Standards, Regulations, and Net Neutrality in the Digital Economy

Harald Øverby and Jan A. Audestad

Summary: The digital economy is one of the fastest growing segments of the economy. It includes the production, trade, and transportation of digital goods and services, as well as online ordering of physical goods—also known as e-commerce. The digital economy is made possible by key technologies such as the Internet and mobile communications. One of the success factors of the digital economy is the Internet as an open platform for conducting business and innovation. A key ingredient in the evolution of the open Internet is standardization. In its early stage, the digital economy was an open marketplace with few market regulations. However, as the digital economy is expanding in size and scope, increased regulation of digital markets is taking place in many parts of the world.

This paper examines standardization and regulation efforts in the digital economy, in particular, the impact these standards and regulations have on the evolution of digital markets. The paper first presents the technological infrastructure underpinning the Internet and its corresponding business landscape, followed by a discussion of the role regulations and, in particular, net neutrality play in innovation and the evolution of digital businesses.

I. Introduction

The digital economy encompasses the production, trade, and transportation of digital goods and services and online sales of physical goods—also termed e-commerce. From being an almost non-existent part of the global economy in the 1970s, the digital economy has grown to constitute about 4–10% of the GDP in most developed countries.[1] This number is expected to increase in the future as a result of the ongoing digitization of the industry and the public sector. One such digitization effort is *industry 4.0*—a term coined in a German governmental project in 2011—aiming at transforming the traditional manufacturing industry into its next stage of evolution by incorporating advanced Information Technologies (IT) such as sensor networks, cyber-physical systems, artificial intelligence, and Internet of Things.[2]

An essential part of the digital economy is standardization—the process of making digital goods and services conform to a standard to promote interoperability, compatibility, quality, and competition. Standardization has been central to the development of the Internet from its early designs in the 1960s and to the development of all generations of public mobile communication systems since the Nordic Mobile Telephony

[1] *Measuring the Digital Economy* by the International Monetary Fund, Feb. 2018

[2] See: https://en.wikipedia.org/wiki/Industry_4.0

(NMT) in the late 1970s. Standards are critical for global interconnectivity in communication networks which, in turn, enables growth of the global market for digital goods and services. Standards also foster competition between suppliers of digital goods and services and reduce switching costs in the markets, for example, if a user of a particular service (e.g., mobile phone service) switches to another service supplier.

Another essential part of the digital economy is regulation—the intervention of governmental, legal, social, economic, or technological authorities to restrict operations or evolutions in digital markets. The Internet was initially an open network free for anyone to access and use.[3] There were very few restrictions on the use of the Internet. However, with the increased reliance on Internet-based services to perform mission-critical operations in the society, an increased need for regulations emerged. This is because the unmanaged and sometimes haphazard evolution and operations of the Internet were not always in line with society's needs. One example is the market failure that emerges due to the appearance of natural monopolies in the digital economy. Such natural monopolies emerge due to strong network effects and products with zero marginal cost. The consequences of the appearance of such monopolies may be high switching costs and lock-in of customers, reduced investments in innovation, and over-priced products. Market regulations have been implemented to combat the negative effects of natural monopolies. Another example of negative effects is the exploitation of personal data of customers using Internet services. Some companies have, uncritically, exploited personal data for their own economic gain, thereby creating unwanted monopoly situations. Legal regulation such as the General Privacy Data Regulation (GDPR) in the EU and the EEA is one example of measures to combat these exploits.

The major contribution of this paper is a presentation of standards and regulations in the digital economy, including selected examples of how standards and regulations have had an impact on the digital economy since its inception in the 1960s. The paper is organized as follows:

- Section II presents the basic properties of digital goods and services.
- Section III introduces the technological infrastructure supporting the digital business.
- Section IV describes how the technological infrastructure shapes the business landscape.
- Section V discusses the role of standardization in the Information and Communication Technology (ICT) and why it is important.
- Section VI provides an overview of the most important standards organizations responsible for the evolution of various aspects of the digital network and its applications.

[3] The Internet originated from the ARPANET, a US Defense Research Project that also included academic partners, mainly in the US. During its early phase (until the 1980s) the ARPANET evolved into what we now call the Internet and was mainly used by academics with no or little regulation.

- Section VII discusses the market implications of standards.
- Section VIII presents the importance of interconnectivity, interoperability, and backward compatibility and how it is solved.
- Section IX discusses he complex problem of trust and security in the ICT.
- Section X describes the complex issues related to numbering, identification, and addressing in mobile networks and the Internet.
- Section XI discusses why regulations are required in ICT in order to ensure competitive fairness in the market.
- Section XII describes the general aspects of net neutrality.
- Section XIII explains what is understood by search and device neutrality.
- Section XIV discusses the business implications of net neutrality.
- Section XV explains how zero-rating service access is used by some application service providers to reach customers in certain parts of the world and why this may violate net neutrality.
- Section XVI concludes the paper.

II. Basic Properties of Digital Goods and Services

By a digital good or service we mean a product that exists only as stored software and information on computers and that can be delivered to the users over the Internet. The latter condition means that the good or service is *networked*. Examples of digital goods and services are Facebook, eBay, e-books, webpages, and emails. These products possess some unique features:

- The marginal cost is zero. This means that the cost of producing an additional item of the good or service is nil. Examples are adding a new user to Facebook, doing a Google search, accessing and downloading a webpage, making a phone call on Skype, initiating an eBay transaction, downloading an e-book or a film, and reading a Wikipedia page. This is different from physical goods such as cars and paper books, for which the marginal cost is larger than zero.
- The cost of delivering one copy of the digital good or service is zero since the use of Internet is subject to fixed and mostly traffic independent charges. Therefore, the delivery cost per item tends to zero if the number of items is large.
- The cost of storage is also nil since, for example, only one copy of an e-book need be stored on a digital storage medium requiring very little physical space.
- The average return per user (ARPU) for a digital good or service is often zero or, in other words, the service or good is gratis for the user. In these cases, the supplier must generate income from other sources such as advertisements (Facebook) or benefactors (Wikipedia). ARPU is not zero for all digital goods; for example, for receiving e-books and music (e.g. Spotify), a fee per downloaded item usually has to be paid to the originators.

- Digital goods and services are non-rival; that is, the instance that one customer is using or purchasing the good or service, does not exclude others from purchasing or using it. This may be different for physical goods because of the way physical goods are produced (limited production volume) and stored (limited storage volume). A film can be viewed simultaneously by millions of viewers over the Internet, while a film theater, in comparison, usually allows only a few hundred simultaneous viewers. This puts several digital goods and services in the category of public goods. Such goods are often prone to market failure so that regulations or other mechanisms must be employed to ensure a well-functioning market.
- The marketplace for digital goods is global: there is no constraint associated with the location of the retailer and the purchaser.

This paper considers some characteristics of digital goods and services that are upshots of how they are produced, stored, and distributed. One central issue is the impact that the structure of the Internet and interacting software modules has on digital businesses, standards, and regulations. Therefore, we continue with describing the basic structure of ICT systems.

III. The Technological Infrastructure of Digital Goods and Services

In many people's mind, the term Internet seems to mean both the digital network infrastructure transporting bits from one place to another and the services and digital goods that this bit-transport technology supports. This confusion is caused by no or little insight into the technology forming the basis for digital services and may sometimes lead to false conclusions concerning various economical, juridical, and societal aspects of the digital economy. Therefore, we first present a simple picture of the infrastructure of the information and communication technology (ICT) permitting us to construct, market, purchase, and utilize digital services and goods, or, in other words, the infrastructure which enables entities (persons or machines) to produce, disseminate, and exchange digital information creating new business opportunities and changing existing ones.

