Part 2: Where are we now?

Having sketched the development of the Internet from the late 1960s to the late 1990s, in Part 2 of this report we focus on more recent developments and their implications for a future Internet. The goal is to provide an overview of some of the key issues and highlight trends that bear on our present thinking about the future of the Internet.

6. New Forms of Collaboration and Interaction

With the World Wide Web taking off in the late 1990s, the Internet ecosystem reached its next stage. This section describes the circumstances under which the Internet went public, sketches the main drivers behind this growth and describe how the Internet turned into the social web with its new forms of collaboration and interaction.

6.1 The Internet Goes Mainstream

The late 1990s and 2000s saw a radical growth of the Internet’s user base. While until around 1995 the Internet had largely been the domain of technologically savvy researchers, geeks, businessmen and amateurs, the new web-based services and markets opened up the network for people who had no particular previous affinity to networked computing. The growth in terms of Internet users is hard to measure and can only be estimated. According to Internet World Stats, the total number of Internet users increased from 360,985,492 in 2000 to an estimated 1,596,270,108 in 2009, which means that today well over 20% of the world’s population are online.107 More reliable are counts of Internet hosts, i.e. machines connected to the Internet. As Figure 4 shows, the number of hosts on the Internet has grown significantly from just over 2 million in 1992 to well over 625 million in January 2009.108

---

108 The survey treats virtual hosts as single hosts.
Similarly, the number of websites has grown exponentially from just a small number in 1996 to 232 million in April 2009 (Figure 5).

The growth in terms of users, hosts, and websites can be seen as the result of a number of technological, social, and economic developments. The uptake of broadband connections in households in the early 2000s has enabled a new range of applications, allowing for the uploading and downloading of rich media files and applications. The increasing bandwidth marked a significant improvement compared to previous years.

---

to the earlier dial-up connections with limited throughput and robustness. Also
processing and storage capacities of computing devices increased steadily, making
room for more complex and interactive applications as well as the transmission of
complex multimedia files in an increasing number of formats. Finally, a new
generation of software with graphical user interfaces and more user-friendly designs
made it easier for non-geeks to take part in the network of networks and emerge as an
important and commercially lucrative user group.

From a social perspective, the newly accessible technologies attracted a large group of
new users. Young people, today’s “digital natives”\textsuperscript{110}, take for granted the range of
applications and web services they have grown up with. The new Internet has
supported many new forms of expression, making it increasingly attractive for users
to build new identities online and take advantage of pervasive pseudonymity. At the
same time, communities have developed around online worlds, games and
collaborative projects, drawing more people further into online activities. Many other
activities now have some online component, be it politics, hobbies, or commerce.
Once critical mass was reached, network effects made the communication networks
even more useful and has recently become a common feature of life in the developed
world to be “online” or even “always on.”

Economically, the new technologies and devices have become increasingly affordable
and allow for greater connectivity of more and more people. The low search costs of
online services have at least theoretically benefited a “long tail” economy, allowing
retailers big and small to match marginal products with customers.\textsuperscript{111} Retailers like
Amazon.com are important players on the web, selling extremely niche special-
interest literature, music and video alongside their predominant business in
bestsellers. The same is true of many other diversified products and services from
flights, vacations, and jewellery to furniture, medicine, and even cars. Peer-to-peer
marketplaces like eBay.com have made it increasingly easy for individuals to sell and
buy the most idiosyncratic things.

\textbf{6.2 The Rise of the Social Web}

Naturally, the widespread adoption of Internet technologies and their increasing
pervasiveness had consequences for how the web was used, what it was used for, and
the role it played in the everyday lives of users. After the hype around “electronic
commerce” in the late 1990s and the burst of the dotcom bubble in the middle of
2000, a range of new services emerged that enabled new forms of interaction with and
through technology.

The most popular label applied to this development is “web 2.0,” commonly used to
describe new approaches to “facilitating communication, information sharing,
interoperability, and collaboration on the World Wide Web.”\textsuperscript{112} According to Tim
O’Reilly, to whom the concept is originally attributed, the key tenet of web 2.0 is to
“[b]uild applications that harness network effects to get better the more people use
them.”\textsuperscript{113} Also called “participative web” or “read/write web”, this new understanding

\textsuperscript{110}\textit{Cf.} John Palfrey & Urs Gasser, \textit{BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF
DIGITAL NATIVES} (2008).
\textsuperscript{111} For a more detailed analysis of how digitally networked technologies have affected business, see
section 12.
\textsuperscript{113} Tim O’Reilly, Web 2.0 Compact Definition: Trying Again, Oct. 12, 2006,
of the Internet as a communications platform is based on intelligent web services and applications that enable users to collaborate and contribute to developing, rating, extending, commenting and distributing content as well as other Internet applications.\textsuperscript{114}

Examples of such applications abound. The online encyclopaedia Wikipedia, blogging services like Blogger, LiveJournal and Twitter, photo- and video-sharing websites like Flickr or Kaltura, file-sharing applications like Napster and BitTorrent, news aggregators like Digg, Reddit and Slashdot, collaborative link collections like Delicious, or contextualised advertising like Google AdSense—all these services build in one way or another on the intentional (or trans-intentional) participation of users and the data produced through their activities.

