of authors and creators, distributors, the Internet industry, and users.**

Modern technologies and above all the Internet have made the distribution of digital content in the form of news and texts, pictures and

Continued: Violations of Law and Liability on the Internet

photos, music, videos etc. easier, cheaper, and faster than ever before. This has produced many benefits. Journalists and bloggers have been able to access readers more directly; young artists have been facilitated to step into the spotlight more easily and become international pop stars; "YouTubers" and "Instagram influencers" have become job titles. However, an area that has not kept pace with this development and which has barely developed further is that of copyright.

The Internet offers European companies and users substantial potential that can be exploited. Artists, authors, journalists, etc. must not be left out of the loop. Modern copyright law should not play off the provision of digital content and its appropriate remuneration and uncomplicated application against each other. The protection of fundamental rights must also be taken into account and the technical possibilities must be respected. Modern copyright law must also include the technology-neutral development of rights and obligations.

eco endorses the vigor in this field of law, but calls for the joint development of modern regulations in order to both reconcile the legitimate interests of authors and creators, distributors, the Internet industry, and end users, and to capitalize upon digitalization's potential.

The current discussion status and the draft proposals submitted for the amendment of copyright law are disadvantageous for the Internet industry and will have an inhibiting effect on innovation. Copyright must not be used to protect traditional business models, and new business models must not be disadvantaged on a one-sided and unbalanced basis.

Infrastructure and Networks

12 **The EU must develop a consistent strategy – incorporating elements such as research, education, training, and energy costs – to ensure digital self-determination on the basis of high-performance digital infrastructures.**

The further digitalization and competitiveness of Europe as a business location requires the Europe-wide availability of high-performance gigabit networks, gigabit-capable connections, and state-of-the-art mobile communications networks. A functioning ecosystem of digital infrastructures also includes data centers, colocation providers, and cloud infrastructure providers, as well as reliable and high-performance Internet exchange points.

According to the EU Commission, only six percent of the data available worldwide is physically stored (hosted) in data centers in Europe. Viewing this sub-segment of digital infrastructures strategically as constituting the backbone of digitalization will therefore be decisive for the success of European digital performance and digital self-determination.

From eco's point of view, a consistent strategy is required, which must incorporate research in this area and its promotion, training and further education and, last but not least, a competition-conducive approach to energy costs. Since these fields and responsibilities are invested in different state bodies, an interdisciplinary and interdepartmental approach is necessary.

When it comes to the development of high-speed networks, in addressing the need to adapt public funding schemes, a significant increase in the current 30 Mbit/s threshold should be introduced. This is ultimately necessary in order to enable the objectives of the EU Commission's Gigabit Strategy 2025 to be achieved.

eco is firmly of the opinion that the expansion should take place primarily in the private sector and that the distortion of competition caused by subsidies must be prevented. Bearing in mind the perspectives of social participation, research, the economy in general, and the Internet industry in particular, care should be taken to ensure that all white and after that gray areas are opened up as quickly as possible in order to be gigabit-capable.

The associated positive effects for the economy, society, and the state are clear and indisputable. The Internet industry would naturally especially benefit and could thus offer its customers services that are more efficient. In this context, we can only encourage the European institutions to take measures that contribute to the realization of the digital single market and that are in line with private competition.

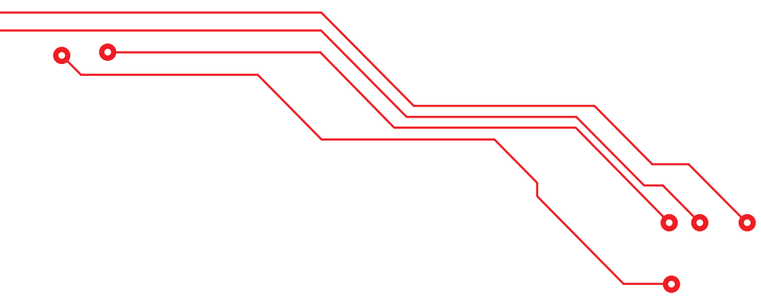
Continued: Infrastructure and Networks

13 **The EU needs to maintain and further develop its well-balanced regulatory approach to safeguarding the free Internet and being innovation-friendly.**

The Internet is facilitating the creation of a digital ecosystem that is distinguished by low-threshold market access, low market entry costs, and scaling effects. It thereby enables smaller and still undiscovered companies and start-ups in particular to offer innovative new services and business models.

eco regards the principle of net neutrality as a valuable building block for the Internet industry, and sees its anchoring in the Telecoms Single Market Regulation and concretization by BEREC as an important step in the right direction. The application of this principle shows that the national regulatory authorities have been equipped with suitable instruments which, in the main, they are applying in moderation. This balances the interests of users with providers of Internet access, content, and applications.