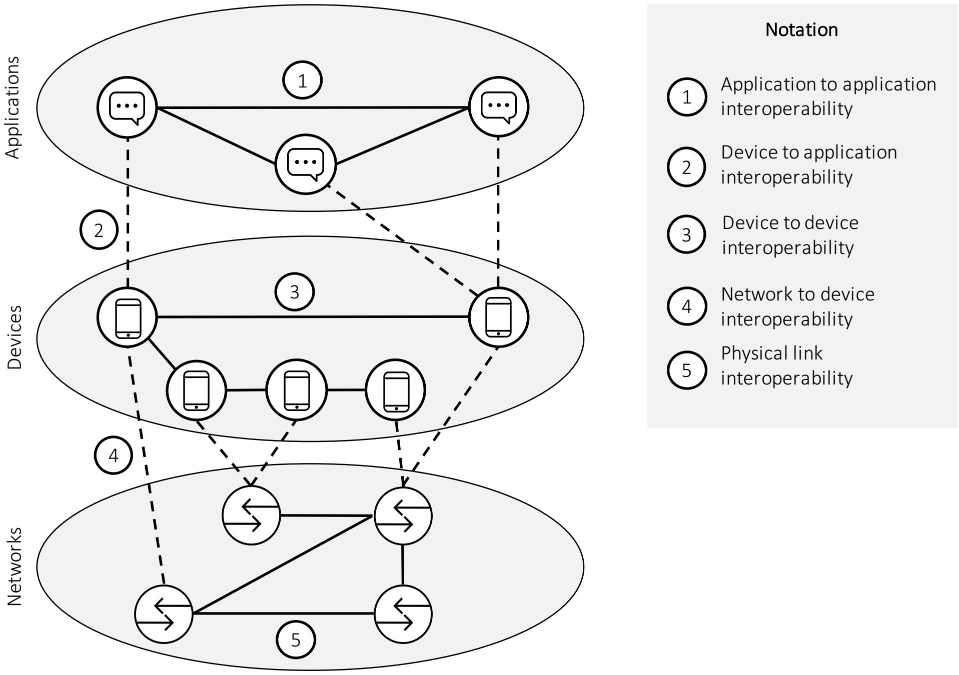
Applications
Devices
Networks
1
2
3
4
5
Notation
1 Application to application interoperability
2 Device to application interoperability
3 Device to device interoperability
4 Network to device interoperability
5 Physical link interoperability

Figure 1. The technological infrastructure of digital goods and services.

The technologies behind all digital goods and services are the Internet—or the IP network as it is also called—and all protocols, access technologies (e.g., optical fiber, mobile radio, satellite, and copper wires), and applications built on top of the physical network (e.g., the World Wide Web, email, Facebook, Google, Twitter, and eBay). It is convenient to visualize the digital good or service as elements in a three-layered arrangement as shown in Figure 1. This simple model may also be referred to as the technological infrastructure of ICT. The three layers are:

- The bottom layer (networks) is the physical network over which data are sent. The network consists of routers for transferring data from sender to receiver and support-systems for network management, maintenance and surveillance. This is the IP network and constitutes, by definition, the Internet. The Internet is thus the technical infrastructure supporting the transfer of bits between entities. At this layer the Internet Service Providers (ISPs) reside. Their business is to transfer bits and deliver them to the correct destination and to connect user equipment to the network infrastructure.

- The second layer (devices) consists of the devices connected to the physical network; that is, laptops, mainframe computers, mobile smartphones, automobiles, smartwatches, refrigerators, infrastructure components, payment terminals, television sets, and all other devices and gadgets containing processing and storage units. These devices are often referred to as *hosts* because they accommodate the processing of the software at the layer above. The devices are connected to the network over access systems such as copper wires, mobile radio, satellites, and optical fibers. Particular protocols (e.g., TCP and UDP) exist between the devices to support reliable transfer of information between them.
- The uppermost layer (applications) consists of software modules and data programs that run on the devices in the layer below. This may be simple modules such as a single webpage or a PDF document, complex processes distributed over several devices at different locations (e.g., power distribution systems, the IP network itself, financial networks, and worldwide arrays of telescopes for astronomical observations), or publicly available services and goods such as electronic newspapers, email, social services, banking, and e-commerce. This is the realm of the Application Service Providers (ASPs) such as Google, Facebook, Twitter, and eBay. Massively Multiplayer Online Games (MMOGs) are also software applications offered by ASPs.

The layered structure of Figure 1 is essential for the comprehension of the different aspects of digital businesses: the need for standardization of basic functions, various aspects of competition and cooperation, relationships between ASPs and ISPs, formation of de facto (or natural) monopolies, and why market regulation is required in certain cases.

The complex structure of the ICT requires definition of what is going on between entities in the same layer and between entities in adjacent layers. This corresponds to specification of five interfaces as shown in Figure 1. These interfaces are:

- The physical links supporting interoperability between IP networks owned by different operators (ISPs). This includes specification of technical interfaces as well as operational and economic agreements. The latter incorporates transit and terminating traffic agreements, traffic management, and payment for the use of the network of other ISPs for transiting information.
- Interface between the network layer and devices. The access technology is usually based on international or regional standards for access such as the 4G or 5G standards for mobile access or optical fiber for fixed access (fiber-to-the-home (FTTH)). The most important requirement is addressing. The devices must have an address which is globally unique. These are the IP numbers. We will come back to some important issues concerning addressing in the Internet in Section X.

- Devices must also be capable of exchanging and sharing information between them using end-to-end (or device-to-device) protocols such as TCP and UDP supporting the information transfer between application modules on the application layer. One particularly important protocol is the Transport Layer Security (TLS) encrypting the information contained in TCP/UDP packets. This protocol protects against eavesdropping and tampering of information, for example, emails, interactions with webpages, banking and payment services, and voice and messaging services.
- The interface between the devices and the applications is identified by an address element called *port number*. The port number tells the computer which type of software module must be invoked in order to interpret and process data.
- Finally, rules must be defined for interaction between software modules at different locations. This includes definition of application protocols (e.g., https, FTP, and SMTP) and address formats for accurately identifying the remote software entity. This is the Universal Resource Identifier (URI) (see Section X).

Next, we shall look at some consequences this structure may have on the business landscape of the digital economy. In this discussion, we will only consider businesses directly associated with the Internet.

IV. The ICT Business Landscape

The most significant consequence of the ICT architecture described in Section III is that the digital economy is split into two independent business domains:

- Provision of network services such as baseline Internet operation, fiber optic access systems, public mobile communications networks, and satellite access networks. This is the business domain of the Internet service providers (ISPs) and the Infrastructure Providers (IPs). They earn money from connecting users to the network and transferring bits between them. The IPs are building and operating the communication networks and the ISPs are offering connectivity services to users. Often, a single company is both an IP and an ISP, e.g., Telenor in Norway. However, there exists a special group of companies that are only ISPs, namely the Virtual Network Operators (VNOs) only providing connectivity services to end users without operating a physical infrastructure. Hence, the VNOs must lease infrastructure from an IP.
- The Application Service Providers (ASPs) offer software-based goods and services on a communication network—typically the Internet. These goods and services are essentially independent of the network so long as the network maintains enough capacity, offers sufficient bandwidth and other quality

> measures such as latency, availability, and mobility. The ASPs may earn money directly from the users or indirectly from advertisements, from third parties benefitting from or contributing to the service, from public sources, or from grants. The ASP may produce the content it disseminates or collect and offer content produced by specialized Content Providers (CPs).

In addition, there are manufacturers and retailers of devices and gadgets. They do not play a direct role in the production and consumption of digital goods and services. However, the equipment they produce must be compatible with the standardized network interfaces and applications.

The two types of businesses are depending on each other: The ASP needs the cooperation of the ISPs to deliver the good; the ISP needs the goods produced by the ASPs in order that anyone will subscribe to the network access. However, this does not prohibit companies to act as both ISPs and ASPs at the same time. This is the case for the large network operators and cable television companies owning Internet cables and routers (ISP business) and offering television, video on demand, and other digital services over the network (ASP business). However, their roles as ASP and ISP are in many cases separated to avoid cross subsidizing and unfair competition.

The split between the ASP and ISP business is caused by the structure of the technological infrastructure explained in Section III. The reason is that the device layer in Figure 1 makes the business of the ASP invisible to the ISP. The ISP cannot, in general, distinguish between different services and goods the ASP disseminates over the network of the ISP; for example, the ISP cannot see if the service is voice over IP (VoIP), burglary alarm signals, streamed film, or web access. This means that the ISP cannot levy charges from the ASP or the user receiving the good depending on the actual information sent. The principle of flat charges must be applied; that is, the same charge is levied for all services. The only parameters the ISP may use for levying differentiated charges are total traffic volume (in, say, gigabytes downloaded per month), minimum data rate offered at the interface (megabits per second), and certain quality of service (QoS) parameters such as latency (maximum time the network processing delays a packet), and real-time performance (in particular for telephony, multiplayer games, and real time video). If other parameters are to be used to discriminate between services, Deep Packet Inspection (DPI) must be employed to every packet passing a particular router. See also Section XIV.