Different types of such user-generated content can be distinguished:\textsuperscript{115}

- **Text**: amateurs share poems and stories in BBS and forums to get feedback from their peers. A very successful genre is, for example, fan fiction, where authors use existing characters from movies or other fiction to write and publish their own stories.\textsuperscript{116} Other examples are user-generated news and citizen journalism, which can be found on websites like OhMyNews, Liveleak or Twitter.
- **Photos**: thanks to the widespread proliferation of digital cameras, photos can be shared easily by uploading them to websites like Flickr.
- **Music**: with the right software and a microphone, users can produce podcasts, i.e. radio-like broadcasting shows, or remix existing songs into new ones.\textsuperscript{117}
- **Video**: user-generated video includes home videos, but also lip-synching performances or remixes of movie trailers. A number of websites provide outlets for footage shot and edited by amateur journalists.
- **Comments & Feedback**: A final category of user-generated content includes the comments and feedback people post about products, services, or whatever else they are interested in. For example, product reviews and “online word of mouth” may help companies improve their product line and help other users make better-informed purchase decisions. Similar patterns can be found on rating sites or Q&A forums like “Yahoo! Answers.”

As diverse as these types of user-generated content are the platforms on which they are distributed. Many of these developed new business models, attracting large numbers of users.

- **Blogging and podcasting services** allow for cheap and easy publishing and editing.

\textsuperscript{115} Cp. OECD, PARTICIPATIVE WEB, supra note 109, ch. 4.
\textsuperscript{116} See, e.g., the websites fanfiction.com and quizilla.com.
• Photo- and video-sharing sites like Flickr and YouTube provide platforms for personal publishing but also more professional broadcasting channels.

• Wikis and other text-based collaboration platforms let users collaboratively edit text.

• Aggregators and social bookmarking services gather decentralised feedback and process them into new and useful meta-data.

• Social networking sites like Facebook, MySpace or Cyworld let users create profile pages and interact with one another through their websites.

• Virtual worlds like Second Life or World of Warcraft constitute more or less immersive environments, in which people move and interact through graphic-based avatars, building (or better: coding) their own worlds.

While data on the extent and forms of user participation in the social web is hard to find, some statistics show that certain aspects like posting messages to chat rooms, newsgroups or forums, using peer-to-peer file sharing sites and creating web pages are very popular. According to a recent OECD survey, especially younger users are active content creators. Between 55% and 70% of all Internet users aged 16-24 posted messages to chat rooms, newsgroups and forums in 2005 in Hungary, Denmark, Iceland, Finland, Norway, Germany, Poland, and Luxembourg; in many OECD countries more than a quarter of users in this age group have created a web page (Figure 6). Another study finds that 13% of Europeans were “regularly contributing to blogs”, while 12% were “downloading podcasts at least once a month” in 2005.

Among the most popular platforms of the social web are social networking sites. 41.7 million regular users of social networking sites were counted in 2008 while more than 56% of the European online population visited social networking sites in 2007; from 2007 to 2008, the number of visits saw an increase of 35%.

Figure 6: User-generated Content Creators Aged 16-24 in the EU as a Percentage of Internet Users in 2005

(Source: OECD, Participative Web and User-Created Content (2007), p. 20)

User-generated content

---

118 See OECD, PARTICIPATIVE WEB, supra note 109, at 20.
websites are among the most frequently visited and fastest-growing worldwide. In May 2009, the web ranking service Alexa counted YouTube, Wikipedia, and Blogger among the top 10 most visited websites. The social networking site Facebook currently counts 250 million active users\textsuperscript{121}, the VoIP service Skype reports more than 400 million registered users in 2008.\textsuperscript{122}

It has been argued that the advent of the social web has brought about significant transformations in culture and creativity. The argument is that the decentralised end-to-end architecture of the Internet has enabled new forms of participation and the "democratisation" of knowledge production in a "participatory culture".\textsuperscript{123} The distinction between consumers and creators of information and knowledge is increasingly blurred due to advanced options for interacting with content and other users in a number of ways.\textsuperscript{124} It has been argued that individuals and small groups “can express themselves, exchange views, and create their own information environment with a reach and efficacy not possible since the rise of mass media”.\textsuperscript{125}

Referring more generally to processes of innovation also in non-Internet contexts, Eric von Hippel described how users and consumers have become major sources and drivers of innovation in the development of software, information goods, and physical products.\textsuperscript{126} Thus, while creative participation seems greatly enhanced by the widespread use of broadband communication and networked computing, the process does not appear to be exclusive to the Internet.

At the same time, some authors have offered more critical perspectives on this development. For example, it has been asked what the concept of “information quality” should mean in a world of engaged amateurs and how it can be ensured.\textsuperscript{127} In a world in which information is seemingly limitless, how can we distinguish between "urban myth" and reality? How is relevance constructed and who decides on the criteria for what counts as useful and what not? What effect is digital multi-tasking having on the attention span of individuals at any age, and how can this be better managed?

6.3 Opportunities and Challenges of Peer Production

Given the popularity of the social web, authors have tried to conceptualise its dynamics in more theoretical terms and think about its broader social and economic implications. One of the most widely discussed analyses comes from Yochai Benkler,

\textsuperscript{123} See, e.g., Urs Gasser & Silke Ernst, \textit{From Shakespeare to DJ Danger Mouse: A Quick Look at Copyright and User Creativity in the Digital Age}, Berkman Centre Research Publication No. 2006-05, June 2006.C
\textsuperscript{125} Id., at 567.
\textsuperscript{126} See Eric von Hippel, \textit{DEMOCRATIZING INNOVATION} (2005).
who has coined the concept of “peer production” to capture the activities on new platforms for cooperation and collaboration on the social web.\textsuperscript{128}

Peer production refers to “production systems that depend on individual action that is self-selected and decentralised, rather than hierarchically assigned.”\textsuperscript{129} The claim is that these peer production systems differ substantially from market-based price systems and managerial structures for coordination. Peer-produced information is regarded as an integral element of the emerging “networked information economy,” turning producers and consumers into equal users of an information commons.