For the future, it is important to maintain and further develop this balance, e.g. with the 5G mobile communications standard, in order to promote innovation on the one hand and maintain a free Internet on the other. From eco's point of view, the codification of net neutrality also represents a competitive advantage for Europe in international terms.



Services and Competition

14 **Within the scope of media convergence, the EU must establish a consistent regulatory framework which subjects similar services and products to the same rules.**

The Audiovisual Media Services (AVMSD) Directive is central to the regulatory treatment of different types of media in the age of increasingly converging media forms. The revised version also continues to distinguish between services which are technically linear (classic TV and radio services) and those which are non-linear (online services such as video portals or video-on-demand services). In the practical implementation of the directive in the Member States (e.g. in Germany), this leads to attempts to extend the principles of broadcasting regulation to apply to the Internet. However, this is not in the interest of a modernization of the legal framework. The Internet differs fundamentally from broadcasting, both technically and in terms of its various forms of access.

Within the scope of media convergence – which makes it possible to transmit TV and radio programs in a linear manner on the Internet or to make them available on demand in a non-linear form in a media library or a catalog – eco no longer considers the technical feature of linearity to be a sensible differentiation criterion for regulation. Rather, the aim should be to create a consistent and comparable regulatory framework that subjects similar offers to the same regulations.

Regardless of the nature of the supplier and of the transmission or usage preference, directly competing offers should be subject to an equivalent level of regulation in order to avoid distortions of competition. Possibilities for law enforcement should also be taken into account and deregulation should – wherever possible – be favored over regulation that cannot be effectively enforced.

A further priority is to generally examine where and how deregulation is possible. For example, German broadcasting regulation subjects platforms and platform providers in particular to a strict regulatory framework that is evidently too extensive and detailed. In order to further promote the availability and provision of new services as well as offers and competition in the European single market, when it comes to the AVMSD, care should also be taken in the future to ensure that it does not impose too narrow a framework for the development of platforms and user interfaces.

New products and services – e.g. smart loudspeakers and televisions or the Internet of Things, artificial intelligence, blockchain and distributed ledgers, or Big Data – are not only creating a paradigm shift in the interaction between people and Internet technologies, but also offer potential for technological developments and companies. The future application of artificial intelligence in particular will bring with it extensive cross-sectional functions in the field of digitalization and reorientation of industrial and service processes, and this will

Continued: Services and Competition

pave the way for innovative business models. At the same time, there is growing concern about the demands placed on these products.

Security concerns play just as important a role here as matters of product design and requirements. Practicable policies must be adhered to. At the same time, an in-depth analysis must be carried out of any additional practicable rules and the extent to which these rules also accommodate digital sales channels and business models. Digitalization must not be used as a pretext to cement the business models and siphoning mechanisms of established industries by means of misguided regulation.

15 The EU must take a firm stand against protectionist tendencies that penalize digital services and business models, both in individual Member States and at European level.

The Internet industry and digitalization are popularly described as "disruptive", as they shake up the market of established companies with innovative services and offers. Some attempts (such as with the AVMSD) are being made to squeeze services into existing formats without paying attention to the specificities that new technologies bring with them. On the other hand, attempts are being made to set new standards for the Internet industry in order to offset its advantages and thus minimize disadvantages for the "old economy" (e.g. digital tax).

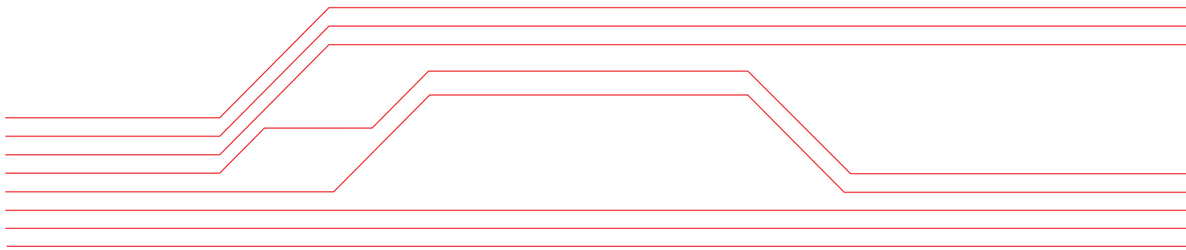
With its multitude of different business areas and products, the Internet industry itself is highly heterogeneous. eco is therefore of the opinion that no specific regulations in general competition law can be created for it and that any regulations must be differentiated in order to do justice to heterogeneity and to give the Internet the necessary room to maneuver as the innovation engine of the European economy. In contrast, the protectionist aspirations that are emerging in some Member States as well as at European level represent a disadvantage for digital services and business models, impede and delay digitalization in Europe, and stand in the way of the realization of the digital single market.