The most important reason why the ISP cannot distinguish between the different services is that most services are using the Hypertext Transfer Protocol Secure (HTTPS). The protocol is encrypted and there is no simple way that the ISP can identify the type of service currently running atop of the protocol. It is even difficult to do that if the unencrypted version of the protocol, HTTP, is used. Another reason has to do with the way in which digital information is sent. In some case, all information is contained in a single IP packet (for example a webpage). In other cases, the information is spread oved several IP packets (for example, a telephone call on Skype or a streamed movie). Even if the ISP knows the type of service, it is impossible to determine how many packets are sent for the execution of that service from information contained in the header field of the IP packet alone. Finally, IP packets for different services may be statistically multiplexed such that in the stream of IP packets some packets belong to service 1 while other packets belong to service 2. There is no simple way for the ISP to charge the services imbedded in this intermixed packet stream individually.

One exception is mobile network operators. In the mobile standards 2G (GSM) and 3G, the mobile operator can distinguish easily between telephone calls, SMS, and transfer of data, though the mobile operator cannot distinguish between the different data services for reasons just explained. The mobile operator may then levy charges depending on these basic services. The operator may even charge different types of telephone calls differently, for example, international calls, calls from roaming users, calls to value added services (premium rate calls), free-phone calls, and calls to particular numbers. This picture is slightly changed with the all-IP technologies of 4G and 5G, though there are still some opportunities to levy service-dependent charges in some cases. One reason is that voice calls are transferred over the mobile network using a particular voice-over-IP standard called VoLTE, requiring special handling at the interface between the mobile network and the fixed Internet.

The businesses of ISPs and ASPs are separated because of the technology behind the Internet and not for commercial or regulatory reasons. There is, therefore, no particular advantage for ISPs to also become ASPs and, vice versa, for ASPs to also become ISPs. There are no or few benefits from merging an ISP and an ASP since their business operations are vastly different. This includes business strategy, value production, and customer groups.

V. Role of Standards in the Information and Communication Technology

Standards are necessary to ensure interoperability between users and providers, consistency of service offers, protection against abuse, and maintainability of quality. In the Information and Communication Technology, standards are critical since there are several different types of technical equipment produced by different manufacturers from different parts of the world (e.g., smartphones and laptops). Lack of standards will result in situations where international deployment of services is not possible.

The need for standards in ICT is also evident from Figure 1 showing that five interfaces need to be standardized to provide interoperability. That these standards are strictly followed is particularly important for the development and management of digital goods and services designed for the global marketplace. Standards are needed for several reasons:

- Standards are the tool by which worldwide ICT markets can be created, where the foremost prerequisite is that the devices at each end of the connection are capable of communicating irrespective of where they are located and to which ISP they are connected.

- Standards are required for creating a competitive market, for example, for end user equipment. This includes procedures for how to connect devices to the network, how different types of equipment (e.g., laptops and smartphones) can interoperate, and how to locate and identify remote equipment.
- Standards enable cooperation between stakeholders responsible for performing different tasks in the execution of certain services, for example, banking services where financial institutions may cooperate with third party service providers for trusted customer identification (e.g., offering Liberty Alliance services[4]), authentication (e.g., mobile operators), card verification (card issuers), and transaction managers (e.g., point of sale operators). This requires not only technical standards but also legal, economical, and managerial ones.
- Standards for distributed processing are required to allow computers to cooperate in performing a common task, where the various elements of the service are executed at different computers at remote locations. This category includes concepts such as cloud computing and grid computing. Examples are the Internet itself, massively multiplayer online games, aircraft control systems, and large scientific simulation models requiring more computer power than is available in even the largest supercomputers.

International ICT standards ensure interoperability between users globally. These are standards related to telecommunications networks (e.g., the Internet protocol stack and the family of mobile network standards developed by 3GPP), presentation formats (e.g., HTML), and Internet naming and addressing formats and usage (e.g., URL and URI). These standards are not subject to legal agreements between countries; that is, they are not *de jure* standards. On the contrary, the ICT standards are *de facto* standards developed by manufacturers, universities, voluntary groups, or individuals to support the international ICT infrastructure. If the proposal is valuable, it may be taken into use and thereby becoming an international standard. The World Wide Web is the most evident example, starting as a project to facilitate communications between the particle physics laboratory CERN outside Geneva and cooperating universities worldwide. Within a few years the WWW became the *de facto* standard for the biggest usage of the internet, namely information posting and browsing.

The layout and content of the digital good or service itself is not usually subject to standards: there is no standard concerning the content and presentation of, for example, Facebook, Twitter, Netflix, and Apple and Android apps. To reach the market, they must only support the standards required for accessing the network and for transferring the information to the users.

[4] Official website: http://www.projectliberty.org/

VI. Standards Organizations

There are several organizations and groups specifying and standardizing ICT infrastructures, protocols, and operations; that is, the evolution of services and applications based on the Internet. In this section, we will just look at the few of them having the biggest impact on the evolution of the technology and services supported by ICT. Some of these groups are based on international charters (ITU, ETSI, 3GPP), while other are nonprofit interest groups dedicated to a particular field of standardization (the Internet Society, the World Wide Web Consortium). Most of these standards are open source standards, meaning that anyone nay load down the standards free of charge. Exceptions are ITU and ETSI where the newest standards are subject to certain fees.

ITU[5]

The world's oldest standardization organization is the International Telecommunications Union (ITU). ITU was established in 1865 for the standardization of the emerging telegraph service. ITU was included as a specialized organization in the United Nations in 1947. The union is responsible for the standardization of telecommunications networks, equipment, technical interfaces, network management, services, and operations. This includes, in particular, the standards for the telephone network and mobile networks and, to a lesser degree, the standardization of the Internet and ICT. In fact, at the meeting of The World Conference on International Telecommunications 2012 (WCIT-12) the European Parliament presented a resolution where it "Believes that the ITU, or any other single, centralized international institution (e.g. ICANN), is not the appropriate body to assert regulatory authority over the internet."[6] The major concern was that ITU regulations, in particular on tariffing, may undermine the principle of network neutrality. Several other countries supported this view, amongst others, the USA, India, Australia, and Japan. Nevertheless, a new resolution was accepted by 86 of 152 countries stating rather vaguely ~~t~~ "to invite Member States to elaborate on their respective positions on international Internet-related technical, development and public-policy issues within the mandate of ITU at various ITU forums including, inter alia, the World Telecommunication/ICT Policy Forum, the Broadband Commission for Digital Development and ITU study groups."[7]

[5] Official website https://www.itu.int/en/Pages/default.aspx

[6] European Parliament resolution on the forthcoming World Conference on International Telecommunications (WCIT-12) of the International Telecommunication Union, and the possible expansion of the scope of international telecommunication regulations (2012/2881(RSP)) http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=B7-2012-0499&format=XML&language=EN

[7] International Telecommunications Union, Final Acts: World Conference on International Telecommunications, Dubai, 2012

ITU is not the dominating organization behind the Internet today, and will most probably not be so in the future because of the opposition expressed by the EU, USA, Japan and several other technologically advanced countries. For the evolution of the Internet and digital services, the ITU may become an organization that is not generating the standards but rather ratifying standards produced by more specialized organizations.

ETSI[8]

The European Telecommunications Standards Institute (ETSI) was established in 1988 as an offspring of the *Conférence européenne des administrations des postes et des télécommunications* (CEPT). ETSI is an independent standardization organization for the EU and associated European states (e.g., Switzerland, Norway, and Turkey). Industries and organizations of these countries are the full members of ETSI. In addition, there are several organizations and industries from other counties outside Europe that are associated members, for example, USA, Japan, People's Republic of China, India, Brazil, Australia, and Canada. Currently, ETSI has over 800 full and associated members.