Commons theory features prominently in analyses of new forms of collaboration. The rubric of commons denotes a particular institutional way of structuring rights to access, use, and control resources. Most importantly, no single person has exclusive control over the use or disposition of any particular resource. Constraints, if any, are symmetric and apply in the same way to each individual user.\textsuperscript{130}

One could argue that these new forms of collaboration echo many of the foundational architectural principles of the early Internet. In order to realise the pervasive network effects characteristic of the social web, the platforms need to be “open” in the broadest sense, allowing cheap and easy access for a large number of users. Also the idea of the architectural principles can be found in many of the new concepts like “collective intelligence” or “crowd wisdom.” In this context, intelligence does not refer to the capacities of the hard- and software connected to a network, but the possibility of tapping the feedback of a large number of people.

Another parallel can be found in the practices of early and contemporary Internet communities. For example, the early RFC procedures for putting out a new idea or standard for discussion with a community of peers is not too different from the practices that have made the online encyclopaedia Wikipedia so successful, where all edits are made public and are reviewed by an unspecified group of pseudonymous contributors. Hence, in the same way that the initial “network of networks” grew rapidly through the principles of interoperability, redundancy, and end-to-end, most platforms on the social web depend on these features to scale effectively and reach critical mass. In all these cases, network effects will only work if access to the networks is open in principle, i.e. with minimal economic, technical, social and institutional barriers.

However, while peer production and the social web may stimulate creativity and generate considerable social and economic value, it also poses some new regulatory challenges, which are discussed more thoroughly in the next section. Key questions here concern liability for peer-produced information. For example, to what extent should platform operators be held responsible for the actions of individual users on their platforms, such as defamation or copyright infringement? This is especially problematic since the social web is not based on a regime of trusted parties like the early Internet. Rather, identities are largely ephemeral with contributors staying anonymous. While this lowers the barriers to participation, it may also allow users with malicious intent to take advantage of the situation. Another issue is the distribution of rights in the works produced on the social web. Creative Commons has developed a successful and easily understandable licensing scheme to facilitate this

\begin{footnotes}
\item[128] See Benkler, supra note 86, ch. 3.
\item[129] Id. at 62.
\item[130] Id. at 61-62. See also Elinor Ostrom, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION (1990).
\end{footnotes}
7. Governance and Regulation

The “webification” of the Internet has posed new challenges to governance and regulation. With the steady influx of new users turning the web into an attractive platform for retail and service industries, an increasing number of businesses started claiming their territories and built web presences to compete in the “new economy.” Not surprisingly, this shift in quantity and quality of Internet use had substantial implications for governance and regulation. Four aspects seem particularly noteworthy: the never-ending story of ICANN and the struggle for control over the domain name system (7.1), the emergence of inter-governmental initiatives and multi-stakeholder approaches (7.2), the attempts by national governments to indirectly regulate Internet-mediated activities (7.3), and the evolution of community governance and “netizenship” (7.4). This section closes with a brief overview of the main regulatory issues currently on the policy agenda (7.5).

7.1 The Case of ICANN and the Politics of the Domain Name System

As a global federation of networks, the Internet has only a few centralised resources that would require a central coordinating authority. One such area is the standards and protocols that ensure interoperability and connectivity. The responsibility for standard setting at the level of the network lies with the Internet Engineering Task Force and its informal community of tech-savvy volunteers. The World Wide Web Consortium (W3C) has taken on a similar role for the web since 1994. So far, W3C has published more than 110 standards called “W3C Recommendations.” In contrast to IETF’s rather loose-knit organisation, W3C consists of more than 400 institutional members around the world and a smaller full-time technical team of experts, driven by the belief “that the most fundamental Web technologies must be compatible with one another and allow any hardware and software used to access the Web to work together.”

However, the main subject of debates over Internet governance from the mid-1990s has been over the Domain Name System (DNS), which translates human-readable addresses into IP addresses.

Historically, the DNS played a rather peripheral role. The IETF had conceived of domain names as arbitrary strings of characters, which were allocated on a first-come, first-served basis: “[r]egistration of the mapping between domain name and IP address confers no ownership beyond establishing this relationship for Internet

---

133 The history of standard-setting arrangements can be read as an avalanche of ever-new acronyms: ARPA and the Network Working Group (NWG) with their original authority over network connectivity, the Internet Configuration Control Board (ICCB) as an advisory group for ARPANET, the foundation of the Internet Activities Board (IAB) in 1984, the split of IAB’s board into the Internet Engineering Task Force (IETF) for protocol development and the Internet Research Task Force (IRTF) for long-term planning, the adoption of IETF’s standards by all major U.S. government agencies, and the foundation of the Internet Society (IS) in 1992 with oversight of IAB and IETF as a major step in the privatization of Internet infrastructure. See generally, Ian Brown, Standards (Global): Internet Engineering Task Force, in: Chris Marsden et al. (eds.), Options for and Effectiveness of Internet Self- and Co-Regulation – Phase 2: Case Study Report, January 15, 2008, pp. 51-60
135 W3C Website, About the World Wide Web Consortium (W3C), http://www.w3.org/Consortium/Overview (last visited June 1, 2009).
136 For a comprehensive overview, see Mueller, supra note 132.
addressing purposes.”

This engineering ethos could not be upheld with the advent of the web. With demand skyrocketing during the 1990s, domains became critical brand icons for individuals, companies, and organisations. Inevitably, fierce conflicts emerged over legitimate claims to domains. The domain name system became political.