16 The EU must take greater account of start-ups and small and medium-sized enterprises in legislative proposals and establish appropriate and equitable market and competitive conditions.

A further example in the area of competition law is the regulation of digital platforms in an effort to strengthen the digital single market, which in 2018 became a central building block of European policy. Against this background, the introduction of the so-called P2B Regulation (regulation on promoting fairness and transparency for business users of online intermediation services) can be seen as a further attempt to impose additional obligations on digital platforms.

However, it should be acknowledged that, as things stand at present, these regulations would affect not only powerful market players, but also smaller platforms and SMEs. These could be significantly hampered in their development by the additional requirements, which could in turn result in an even greater concentration of digital platforms.

eco accordingly calls on the EU Parliament and the European Council to critically review the scope of application, the specific individual requirements, and the target groups of the proposed regulation. In addition, consideration should also be given to the technical feasibility of the provisions and the reality that a regulation on the organization of business relations and not a consumer protection regulation is being created.



Digital Industry and Digitalization

17 The Council of the European Union should pull back from its plans for a digital tax and instead work towards a single taxation system that taxes all companies according to the same principles.

The Council of the European Union took on the project of a digital tax, aimed in particular at companies which do not generate their revenues or profits in the country of tax residence. However, such a digital tax would be detrimental to all companies offering digital goods or services and would discriminate against them compared to other (traditional) suppliers. Instead, existing taxation rules should be fundamentally reviewed and adapted in a sensible manner to fit the needs of a connected and globalized economy. This would entail a uniform taxation of all companies according to the same rules and principles, imposing an equal tax burden on them, and thus enacting tax justice – regardless of business models or distribution channels. Taxation models that impose special taxes on online advertising (as opposed to print) or on software purchased online (as opposed to software on media) would, conversely, place digital business models and Internet companies at an unjustifiable and immense competitive disadvantage.

18 EU Member States must abolish internal virtual borders and guarantee free movement of data within the EU.

In a connected European digital single market, it is essential to remove barriers and obstacles to market access. This also includes virtual restrictions on the localization of services and data. Within the EU, it should be possible in principle to offer services from any Member State, including services for public contracts and the use of non-personal data from public administration. Particularly since the entry into force of the General Data Protection Regulation and its accompanying legal security requirements, it is no longer justifiable that, for example, the physical storage, processing, or use of data and Internet services should be restricted to the respective Member State.

For example, the free movement of data enables Internet companies to select locations according to criteria such as security, efficiency, and availability and to offer the same services across borders.

19 The EU must develop a coherent European strategy to strengthen the development and deployment of artificial intelligence and blockchain technologies.

In April 2018, the EU Commission presented its proposal for a strategy for artificial intelligence (AI) in Europe. The main pillar of this strategy is to strengthen research. In addition, the Commission hopes to broaden the use of AI in the context of the digital single market. Both approaches are to be welcomed in principle, but require further concretization. In particular, the EU should also accord a greater focus to market-oriented application of AI solutions.

A central aspect here is the facilitation of simplified access to data for training artificial intelligence. It is also important that the ambitious goals which the EU Commission would like to promote with a budget of 1.5 billion Euro are not undermined by regulation elsewhere, as could happen, for example, with the ePrivacy Regulation.

The Commission has got the EU Blockchain Observatory and Forum off the ground. Its aim is to draw attention to important developments in blockchain technology, to support European blockchain actors, and to intensify European interaction amongst the various stakeholders engaged in blockchain activities.

Blockchain technology, which involves information packets being stored decentrally on the Internet, is considered an important breakthrough, given that it ensures a high level of traceability and transparency for online transactions. It has the potential to change digital services and business models in a variety of areas (e.g. healthcare, insurance, finance, energy, logistics, and rights management).

eco would very much like to see a unified European strategy to strengthen the use of AI and the development and deployment of blockchain technologies. In this context, it should also be recognized that strengthening digital services and products on the basis of AI or corresponding systems and the blanket regulation of algorithms – especially in the form of ex ante regulation, as is currently being considered – would be detrimental to the desired promotion of important future technologies and innovations.

eco – Association of the Internet Industry
Capital Office
Französische Straße 48
10117 Berlin
Phone: +49 (0) 30 20 21 56 7-0
Fax: +40 (0) 30 20 21 56 7-11

Email: berlin@eco.de

international.eco.de

CEO: Harald A. Summa
Managing Director: Alexander Rabe