ETSI is now regarded as the World's most influential, progressive, and successful standardization organization on all aspects of information and communications technologies, including new fields such as machine-to-machine (M2M) technologies and the Internet of Things (IoT). ETSI has taken over many of the roles ITU had previously, publishing more than 2000 standards per year.

From GSM to 3GPP

Standardization of public mobile communications plays a particular role in the evolution of digital services. The successful standardization of GSM was also one of the major arguments for establishing ETSI. Therefore, we will describe some of the events leading to the current standards for mobile communications.

The evolution of digital mobile communications started in 1982 when 17 European countries decided to jointly specify a pan-European digital mobile network. The group set up for doing the task was named *Groupe Spécial Mobile*, GSM, later the system the group specified was renamed the Global System for Mobile communications, also abbreviated GSM. In 1982, several incompatible systems for land mobile systems existed or were about to be put into operation in Europe: NMT in the Nordic countries, the Netherlands, Switzerland, and Spain, TACS in UK, C-Netz in Germany, and Radiocom 2000 in France.

In order to make sure that GSM was built and not put aside as an interesting future option, 13 European countries signed a Memorandum of Understanding (MoU) in 1987 obliging that "operational networks shall be procured in each of the countries by the network operators based on the CEPT recommendations with the objective of

[8] Official website https://www.etsi.org/

providing public commercial service during I991."[9] Therefore, GSM operation could commence in Europe in 1991/1992. GSM was not only built out in Europe; within a few years, GSM had become the preferred mobile network standard in most of the world.

GSM is a European standard that became a worldwide *de facto* standard. What is more important is that the GSM standardization process became the norm by which all later mobile standards—3G, 4G, 5G, and variants thereof—are made. This includes features such as service definition, network architecture, roaming, handover, subscription modules, addressing, and so on. The standardization process is also an example of an open and dedicated cooperation between companies that later would become competitors as network operators, suppliers of network equipment, and manufacturers of user terminals. This is a particular form of *coopetition*. Coopetition implies that the companies may both cooperate and compete either at the same time or at different stages of the evolution. The reasons for coopetition in developing a technological standard are several:

- Instead that one company or organization carries the total development cost, the costs are shared between several partners; the total cost of developing the rather cheap GSM standard was more than 100 million euros and required more than 1000 man-years of expert work. The development of the 4G standard has required several times as many resources.
- A global standard makes the total market much bigger and, as a consequence, the market for each participant is also bigger.
- The economic risk of participation in projects based on standards with global market potential is much smaller than for implementing a local standard.

The work on a global mobile network standard was initiated in ITU in 1986 under the name Future Public Land Mobile Network System (FPLMNS). The work progressed very slowly, and no significant results were obtained until 1998 when the project was taken over by the newly formed organization 3rd Generation Partnership Project, 3GPP.[10] 3GPP is a collaboration between the major standardization organizations in the USA, Europe, and Asia. The technical support team is located at the headquarters of the European Telecommunications Standards Institute (ETSI) in Sophia Antipolis, France. The standardization work is based on voluntary contributions from more than 370 member organizations.

3GPP is responsible for developing the standards for 3G, 4G, 5G, and beyond. 3GPP has also taken the leadership in developing Internet standards for applications in mobile systems such as new Voice-over-IP standards, the IP Multimedia Subsystem (IMS) for application in all-IP mobile systems, and access technologies and architectures for the Internet of Things.

[9] See: http://www.gsmhistory.com/wp-content/uploads/2013/01/5.-GSM-MoU.pdf

[10] 3GPP official website: http://www.3gpp.org/

All standards made by 3GPP can be accessed and loaded down free of charge by anyone and are, in this respect, open source standards.[11]

Internet Society[12]

The Internet Society is an American nonprofit organization in charge of promoting the standardization and policies of the Internet. The organization also has several offices outside the USA (for example, in Geneva and Brussels to be close to both the UN policy group on information technology issues and the political and technological power center of Europe). The organization has no legal influence on the ICT evolution. On the other hand, the informal influence is enormous.

The internet Society is the home for several legally informal standardization bodies, the most important of which are:

- The Internet Engineering Task Force (IETF) is in charge of developing and promoting Internet standards. There is no formal membership of the organization and anyone may contribute to the work by issuing Requests for Comments (RFCs) which may contain amendments or additions to existing standards or proposals for completely new standards. The proposal may be accepted by the Internet Engineering Steering Group and becoming a new Internet standard. Even so, it may be rejected or ignored by manufacturers and Internet providers and never implemented. Being so loosely organized, the Internet may evolve in an unplanned and haphazardly way. This has so far been the major forte of Internet.
- The Internet Architecture Board (IAB) is an informal advisory group in charge of inducing some degree of consistency on the evolution of the Internet, amongst others by sorting out RFCs that may become useful additions to the Internet technology. This induces some direction to the evolution of the Internet.
- The Internet Engineering Steering Group (IESG) is the forum that finally endorses new Internet standards.

Note that ITU plays no important role in the standardization of the internet. On the other hand, 3GPP is playing a more and more important role, in particular, in the development of the Internet of Things.

World Wide Web Consortium[13]

The World Wide Web Consortium (W3C) is an independent organization in charge of standardizing web services. The organization was established and is currently managed by the inventor of the World Wide Web, Tim Berens-Lee. The charter is to standardize

[11] See: http://www.3gpp.org/specifications/releases

[12] Official website: https://www.internetsociety.org/

[13] Official website: https://www.w3.org/

and develop the WWW technology and promote WWW-derived services. This includes presentation languages (XML, HTML), formats (XForms), procedures (SOAP), and protocols (HTTP, HTTPS). The W3C standards are independent of the Internet standards. The only requirement is that the Internet exists as an underlying network for communications.

Institute of Electrical and Electronics Engineers

Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA)[14] develops standards within a broad range of technologies where telecommunications is just one of them. The most important standards are assembled in the 802-series. This series includes standards for the Ethernet, WiFi, Bluetooth, Zigbee, body area networks, and other local area technologies. These technologies define how various types of equipment can be connected to the Internet or interconnected locally to form local area networks for different purposes. While all the organizations listed above are authorized standardization bodies either directly or through association with other organizations, the IEEE is not. The IEEE is rather a loosely knitted community of scientists and engineers participating in developing the standards. Despite of this, IEEE-SA is one of the most influential standardization bodies in the world, having specified most of the local communications technologies surrounding us.

VII. Market Implications of Standards

Standards have significant implications on competition and on how digital services evolve in the markets. Standards are drivers for commoditization—even complex services like mobile communication and Internet access are commoditized. The user will, for example, not experience any difference using smartphones from different manufacturers or receiving the service from different mobile network operators. Commodified services compete primarily on price and not on other features. This means that it is easy for users to switch to competing service providers since all other features except price are more or less the same. In such a market it is difficult for the provider to lock in consumers because the switching costs both for the consumers and the supplier are small.

It is more likely that *de facto monopolies* develop in markets without standards or with more than one competing standard because a consumer must choose between equivalent services from different suppliers that are technically incompatible. In this case, it is expensive for the customer to switch to another supplier. Moreover, network effects may dominate in the competition so that one of the providers ends up as a monopoly. One example is the competition between the video recording standards

[14] Official website: https://standards.ieee.org/

VHS and Betamax in the 1970s and 1980s. VHS and Betamax offered similar capabilities but were not compatible since there was no common standard for video recording. VHS cassettes could not be played on a Betamax recorder and vice versa. In fact, VHS and Betamax were competing industrial standards developed by different companies. Because of network effects, both standards could not coexist in the market—over time one of the standards would outcompete the other. By the mid-1980s, it became clear that—for various reasons we will not discuss here—VHS had won this "videotape format war." All the engineering and marketing efforts put into Betamax was in vain and had no benefit for the company developing it and for society.

The narrative of VHS vs Betamax shows us that competition among standards can be very expensive. The lesson from this case is that it is better first to *cooperate* and thereafter to *compete* once the standard has been agreed upon. This has been the case for almost all ICT standards developed during the last 30 years. Suppliers of equipment or services first cooperate to develop an international standard. Once the standard is agreed upon, it is freely available for any supplier of equipment or services. The suppliers may then develop products and services based on this standard and compete for market shares. The benefit for the manufactures and the service suppliers is that the cost to develop the standard is small for each participant and that the total market becomes larger. As mentioned in Section VI, this was the successful approach taken by GSM and later by 3GPP in developing the mobile standards.