As a consequence, a variety of actors and organisations struggled with the question of how to best to govern the operation of the root servers, the allocation of domain names, and the administration of top-level domains (such as .com and .org). Originally, the U.S. government delegated the authority over Internet addresses to the Internet Assigned Numbers Authority (IANA), managed single-handedly by John Postel at the University of Southern California. After the contract expired in 1997, the U.S. Department of Commerce decided in September 1998 to establish a new self-governing organisation for overseeing the DNS: the Internet Corporation for Assigned Names and Numbers (ICANN).

Incorporated as a non-profit corporation under Californian law, ICANN operated on the basis of a Memorandum of Understanding with the U.S. Department of Commerce.Governed by a board of fifteen voting directors, five of which had initially been selected through Internet-wide elections, ICANN exercised its power following broad consensus, for example when creating new top level domains or reassigning the power to register domain names for certain geographic areas. Yet, despite these institutional arrangements, ICANN remained the subject of fierce criticism.

While some criticised the lack of democratic procedures and the perceived influence of lobbyists, others voiced scepticism about ICANN’s dependence on the U.S. Department of Commerce. European governments were critical of the structural U.S. dominance and called for an international approach to naming and numbering. As early as 1998, the European Commission feared that an organisation like ICANN would “consolidate permanent U.S. jurisdiction over the Internet as a whole.” Other conflicts were triggered, for example, during the lengthy negotiations over a new .eu top-level domain.

This long-standing political struggle is likely to resurface soon: the current agreement between ICANN and the U.S. Department of Commerce will expire on September 30, 2009. Havingfavoured various intergovernmental, multi-stakeholder, and rights-

---

138 Internet Corporation for Assigned Names and Numbers [ICANN], http://icann.org/ (last visited June 1, 2009).
139 Memorandum of Understanding between the U.S. Department of Commerce and Internet Corporation for Assigned Names and Numbers (Nov. 25, 1998), http://www.icann.org/general/icann-mou-25nov98.htm.
140 From the vast literature about ICANN, see only Tamar Frankel, Governing by Negotiation: The Internet Naming System, 12 CARDOZO J. INT’L & COMP. L. 449 (2004); .
based solutions in the past, the EU Commissioner for Information Society and Media Viviane Reding has now called for a full privatisation of ICANN, accompanied by an independent judicial body and a “G12 for Internet Governance.” It is not year clear what position the Obama administration will take.

7.2 International Initiatives and the Rise of Multi-Stakeholderism

Partly as a reaction to the continuing struggles over ICANN, its failed experiments in self-governance, and perceived U.S. dominance, another development started to take root in the late 1990s: the emergence of multi-stakeholderism, an approach that aims to bring representatives from all areas of society into the policy-making process—and not just governments. It was felt that also the private sector, civil society, and international organisations should hold a “stake” in the governance of the Internet.

A first move in this direction was launched in 1998 when the ITU took the initiative to organise a World Summit of the Information Society (WSIS). The plan was formally approved in a UN General Assembly resolution in 2001 and foresaw a multi-year two-phase WSIS process. The goal of the first phase (“Geneva Phase”) was “to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all” and resulted in a Declaration of Principles and a Plan of Action. The second phase (“Tunis Phase”) aimed “to put Geneva’s Plan of Action into motion as well as to find solutions and reach agreements in the fields of Internet governance.”

While WSIS had started with a rather comprehensive focus on information society issues in general, Internet governance proved to be a contested topic. Especially the ongoing intergovernmental conflicts over ICANN dominated the agenda of the 2003 Geneva meeting—excluding the majority of stakeholders that were originally supposed to play a more important role. As a consequence, a special Working Group on Internet Governance (WGIG) was set up in 2003. In a series of meetings that now also involved non-governmental stakeholders, WGIG developed a working definition of Internet governance, identified relevant public policy issues like infrastructure management, security, privacy, intellectual property, and international development, and recommended the “creation of a new space for dialogue for all stakeholders on an equal footing on all Internet governance-related issues.” The WGIG report was an important input for the 2005 Tunis phase, which incorporated

---

142 See, e.g., Viktor Mayer-Schönberger & Malte Ziewitz, Jefferson Rebuffed: The Future of Internet Governance, 8 COLUMBIA SCIENCE AND TECHNOLOGY REVIEW 188 (2007) for an analysis of the WSIS negotiations in the light of these conflicts.
144 See International Telecommunication Union, Basic Information: About WSIS, http://www.itu.int/wsis/basic/about.html (last visited June 1, 2009).
147 See International Telecommunication Union, Basic Information: About WSIS, http://www.itu.int/wsis/basic/about.html (last visited June 1, 2009).
148 See Hofmann, Internet Governance, supra note 69, at 17.
some of its ideas in its final outputs, the Tunis Agenda\textsuperscript{150} and the Tunis Commitment.\textsuperscript{151}

While the WSIS process had made clear that the Internet is an essential component of the information society, it had not resulted in any concrete policies. On the contrary, governments and other stakeholders were at odds over their respective roles and control over infrastructure. As a way out of this heated debate, Paragraph 72 of the Tunis Agenda recommended a new arena for multi-stakeholder dialogue about Internet-related international public policy issues: the Internet Governance Forum (IGF). The Tunis Agenda also set out principles that determined the scope and approach of the new IGF. On the one hand, it defined Internet governance as “the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet” (Paragraph 34). On the other hand, it stated that Internet governance should be “multilateral, transparent and democratic, with the full involvement of governments, the private sector, civil society and international organisations”, thus strengthening the multi-stakeholder approach (Paragraph 29). While convened by the U.N. Secretary General, the IGF did not follow formal U.N. procedures. With a five-year mandate from 2006-2010, it conducts annual meetings, which are open to anyone and so far have been held in Athens (2006), Rio de Janeiro (2007), and New Delhi (2008). The IGF does not have any decision-making authority, but can identify problems and recommend solutions to the relevant publics.

While these attempts to create multi-stakeholder regimes have received a lot of media attention, some have questioned the benefits of this development. For example, it has been criticised that a key group that could tackle many of the new policy problems by designing tools for user and grassroots initiatives—computer scientists—are missing from the deliberations.\textsuperscript{152} Others have argued that a focus on broad categories and concepts like “stakeholders” distracts from the fact that most governance actually happens on the ground in the context of everyday interactions of individual users, and not in abstract discourses about institutions, processes, and organisations.\textsuperscript{153} It is therefore difficult to say whether the IGF has any regulatory effect beyond providing a new discussion forum for Internet-related policy issues.

7.3 New Forms of Government Regulation and Co-Regulation

It has long been observed that the regulatory capacity of nation states and supranational entities like the European Communities is seriously challenged in digitally networked environments. Costly or simply impossible enforcement, quickly outdated legislation, jurisdictional limits, clashing value systems, unintended consequences, and knowledge gaps on part of regulatory agencies—national and supra-national regulators have been struggling with such problems since the early days of the Internet.

However, while it can be argued that these concerns marked the beginning of Internet governance as a field for policy and research, governments are far from giving up on Internet-related issues. On the contrary, regulators have intervened on a number of occasions, ranging from the European competition law case against Microsoft to consumer protection in e-commerce, the regulation of telecommunications industries, and data protection legislation. In addition to these traditional forms of regulation, a number of new and “light” forms of regulation have been developed that are intended to allow regulatory agencies to exercise authority in digitally networked environments.

A prominent example of such alternative approaches concerns intermediary regulation. When the actual targets of a certain policy cannot be reached directly, governments traditionally resort to indirect forms of regulation by trying to influence third parties, on which the actual target depends for its activities. Such indirect enforcement strategies work best when the third party is a gatekeeper, i.e. provides some essential service in the absence of which the illegal activity could not be conducted. In the context of the Internet, these are usually those who carry, host or index other people’s content: ISPs, search engines, hosting companies, and platform operators. A common strategy is therefore to impose legal liability on these gatekeepers and thereby “delegate” responsibility for enforcement to private entities. While sometimes developed under general doctrines of tort law, many countries have established explicit rules that specify the conditions under which certain intermediaries are required to take action against supposedly illegal behaviour on their platforms. In the EU, for example, the E-Commerce Directive foresees a gradual liability regime for ISPs depending on their functions as mere conduits, caching providers, or hosts. The challenge in these cases is to strike the delicate balance between imposing costs on innocent third parties and mitigating the harm done by the actual targets. This is especially important since users have very different rights to appeal depending on whether they are regulated by a private actor or a public agency. Because of the potentially serious consequences for platform operators, the discussion is sometimes framed in terms of “safe harbours” for intermediaries.

Another approach, which has recently gained currency, is referred to as “co-regulation.” Co-regulation denotes a form of regulation which is neither state command-and-control regulation, nor “pure" self-regulation as observed in industry-led standard setting. Co-regulation implies “an appropriate level of involvement by the public authorities” combining non-state regulation and state regulation in such
a way that a non-state regulatory system links up with state regulation. A recent example of co-regulation in action is the German regime for the protection of minors in the media, which includes an independent commission (Commission for the Protection of Minors in Media, Kommission für Jugendmedienschutz, KJM) overseeing the self-regulatory activities of media companies. 

A key challenge here is to find ways to guarantee transparency, accountability and due process in these often complex institutional arrangements between public and private actors.

In addition to such forms of more or less direct government regulation, a variety of industry-led self-regulatory initiatives can be observed in Internet-related settings. For example, search engine providers in Germany have voluntarily adopted a code of conduct that requires signatories to exclude certain content form search results. A key question here is to what extent such initiatives are primarily attempts to pre-empt government regulation and thereby circumvent constitutional protections against censorship or related guarantees of fundamental rights like freedom of speech and due process.

7.4 Evolution of Community and Grassroots Governance

Besides intergovernmental struggles over the domain name system, global initiatives for multi-stakeholder solutions, and new forms of direct and indirect government and industry regulation, community and grassroots governance have also developed further on the web. The advent of social media has led to a range of new mechanisms and regimes that are often forgotten in the shadow of the high-profile discussions over Internet governance at IGF, ICANN and regulatory agencies. In contrast to the previous sections, the focus here is not on governance of infrastructure, but on governance on and through infrastructure.

Community governance regimes are as diverse as the communities in which they operate. The online marketplace eBay, for example, has developed a variety of mechanisms to protect users from fraud and establish trust among strangers. A famous element of this regime is the Feedback Forum, which allows users to rate and comment on the performance of transaction partners for future users’ reference. A similar regime has been developed for the online news website Slashdot, where a two-tiered distributed moderation system allocates visibility and social status. Such decentralised systems often help establish the communities they govern in the first place.