VIII. Interconnectivity, Interoperability, and Backward Compatibility

Interoperability is the key feature of the Internet. The attractiveness for the users is that each user can communicate with any other user or webpage, for example, on email or via web browsers, independently of the technology employed by the other user. Interoperability must therefore exist between networks designed with different network technologies and between user equipment of different brands and standards. Otherwise, the Internet will split up into incompatible islands and loosing much of its value.

In the physical network, technical standards and economical and legal agreements are required to interconnect networks owned by different ISPs. Nontechnical agreements may include remuneration for transiting and terminating traffic, fair terms of competition, and minimum quality of service requirements (e.g., availability, minimum guaranteed data rate, and maximum latency and data jitter).

There are two incompatible network protocols in the Internet: the Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6). IPv4 was specified in 1983 and is still used in several networks. IPv6 was ready for implementation in 2006 but the adoption rate has been very slow until recently. IPv6 was developed to provide more addressing space than in IPv4. The adoption of IPv6 rate has now increased rapidly because IPv6 is the only network protocol used in 4G and 5G mobile networks.

The Internet, therefore, consists of islands based on IPv4 and IPv6, and a technology called tunneling is used to transfer IPv6 packets across IPv4 networks and vice versa. Tunneling means that the IPv6 (IPv4) packets are imbedded in the data field of IPv4 (IPv6) packets. On the other hand, most terminal equipment contains software for both IPv4 and IPv6 so that the equipment can be connected to either type of network. This ensures interconnectivity in the Internet.

Interoperability between mobile phones (smartphones) and mobile networks are supported by backward compatibility, implying that, for example, a 4G telephone can access 2G (GSM) and 3G networks. This is achieved by implementing the radio and signaling interfaces of all three standards in the telephone. This is possible since the evolution of computers have followed Moore's law: the processing and storage capabilities of mobile phones have doubled approximately every one-and-a-half year. This means, for example, that the computational power of mobile phones in 2001 when 3G was introduces, was approximately 60 times bigger than that of GSM phones of the same physical size. Similarly, the computational power had increased by another factor of 60 when 4G was introduced in 2010, and it is expected to increase by still another factor of 60 when 5G is introduced this year (2019).

The backward compatibility of mobile phones is achieved by implementing the three standards in all phone and install algorithms by which the phone can search for and identify the type of network serving a particular area. The selection of network may then be automatic or manual based on information displayed to the user. In order to assure backward compatibility, the network operators operating a 4G network must also operate, at least, a parallel 2G network. Several operators plan to discontinue offering 3G networks since 4G offers much better and faster Internet connections and because they still offer GSM network access. However, there are operators that also have shut down their GSM networks (for example, in USA and Australia).

IX. Trust and Security

Digital services require often cooperation between several stakeholders. One example is banking. Such configurations require that trust exists between the stakeholders and that trustworthiness can be verified to a high degree of confidence. The trust relationships may sometimes exist over several administrative domains (companies or countries) with different legislations, rules of business conduct, and regulations.

Trust may imply several things, for example: [15]

- Secure identification and authentication of communication partners mean that the partners mutually verify the correctness of their identities. Methods include permanent or onetime passwords and cryptographic authentication methods. Secure identification may include more complex procedures involving independent trusted third parties.

[15] See the ISO/IEC 27000 series for a detailed overview of recommendations on information security and related procedures.

- Non-repudiation implies that the originators and receivers of information cannot deny their participation in the exchange of information. This means that the supplier of the good cannot deny having sent the electronic good, for example, deny responsibility if the good contains malware that interfere with or damages the computer of the receiver. Similarly, the supplier cannot deny having received payment for the good. On the other hand, the receiver of the goods cannot deny having received the good. Non-repudiation may be achieved by attaching digital signatures to the messages sent; for example, attach the supplier's digital signature to the good itself and to encryption keys required for decoding encrypted goods, and to attach the receiver's digital signature to messages acknowledging the receipt of the good and associated encryption key.
- Certification implies that a trusted third party affirms the ownership of certain cryptographic secrets such as keys used for digital signatures, authentication, and encryption.

Trust is a legally complex issue. In very many contexts, trust must be based on legally binding covenants and be subject to criminal proceedings if fraud is detected. Therefore, there are few, if any, trusted third parties (TTPs) offering services outside small spheres of influence, for example, specialized enterprises protecting interactions between financial institutions, and mobile network operators offering two-step authentication for clients such as banks and governments (cryptographic authentication of mobile user followed by onetime passwords for authenticating the access attempt). In the early years of the public Internet, it was expected that it would be a lucrative business to be a trusted third party. The business potential was regarded to be huge but all legal problems and pitfalls associated with this business turned out to be many, and the few attempts to establish such companies failed: no one would trust the trusted party! TTPs owned by governments are not trusted because the users of the TTP services may suspect that the government will use the information collected by the TTP for clandestine purposes; privately owned TTPs are not trusted either because the owners of the TTP may misuse the TTP for commercial reasons, for example, selling information gathered by the TTP or interfering with the business of the user; and, finally, the TTP may represent a serious security threat because hackers may gain access to the TTP tampering with or compromising the businesses of the users of the TTP. [16]

[16] The Dutch company DigiNotar issued certificates for public/private keys for the Dutch government's public key infrastructure program. In 2011, hackers broke into the system and issued fake certificates used for criminal purposes, for example, attacking Iranian dissidents (https://en.wikipedia.org/wiki/DigiNotar). The company went bankrupt in 2011 as a result of the break-in.

The Kantara Initiative is a nonprofit consortium developing methods and best practices for secure identification procedures and information security.[17] The Kantara Initiative is a trust-framework provider and does not offer TTP services itself. The consortium supports other organizations and companies in establishing legal and operational trust among them to support security and identification activities. The owners and partners of the consortium are companies and organizations from the computer industry operating in the field of identification and security (e.g., Experian, Radiant Logic, Verizon, Symantec, and ID.me) and standardization organizations such as ISO, ITU, and the Internet Society. The Kantara Initiative is then used to induce and support trust in cases where companies and organizations must cooperate in order to accomplish a common task.

X. Numbering, Identification, and Addressing

Two particular cases relevant for ICT are considered:

- Numbering and identification in mobile networks;
- IP numbering and user-readable addressing in the Internet.

Public land mobile networks

ITU is responsible for defining the principles and formats of telephone numbers and identities in mobile systems. This includes land mobile networks, maritime mobile systems, and aeronautical systems. The principles are much the same in all three cases. IP numbers and other addresses used in the Internet are managed by ICANN (see next subsection).

In land mobile networks, a telephone number is assigned to each subscription. This number is used for the same purpose as in the fixed telephone network, namely to call the mobile subscriber or send an SMS. What is different from the telephone network is that each subscriber is also identified by an independent and globally unique identity called the International Mobile Subscriber Identity (IMSI). The IMSI is also associated both with the telephone number and the Internet address (the IP number) of the mobile terminal. This association is set up at the time of subscription. The format and the country codes associated with the IMSI are allocated and managed by the ITU.

The user is identified by three numbers in land mobile networks: one for placing telephone calls to the mobile subscriber, one for Internet operation, and one for internal identification and location management in the mobile network (the IMSI). The IMSI is used as an identifier for discovering where the roaming mobile subscriber is located in the network and for identifying the subscriber on the radio interface. The IMSI is stored in the SIM of the mobile terminal and a new IMSI is allocated to the

[17] Official website: https://kantarainitiative.org/about/

user when the SIM is replaced by a new one, for example, after damage, if the mobile has been stolen, after technology update, if the user swaps to a different subscription type, or if the user switches to a new operator. If the IMSI is changed, the telephone number or the IP number of the mobile user need not be changed. This arrangement both supports a flexible evolution of the technology (the telephone and IP number is independent of network technology) and is convenient for the user since telephone numbers need not be updated if the IMSI is changed and vice versa.