---


163 See, e.g., Marsden, supra note 159, at 6-7.


Arguably the most discussed phenomenon in the area of community governance is Wikipedia, the online encyclopaedia that anyone can edit. Currently, Wikipedia counts more than 13,000,000 articles in more than 260 languages with over 75,000 active contributors worldwide.\textsuperscript{167} Behind the scenes of this successful project, a complex system of roles, responsibilities, and policies has developed on the basis of the simple claim “ignore all rules.”\textsuperscript{168}

While these emerging forms of governance are usually limited to very specific communities, a different and possibly farther-reaching phenomenon are forms of governance and regulation that originate from skillful technical design embedded in grassroots movements. Usually, these approaches start with an easy and scalable innovation of a technological or cultural kind and then spread widely over the Internet, having a considerable regulatory impact. A prime example is Creative Commons, a non-profit organisation. It offers a free and easily understandable set of licenses to users who want to waive some of the rights they hold in their own creative works.\textsuperscript{169} Another example is StopBadware, an online “neighbourhood watch” that aims to identify and profile malicious software, gathering data in a central clearinghouse and using the resulting information to warn and teach individual users.\textsuperscript{170} For example, in a recent partnership, StopBadware teamed up with search engine provider Google to include badware warnings in its search results. A third example is the networked application Herdict that uses crowdsourcing to learn about and present a real time view of the experiences of users around the globe with filtering.\textsuperscript{171}

While these initiatives promise to scale easily and thus constitute a form of governance that takes advantage of the specific socio-technical dynamics of the Internet, experiences with earlier schemes show that this does not necessarily have to be the case. The Internet Content Rating Association (ICRA), for example, started out as an “end-to-end”-inspired self-labelling regime, but failed to gain sufficient traction among users despite EC funding and U.S. government support. In addition, such socio-technical solutions may lack safeguards and provisions that ensure basic standards of fairness and due process.

7.5 Perspectives and Challenges for Internet Governance and Regulation

Having surveyed some recent developments in the area of Internet governance, it seems appropriate to draw some conclusions about the state of governance and regulation on the web. Given the increasing pervasiveness of networked computing, the struggles for ownership and control are likely to continue. Some key issues on the agendas of policy-makers are:

- **Intellectual property:** In view of ubiquitous peer-to-peer file sharing and copying of digitised information goods, there is an ongoing struggle over

\textsuperscript{169} Creative Commons, \url{http://creativecommons.org/} (last visited June 2, 2009).
\textsuperscript{170} StopBadware, \url{http://www.stopbadware.org/} (last visited June 2, 2009).
\textsuperscript{171} Herdict Web, \url{http://www.herdict.org/web/} (last visited June 2, 2009).
control and ownership in digitally networked environments. Existing regulatory regimes of exclusive rights over intellectual property are either considered too lenient, out-of-date, counterproductive or simply useless. Lobbyists of rights holders and proponents of the “free culture” movement engage in fierce debates about how to define and operationalise “fair use” and exceptions from copyright. New approaches like Creative Commons or blanket licensing schemes are being discussed.\(^{172}\)

- **Privacy:** The dramatic increase in computing power, bandwidth and storage capacity has radically increased the ability of organisations to collect, store and process personal data.\(^ {173}\) This is a potential cause for concern. On the one hand, new technologies like ubiquitous computing, surveillance technologies, biometrics, behavioural advertising, or social networking provide a hitherto unknown arsenal for eroding privacy. On the other hand, general social and political fears of terrorism, child pornography, or organised crime may drive both public and private authorities to make use of these possibilities. Overall, these developments are generally thought to pose a serious challenge to existing privacy laws and principles.

- **Inequality and Access to Knowledge and Infrastructure:** With the increasing importance of networked computing for more and more areas of our lives, being excluded from the Internet may constitute a serious disadvantage. A major focus of regulatory activities will therefore be on ensuring access to infrastructure and knowledge for as many people as possible.

- **Cybercrime:** As discussed in the next section, cybercrime remains a major issue for policymakers and law enforcement agencies. Besides problems with fraud, key concerns include malware, spam and cyberwar attacks.

- **Network management and investments in infrastructure:** Given the crucial importance of both fixed and wireless broadband for the further growth of the Internet, policy-makers need to develop policies to encourage and support investments into infrastructure. In addition, issues of network management at the international level are likely to remain important.

While specific problems will be discussed in greater detail in the following sections, the following themes and trends may be helpful for thinking about the future of governance and regulation in Internet-related settings. A first theme revolves around the question of who, which or what actually regulates. While early debates about Internet governance and regulation were specifically concerned with the role and reach of the state and regulatory agencies in ensuring “order” in digitally networked environments, the discussion now includes a variety of other actors like private companies, industry-based self-regulatory arrangements, community governance, as well as non-profit and activist organisations. Even algorithms and “intelligent” forms of code play an increasingly important role in ordering and coordinating action and challenge our understanding of regulatory agency.

Another theme concerns the question of how to ensure appropriate regimes of checks and balances for these more elusive forms of governance and regulation. While state

---


regulators are—at least in theory—subject to a more or less clearly defined institutional arrangement of oversight and control, this may not necessarily be the case for many of the new actors and governance networks. This has led to approaches that emphasise the need for regulating the regulators in the form of co-regulation or regulated self-regulation. Others have asked to what extent regimes of community governance should be subject to judicial review or should be granted autonomy. At an international level, it has been proposed to adopt an Internet Bill of Rights that could act as a guideline for regulatory activity. This idea has recently gained attention also in the European arena.

The multiplicity of orders and regulatory regimes is not a fundamentally new phenomenon. Competition and interaction among a variety of non-state regulatory regimes has long been noted by analysts in areas as diverse as international diamond trade, cattle farming and Wikipedia, challenging the conventional set of analytical and conceptual tools of lawyers and political scientists. One of the key challenges will therefore be to figure out how best to understand these new developments and manage their interactions and frictions on a day-to-day basis.