Internet

Equipment in the Internet is identified by IP numbers. The structure of these numbers is not, like telephone numbers, suitable for direct use by humans. In IPv4, the address consists or 32 bits usually presented as four 3-digit decimal numbers separated by a dot, e.g., 129.241.39.11; in IPv6 the address length is 128 bits represented as eight 4-digit hexadecimal numbers separated by a colon. These numbers are hard for humans to remember and write into the address fields. Therefore, the Internet also contains a set of human-readable addresses, the two most common ones are email addresses and web addresses. The general forms of these addresses are:

- Email address: audestadj@gmail.com, where audestadj is the local address and gmail.com identifies the mail server to which the mail is to be sent for delivery to the user. The last entry .com is the root name.
- Web address: https://en.wikipedia.org/wiki/URL, where https:// is the protocol, en.wikipedia.org is the host, and /wiki/URL identifies the file in which the information is stored. The part identifying the file may consist of long chains of texts and numbers depending on the file structure at the host where the file is stored. The web address is formally called the Uniform Resource Locator (URL). The web address is translated into the IP address by a Domain Name System (DNS) server. The root name is .org in this case. The significance of the root name is in both cases to identify how and where to find the server that can do the final address translation.

The part of the address identifying the host must be converted to IP addresses so that the network can route the IP packages to the correct destination. The organization responsible for coordinating human-readable addresses and converting them to IP addresses is the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN was established in 1998 by the United States Department of Commerce (USDC). After a long controversy, where the major concern was that the Internet was unilaterally controlled by the U S Government, the contract between USDC and ICANN ended in 2016, and ICANN became a global company independent of the US Government. Before 1998, the numbering coordination in Internet was coordinated by the Internet Assigned Number Authority (IANA), an informal organization located at the University of Southern California, establish in 1972 to coordinate numbering in ARPANET. In 1998, IANA became an operational part of ICANN.

The multi-stakeholder governance model has now been adopted for ICANN. This model implies that individuals, companies, and organizations that are directly influenced by decisions made by an organization either owns the organization, are members of the board, or both. The board of ICANN now consists of people from different organizations and companies all over the world. The main responsibilities of ICANN are the Domain Name System, including allocation of top-level domain names (e.g., .com, .net, .org, .no, .uk, etc.) and operation of root name servers.

Hampering with the root names may have severe impacts on the routing of data packets in the Internet so that the name translation system must be well protected against cyberattacks. Initially, the only root name server for the whole Internet was located at the University of Southern California. Since 2005, the root names are stored in a system of 13 databases located at different sites all around the world in order to reduce the vulnerability of the root name system. The vulnerability is reduced even more by a large number of subordinate name servers also containing root-name information.

XI. Regulations of Information Technology

Regulation (in the digital domain) is the intervention of governmental, legal, social, economic, or technological authorities, by rules or procedures, to restrict the freedom of operations for market participants or to target the evolution of the digital markets. There are several reasons for regulation:

- to avoid inefficiencies in markets such as formation of monopolies;
- to ensure fair competition;
- to assure that the users have correct and adequate information about the market;
- to satisfy collective needs of the public;
- to protect individuals against unethical business conduct and abuse of personal data; and
- to ensure professional and ethical conduct of market participants.

The increased popularity of the Internet in the 1990s triggered the rise of the cyberlibertarian movement. The cyberlibertarian's main opinion is that the Internet should not be regulated by international, regional, or national laws. They claim that the Internet—or cyberspace—does not follow national borders. Data packets are often routed over several countries and legal jurisdictions from the sender to the receiver. Data from a single transaction could even take different paths in the network crossing different national borders. The legislation of a single nation can, therefore, not be applied to the Internet. The Internet user, including ASPs and content providers, could then exploit regulation arbitrage, meaning that the laws of the country with the most liberal laws and regulations would be used, for example, by placing the servers supporting the service in low-tax countries.

The cyberlibertarians argue that the Internet should be allowed to govern itself, democratically, and without any central control.

As a response to the cyberlibertarian movement the cyber-paternalists came on to the scene. They claimed—contrary to the cyberlibertarians—that the Internet should indeed be regulated to function properly. Even though cyberspace invisibly crosses national borders, cyberspace is built up of equipment—routers, switches, terminals, mobile stations, fiber optic cables—owned and used by people or companies under the jurisdiction of the legal framework of a country. The question raised by the cyber-paternalists is not whether cyberspace should be regulated or not, but rather whether such regulations could be done by applying existing laws or by developing new laws and rules particularly for the cyberspace.

Today, most academics and decisions makers agree that the Internet both can and should be regulated. Indeed, legal frameworks of many countries have been or are about to be updated because of the widespread use of the Internet and other related information technologies. One major reason for regulating the Internet is to prevent market dominance. Because of strong network effects and that the marginal cost associated with many digital goods is zero, several markets in the digital economy will be dominated by *de facto* monopolies if regulations are absent.

One example of a *de facto* monopoly is Facebook. The market of Facebook is not regulated and, therefore, prone to market failures. Dominating network effects have turned Facebook into a *de facto* monopoly.

An example where regulations stimulate competition is the regulation of the incumbent telecom operators. The incumbent telecom operators are the former telecom monopolies that continued their business into the liberalized telecom market. In most countries, these markets are regulated, forcing the incumbents to compete with new entrants on fair terms. The new entrants may be operators owning their own network infrastructure or Virtual Network Operators (VNOs) having the legal right to lease capacity from the incumbent at reasonable and competitive costs.

Other areas of regulation in the Internet are to protect consumer privacy (e.g., the General Data Privacy Regulation of EU), to ensure that private telecom operators pay for their use of public goods (e.g., frequencies), and to stop piracy and illegal distribution of content on the Internet. In general, an increasing number of regulations of the Internet have been put in force during the past decade.

Regulating the Internet may not only be done by laws and legal frameworks. The *pathetic dot theory* developed by Lawrence Lessig defines four modalities of regulation, as illustrated in Figure 2:

- Legal: How the legal framework in a jurisdiction is used to regulate.
- Market: How trade, markets, and economic factors are used to regulate.

- Technology: How the technology is used to regulate.
- Society: How norms and societal factors are used to regulate.

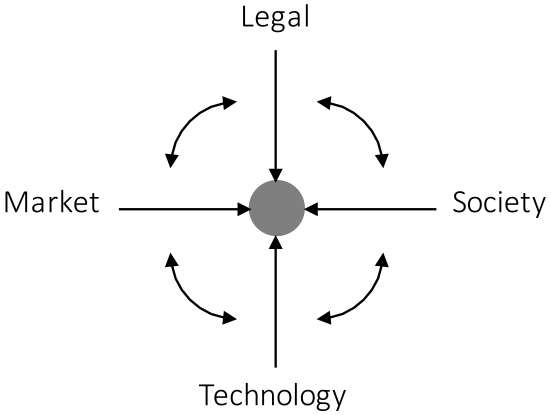

Figure 2. Lessig's four modalities of regulation.

Regulating the digital economy—or a specific sector, domain, or market in the digital economy—can be achieved by using a combination of the four modalities. An example is the regulation of music piracy, in which the main problem is the violation of copyright and illegal downloading and spreading of music on the Internet. Such actions were made possible by the ubiquitous use of the Internet combined with applications or websites such as Napster and MP3.com. This was a major issue in the 2000s and still is, however, with less intensity today since a combination of the modalities described above has been employed to regulate the issue.

In many countries, downloading copyrighted material is illegal by law. People downloading and sharing such material may be prosecuted and punished according to the laws in their jurisdiction. This is an example of *legal measures* in Lessig's model to regulate software piracy. In the 2000s, new services offering access to copyrighted media were launched—Spotify, iTunes, and Tidal. These services created a market for legal access to music and contributed to regulating this market. This is an example of regulation by *market*. The 2000s also saw the emergence of technological copyright protection of music and other media by which copying a specific CD or DVD was not possible. This is the use of *technological measures* to regulate piracy. The last of Lessig's modalities—*society*—is about societal actions to regulate piracy. In spite of the laws passed to regulate piracy, people still in huge numbers continued to download and spread copyrighted material. This was because the general opinion of the public was not to view free music downloading as a crime that should be punished. Campaigns comparing stealing music and stealing cars as the same thing did not have any lasting effect on the public. In many people's opinion, digital goods are different from physical goods since digital goods are non-rival, while physical goods are rival by nature: stealing a non-rival good is not the same as stealing a physical thing from someone.