---

180 See, e.g. Forte & Bruckman, supra note 168.
8. The Seamy Side of Eden: Countering Internet Failures to Protect

As the web has become an integral part of our everyday lives, it has also become an attractive platform for all kinds of criminal activities. As a flipside of greater autonomy, self-direction and individual freedom, there is the risk that certain users may take advantage of the “openness” of the Internet and inflict harm on others. In a world of limited authentication, unclear jurisdiction, and little transparency, deceptive, manipulative and outright malicious behaviours are a significant problem.

8.1 The Scope of Cybercrime

Crimes committed via the Internet and other computer networks are generally referred to as “cybercrime.” The concept comprises a broad range of offences from computer fraud, online stalking, and breaches of network security to the electronic distribution of child pornography, identity theft, and hate speech. A range of organisations is affected. Platform operators and service providers are concerned for the safety of their customers and brand value, governments and law enforcement agencies have struggled with their limited reach and jurisdiction online, and international organisations have launched initiatives to tackle the global dimensions of the problem.

The result has been a variety of approaches to cybercrime, addressing different aspects and concerns. For example, some online communities established teams of private investigators to police their realms. eBay hired its own law enforcement unit when auction fraud became rampant in the early 2000s. Editors on Wikipedia got together and formed an anti-vandalism unit, when destructive behaviour become a common phenomenon. State governments tried to regain their authority in the online realm, tailored their criminal codes to the special conditions of digitally networked environments, and created new laws to address novel offences like cyberbullying or cyberstalking.

At the international level, the most notable attempt to establish a regulatory framework against cybercrime has been the “Convention on Cybercrime,” an international treaty drafted by the Council of Europe with support from Japan, Canada, and the U.S. Originally adopted by the Council in November 2001, the Convention was signed and ratified by 15 states while a further 28 signed it without ratification. The goal of the convention is to harmonise national criminal laws in the area of cybercrime, provide procedures that allow the efficient investigation and prosecution of cybercrime offenders, and establish an international regime for cooperation.

However, in addition to concerns over civil liberties and privacy being unduly affected by the powers granted to national law enforcement agencies under the Convention, some signatories have had difficulties in transposing the provisions of the Convention into domestic law. For example, under U.S. constitutional law and free speech provisions, a ban on virtual child pornography as foreseen by the Convention could not be upheld. Whatever is done to prevent criminal activities from happening on the Internet has to strike a delicate balance between the need to fight crime and preserve the individual freedom that so many see as the unique feature of the Internet.

---

In the following paragraphs, we will sketch some particularly pertinent criminal online activities, assess their nature and challenges, as well as outline some exemplary responses.

8.2 Identity Theft, Phishing, and Other Forms of Online Fraud

Identity fraudsters, phishermen and other scammers all capitalise on the limited authentication capabilities of the Internet and the limited experience of users in making trust-based decisions in digitally networked environments. The web has allowed large numbers of novice users to join the networks, who often start with only a limited degree of media literacy and awareness of security risks.

A key challenge is that computer-mediated communication is largely based on digital representations of identities. The information on which trust decisions are based can, at least in principle, be easily manipulated at low costs. At the same time, the many and often very subtle social cues we are used to in face-to-face interactions do not exist in these environments. Additionally, the scale of Internet-based communications networks allows users to easily connect with strangers they have never met before and therefore lack a history or common friends with. Against this backdrop, it is does not come as a surprise that identity-based fraud and deception are particularly common in these environments.

One of the most common deceptive practices is “phishing,” which follows a simple scheme: a person or organisation pretends to be a trustworthy entity in order to induce a user to reveal sensitive information like usernames, passwords, or credit card details about herself. This information is then used for initiating transactions without the user’s consent, such as withdrawing money from the victim’s account or making purchases with her credit card. The damage inflicted by phishing attacks is substantial. According to a Gartner survey, $3.2 billion was lost to phishing attacks in the U.S. in 2007 with average dollar loss per incident of $886; in the 12 months ending in August 2007, 3.6 million adults lost money in phishing attacks, which is a more than 50% increase from the year before.182

Other studies show that Internet users have real difficulties in detecting phishing attempts.183 There are many different techniques currently used. Besides social engineering, i.e. the creation of plausible stories as a way to solicit responses to e-mails, a common practice includes the use of spoofed websites that imitate the online forms of their real counterparts, soliciting user to “log in with” or “confirm” their personal details. In other cases, a pop-up window opens over the actual site of, for instance, a bank and asks users to enter their details. In designing phishing e-mails, criminals tend to capitalise on the contemporary fears of consumers. For example, it has been observed that in the wake of the economic downturn late 2008 an increasing

---

182 Gartner, Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks, Dec. 17, 2007, http://www.gartner.com/it/page.jsp?id=565125 (last visited May 27, 2009). However, a Microsoft study estimated the loss from phishing attacks much lower at about $61 million per year, see Cormac Herley & Dinei Florencio, A Profitless Endeavor: Phishing as Tragedy of the Commons, NSPW’08, September 22–25, 2008, Lake Tahoe, California, USA.

A closely related and long-standing form of fraud is online identity fraud. In this case, a person uses personally identifying information like a name, address, or social security number to commit fraud under the other person’s name. The U.S. Federal Trade Commission estimates that about 9 million Americans have their identities misused each year (see also Figure 7). While phishing is one way to get hold of personally identifying information, other methods include dumpster diving, skimming, or stealing of wallets and mail. Among the most common uses of other people’s identities are credit card fraud, phone or utilities fraud, bank account fraud, government benefits fraud, or attempts to use another person’s reputation to get a job, rent a house, or evade arrest.