The main point is that regulating the digital economy can be achieved not only by laws but also by markets, business models, economic incentives, technology, design, and societal campaigns. These forces—or modalities as Lessig termed them—work together and influence one another. How well a specific service or part of the digital economy is regulated is the sum of all these effects and their interactions.

XII. Net Neutrality

Net neutrality is the principle that all data on the Internet shall be treated equally by the Internet Service Providers (ISPs). Hence, with net neutrality in force, there shall be no discrimination of the transmission of data based on the identity of the sending or the receiving users, the content of the data, or the associated application. This means that data packets transmitted on the Internet should be given the best-effort service and served on a first-come-first-served basis. This also means that the ISPs cannot perform any kind of blocking of applications, throttling (reducing the transmission speeds of specific applications), or any differentiated treatment of data packets based on the sender or the receiver of the data packets. With full net neutrality in force, even advanced network management to ensure quality of service in the networks may not be performed, e.g., schemes that give different treatment to Internet traffic based on application type (for example, real time speech or video). Net neutrality is an important part of the *Open Internet* concept, in which the Internet shall be open and accessible for everybody without any kind of discrimination. Moreover, under the concept *Open Internet*, any consumer's access to or usage of the Internet should not be driven by financial motivations of the ISPs. Net neutrality effectively reduces the ISPs to a carrier of bits between senders and receivers. Any involvement of the ISPs in higher layer functionalities or other services is in general not compatible with net neutrality.

The term net neutrality was coined by Professor Tim Wu in his paper *Network Neutrality, Broadband Discrimination* (2003) and has been the target of much political debate since then. The main issue is whether or not the principle of net neutrality shall be enforced in the Internet or not.

Proponents of net neutrality claim that equal treatment of all services will foster innovation on the Internet and ensure a democratic platform in which all information is treated equally. If net neutrality is not enforced, ISPs may provide fast lanes to established and dominating Application Service Providers (ASPs) for an extra fee, an action which will strengthen the monopolistic competition among ASPs. ISPs may also block or throttle Internet speeds for ASPs competing with the ISP's own services, for example, an ISP offering traditional voice communication in competition with Skype throttles the Internet speed for Skype to gain competitive advantage.

Net neutrality is also required to ensure that the Internet remains a democratic platform. This is so because, without net neutrality in force, ISPs may block content for some reason, for example, political in violation of free speech and democracy. The ISP may also give unequal treatment—both with respect to pricing and quality of service—to competing social media, strengthening the existing monopolistic competition between ASPs.

Opponents of net neutrality claim that net neutrality will reduce incentives of the ISPs to invest in the network and thus slow down further Internet adoption and technological progress and innovation. The ISPs claim that it will be hard for the ISPs to get sufficient returns on infrastructure investments if they cannot charge large Application Service Providers (ASPs)—such as YouTube and Netflix— extra for their enormous usage of the network. Therefore, it is not surprising that the main stakeholders that favor net neutrality include ASPs such as Facebook, Netflix, and Microsoft, while the stakeholders opposing net neutrality include mostly ISPs.

Many countries have passed legislations on net neutrality. Among them, Chile was the first country to pass full net neutrality legislation in 2010. As a consequence of this law, zero-rated applications—including Facebook zero—are no longer available in Chile. In the US, net neutrality has been a source of conflict since the 1990s. The Federal Communication Commission (FCC) published in 2010 a set of six net neutrality principles to govern the providers of Internet access (i.e., ISPs). These six principles are termed the FCC Open Internet Order:

1. **Transparency:** Consumers and innovators have a right to know the basic performance characteristics of their Internet access and how their network is being managed.
2. **No blocking:** Consumers and innovators have a right to send and receive lawful traffic—to go where they want, say what they want, experiment with ideas—commercial and social, and use the devices of their choice. The rules thus prohibit the blocking of lawful content, apps, services, and the connection of devices to the network.
3. **Level playing field:** Consumers and innovators have a right to a level playing field. No central authority, public or private, should have the power to pick winners and losers on the Internet.
4. **Network management:** Broadband providers need meaningful flexibility to manage their networks to deal with congestion, security, and other issues.
5. **Mobile:** The principle of Internet openness applies to mobile broadband.
6. **Vigilance:** Promptly enforcing the rules to be adopted and vigilance in monitoring developments in areas such as mobile and the market for specialized services, which may affect Internet openness.

In the EU, net neutrality is laid down by article 3 of EU regulation 2015/2120: Safeguarding of open internet access.[18] This regulation is a part of the union's Digital Single Market policy, and was announced in 2015. The law broadly ensures net neutrality in the EU/EAA zones. However, countries within the union may specify stricter net neutrality rules than those in the EU regulation. This is done in the Netherlands and in Slovenia. The EU regulation on net neutrality has been criticized for being vague and open up for prioritization of "specialized services" such as: remote surgery and driverless cars. Such prioritization is in violation of the principles of net neutrality, as differentiated treatment of data packets in the network is needed to give higher quality of service to such services. Another criticism of the EU regulation is that it opens up for zero-rated applications. China, on the other hand, has not enforced net neutrality. On the contrary, China blocks certain services, for instance Facebook, within China for political reasons.[19] Net neutrality in the US is a political debated topic, and the current chairman of the FCC has reversed several of the previous net neutrality rulings.

XIII. Device and Search Neutrality

Two terms related to net neutrality are device neutrality and search neutrality. Device neutrality means that any application should be able to run on any device and that any device should be able to run on any network of any ISP without differentiation of price or quality. As explained in Section III and the following sections on standards, the technical infrastructure of ICT supports these requirements. Search neutrality means that search engines shall return unbiased results to the user optimized to provide the most relevant results based solely on the search keywords provided by the user. Hence, commercial interests, promotion of paid services, or services owned by the company offering the search engine should not be a parameter in the algorithm providing search the results. Device and search neutrality have a less—if any—legal basis compared to net neutrality. However, there have been legal cases where companies—most notably Google—have been fined for breaching search neutrality.

Google has been accused for favoring services from their own ecosystem. For this practice, Google was fined €2.42 billion in 2017 by the European Commission.[20] More specifically, Google was fined for manipulating the search results in Google Search to favor results from Google Shopping—a Google service that allows users to search for products on e-commerce websites. Competing price comparison services were—according to the judgement—intentionally put far down on the list of google search results in such a way that consumers often ignored these results. This is a clear violation of search neutrality since Google used its monopoly dominance in the search

[18] See the full text of the regulation: https://eur-lex.europa.eu/eli/reg/2015/2120/oj

[19] Facebook has been blocked in China following the 2009 Ürümqi riots, and has not been opened yet (March 2019).

[20] See: https://www.theverge.com/2017/6/27/15872354/google-eu-fine-antitrust-shopping

market to favor its own products (Google has over 90% market share in the search market in Europe). Google has appealed the decision. Andrew Odlyzko predicts that device and search neutrality may become "hot topics" in the future when net neutrality is—if it ever will be—enforced, representing "the next step" in regulating the Internet.[21] The legal case of *EU vs. Google* on Google Shopping may mark the start of recognizing the importance of search neutrality.

XIV. Business Implications of Net Neutrality

The business implications of net neutrality are significant. With net neutrality in force, ISPs cannot discriminate data from Over-The-Top (OTT) providers—e.g., Netflix, Skype, and WhatsApp—to curb competition with their own equivalent services. Net neutrality works as a barrier and strengthen the division between the business domains of the ISP and the ASP. The ISP has less—if any—opportunities to enter the business domain of the ASP if net neutrality is enforced. For reasons explained in Section IV, full net neutrality divides the business domains of the ISP and the ASP in such a way that the ISP becomes the transporter of bits—a commodity—and the ASP becomes the provider of the services that uses these bits in its service design. This means that the ASP builds its business on the bit-transportation capabilities provided by the ISP and no other features of the network. Therefore, net neutrality has consequences for the business of the ISP since the ISP is reduced to a commodity and cannot enter the—sometimes lucrative—business domain of the ASP. This is one of the reasons why many major ISPs oppose net neutrality.

The ASP may sometimes be willing to pay the ISP extra for caching parts of their content material closer to the consumer. This may be regarded as advanced network management to increase the quality of the ASP service. In this case, certain types of traffic are given priority over other types of traffic but without discriminating traffic belonging to the same type of service. This can be seen as a "mild" violation of net neutrality. 5G mobile systems are planned to exploit these capabilities to reduce latency and traffic load in Internet of Things applications by providing storage and processing capabilities at the radio interface (edge computing).[22]

The Internet was originally designed as a "dumb pipe" or "dumb network" only capable of forwarding IP packets. David Isenberg denoted the Internet the "stupid network" interconnecting intelligent terminals in contrast to the "intelligent network"

[21] Andrew Odlyzko. Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets. Review of Network Economics, vol. 8, no. 1, pp. 40–60. 2009.

[22] Brandon Butler, What is edge computing and how it's changing the network, Network World; https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html

interconnecting stupid terminals in the telephone network.[23] There is no "intelligence" or functionalities built into the IP network apart from those required for routing IP packets hop-by-hop from the sender to the receiver. Management and control functionalities were limited to keeping updated routing tables in the IP routers. If required, reliable end-to-end communication is ensured by the end-to-end protocol Transmission Control Protocol (TCP); if end-to-end reliability is not required, the simpler User Datagram Protocol (UDP) is used. These protocols contains an address called port number identifying the software the receiver requires in order to interpret the information content of the packet. Sometimes the port number is unique for a certain service. However, in most cases, knowing the port number is not enough information to distinguish between various services. To do so, deeper analysis of the content of the packets is required. Differentiated treatment of Internet traffic will require some form of Deep Packet Inspection.

Deep Packet Inspection (DPI) implies, as a minimum, that the network provider reads the UDP/TCP headers to obtain the port numbers to identify the type of protocol being used (shallow DPI) and, if possible, analyzes the actual information in the packet itself (proper DPI). Sometimes shallow DPI is enough for special treatment of the packet; in other cases, for example, distinguishing between different services using the World Wide Web, deeper analysis is required. Information obtained in this way, together with the addresses of the sender and the receiver, is used to differentiate the traffic, i.e., decide how the packets shall be treated in the router queues (e.g., given priority, throttled, or blocked). Proper DPI is not possible for applications using Transport Layer Security (TLS) such as https since information beyond the port numbers is encrypted and cannot be decoded by the inspector of the packet unless the encryption key has been compromised or provided voluntarily or by law to the authority inspecting the packets. DPI is also impossible for packets sent over Virtual Private Networks (VPN) because these networks are usually protected using the strong IPsec encryption protocol and tunneling techniques where even the addresses of the sender and receiver are hidden so that here is no information available for discriminating the traffic.

DPI is used within local networks both at the sending and receiving end (e.g., stateful firewalls and email filtering) to detect illegal operations, intrusion attempts, spam, and malware, and to prevent sending of protected information.

XV. Zero-Rating

Some ISPs, in collaboration with selected ASPs—such as Wikipedia and Facebook—offer zero-rated access to the Internet. This means that consumers get free Internet

[23] David Isenberg, Rise of the Stupid Network Why the Intelligent Network was once a good idea, but isn't anymore.One telephone company nerd's odd perspective on the changing value proposition, https://www.hyperorg.com/misc/stupidnet.html

access, but then only for accessing selected applications or services. Put in another way, unlimited data volumes are provided for a specific application to users opting for zero-rating access. This practice is in conflict with the current strict definitions of net neutrality since it differentiates Internet access based on application—one service can be accessed for free, while another competing service requires paid access.

One example of zero-rating is Wikipedia Zero offering free access to Wikipedia on mobile devices in some countries in collaboration with selected ISPs.[24] The program was launched in 2012 and provided free access to over 800 million people, mostly in developing markets. After receiving criticism for net neutrality violation, Wikipedia Zero discontinued the program in 2018. In some of the areas where Wikipedia Zero was deployed, it was, in fact, the only choice for many people to access the Internet. In these countries, Wikipedia Zero became synonymous to the Internet. In lack of popular services such as YouTube—which was only available to those with a regular mobile data subscription—copyrighted material started to be spread via Wikipedia. This material was mostly removed by Wikipedia editors; however, it also meant that these editors collectively became a central force in deciding what should be available on the Internet through Wikipedia Zero.

Another example of zero-rating is Facebook Zero, a program providing free access to Facebook. Launched in 2010, it currently provides free access to Facebook in collaboration with selected ISPs in more than 30 countries, both developed and developing countries.[25] Compared to Wikipedia Zero, Facebook Zero is more questionable from a net neutrality viewpoint. This is because Facebook is a commercial service and not a nonprofit service as Wikipedia. Providing free access to Facebook changes the competition in the social media market and may further increase Facebook's dominating position in this market. For many users where the Facebook Zero program is available, Internet is synonymous with Facebook.[26]

Twitter has also initiated a zero-rating program—Twitter Zero—which is available for subscribers of selected ISPs in more than six countries.

Zero-rating gives the ISPs the power to select winners in the digital markets motivated by how much they are willing to pay for zero-rating access of their service. Even though zero-rating means free services for the users, the cost of providing this service is in many cases paid by the ASP. Consumers, when everything else is equal, prefer services that have zero-rated access compared to paid access. Therefore, starting a zero-rating program for a service may be a way to circumvent competition, thereby creating a virtual monopoly for this service.

[24] See: https://foundation.wikimedia.org/wiki/Wikipedia_Zero

[25] See: https://en.wikipedia.org/wiki/Facebook_Zero

[26] In Nigeria, Indonesia, India, and Brazil, where the Facebook Zero program is available, more than 50% of the people believe "Facebook is the Internet". For details, see: https://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/

One issue concerning zero-rated content is that ASPs may offer access to their websites or services for free also in cases where these services are not the best services for the consumers. For instance, a bank with high interest rates for loans may pay an ISP to offer free access to its website to attract customers. This will have an undesirable effect on the free market for loans. A particularly vulnerable target group for such practices is poor people with few other opportunities to access the Internet than through a zero-rated service.

XVI. Conclusions

Digital goods and services are building blocks in the digital economy. With the increased societal dependence on digital services, there is a need to ensure that these services are provided in a well-functioning digital market promoting competition, innovation, low prices for consumers, optimal usage of resources, and respect for individual rights. Standards and regulations are two key areas that—if deployed wisely—ensure that the digital economy exploits its full potential.

The paper presents a broad overview of important issues related to standardization and regulation of the Internet. The paper includes also a survey of standards and standards organizations, describes how these standards shape the digital markets, and argues why regulation is required in the digital economy to support competition on fair terms. The paper raises several issues concerning net neutrality and recent developments such as using zero-rating to provide access to digital services.

Standards and regulations will play a vital role in the future development of ICT and the digital economy, and even more so as the digital economy grows to become a bigger part of the world's economy than today. From being an unregulated business, a number of new legislations concerning ICT, such as laws on net neutrality and data protection regulations (such as GDPR in the EU/EEA), will be established. These legislations will shape the future evolution of the digital economy, requiring new business models and restructuring of the companies in the digital economy, and preparing the ground for future standards and regulations.

XVII. Bibliography

Andrew Murray. Information Technology Law: The Lay and Society. Oxford University Press. 2016.

Andrew Odlyzko. Network neutrality, search neutrality, and the never-ending conflict between efficiency and fairness in markets. Review of Network Economics, vol. 8, no. 1, pp. 40–60. 2009.

Harald Øverby, Jan A. Audestad. Digital Economics: How Information and Communication Technology is Shaping Markets, Businesses, and Innovation. CreateSpace. 2018.

Jan A. Audestad, Internet as a multiple graph structure: The role of the transport layer, Information Security Technical Report, Vol. 12, No. 1, 2007.

Kevin Werbach. The song remains the same: what cyberlaw might teach the next internet economy. Florida Law Review, Vol. 69, Iss. 3, Art. 5, 2018.

Lawrence Lessig. Code 2.0. Basic Books. 2006.

Tim Wu. Network Neutrality, Broadband Discrimination. Journal on Telecom and High Tech Law. 2003.