Figure 7: Incidents of Identity Fraud
(Source: Javelin Strategy & Research, 2009 Identity Fraud Survey Report - Preview (2009), p. 8)

As with other cybercrimes, the policy approaches to identity-based fraud differ. While user education and training are widely recognised as important measures, many countries have amended their legal frameworks to specifically include identity thieves. Private businesses like banks and retailers have invested heavily in fraud prevention, using data mining algorithms to detect irregularities and improve security.

The OECD has developed a set of policy guidelines to enhance efforts to combat identity theft.\textsuperscript{188}

### 8.3 Spam

A further issue and—in the eyes of most—the most ubiquitous annoyance on the Internet is spam. According to industry sources, unsolicited e-mail accounts for up to 80\% of all e-mail traffic.\textsuperscript{189} SpamCop counted more than 1 billion spam messages in its systems over the past 12 months, which amounts to an average of 32.1 spam messages per second.\textsuperscript{190} Spam also has substantial economic implications. While the global cost of spam has been estimated at €39 billion in 2005, analysts gauged the impact on major European economies at about €3.5 billion in Germany, €1.9 billion in the United Kingdom, and €1.4 billion in France in the same year.\textsuperscript{191} McAfee estimates that a company with 1,000 workers each earning $30 per hour will suffer $182,500 per year in lost productivity due to time and IT resources spent on unsolicited e-mail.\textsuperscript{192}

Spam is also closely connected to many other cybercrime activities. While early spam messages were mostly about pharmaceuticals, illicit software or dubious business opportunities, they are now increasingly used for distributing all kinds of malware like viruses or spyware. At the same time, people appear to be increasingly less worried about spam, making use of the filters provided by e-mail providers and becoming increasingly savvy at sorting their e-mails.\textsuperscript{193}

A number of actors have tried to address this problem. State governments have enacted legislation prohibiting the sending of bulk unsolicited e-mail. A prominent example is the CAN SPAM Act of 2003 in the U.S., which included criminal provisions, civil liability, as well as enforcement provisions enabling the FTC to sue spammers. In Europe, Article 13, Section 1 of the Privacy and Electronic Communication Directive stipulates that “[t]he use of … electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent.”\textsuperscript{194} To tackle the problem of enforcement, the European Commission has set up a Contact Network of Spam Authorities (CNSA), which is supposed to exchange best practices and cooperate on enforcement issues across


The OECD has published an Anti-Spam Toolkit, which recommends a comprehensive policy framework for addressing the problem of spam. However, despite these efforts on part of public policy, the measures have been widely criticised as unenforceable and ineffective.

In contrast to legislators and international organisations, ISPs and e-mail providers have tried to address the problem with technical solutions. These included attempts to introduce techniques to verify sender server like PTRRecord Lookup, the AOL Sender Policy Framework (SPF), Microsoft’s Caller-ID or later Sender-ID. Other measures consisted of identifying and blocking spam-sending servers, checking the sending domain, and sophisticated algorithms for content filtering both at the level of ISPs and end-users, including stand-alone and collaborative black and white lists. Other proposals included the payment of bounties to everyone who reports a spammer, the introduction of “spam postage” or “spam taxes” which would make it prohibitively costly for spammers to distribute messages in bulk, or the provision of a special “safemail” service for sensitive communications.

While punctuated interventions against spammer-friendly ISPs have eliminated some sources of spam, these measures and ideas have not so far succeeded in significantly reducing the overall number of spam messages. Increasingly, spammers have moved from central servers to so-called botnets, i.e. networks of malicious programs running on hijacked computers.

8.4 Badware

Badware is used to describe “software that fundamentally disregards a user’s choice regarding how his or her computer will be used.” The concept thus comprises many different and more specific forms of malicious software, such as “malware,” “spyware,” or “adware.” Common experiences of users with badware range from the annoying to the criminal. There are, for instance, the notorious free screensavers, which suddenly start generating advertising pop-ups on a computer screen without

---


198 For an overview, see Bambauer, supra note 197, at 15-31.


201 See, e.g., Bambauer, supra note 197, at 87-93.


203 Id.

soliciting consent first. Trojans can install themselves clandestinely, sniff around a user’s hard drive and report the results to a remote server without anyone taking note. Similarly, keylogger programmes transmit every keyboard stroke, including usernames and passwords typed when visiting a website. Viruses and worms may spread quickly from computer to computer.

The impact of badware ranges from performance loss on infected computers to more serious crimes like identity fraud based on personal data stolen through a badware attack. Computers may also be turned into a remote-controlled “zombie” machine that allows the attacker—among other things—to send out spam or phishing messages from the computer. While traditionally badware had been distributed through e-mail attachments, badware is increasingly spread through malicious code in ordinary websites that trigger automated “drive-by downloads” when a user visits the site. In other cases, badware may be bundled with legitimate software as an incentive to download.

According to CERT/CC statistics, the number of reported security incidents has increased exponentially with the uptake of the web (see Figure 8).\(^\text{205}\) While the social and economic impact of badware is hard to quantify, it is estimated that the badware industry accrues an annual value of over $2 billion. It is further estimated that about 59 million Americans currently have spyware or other malicious badware installed on their computers.

![Figure 8: Number of Security Incidents Reported to CERT/CC 1988-2003](source: Zittrain, The Future of the Internet – And How To Stop It (2008), p. 48)

A key challenge in combating badware is that it is so difficult to avoid by regular users. Badware is mostly installed and operated without the knowledge of the user. This lack of disclosure has therefore sparked a number of initiatives that try to tackle the problem in very different ways. One approach pursued by organisations like the OECD proposes a partnership among international organisations, aiming “to turn malware into a high-risk/low-return activity.”\(^\text{206}\) The challenge here is that such

\(^{205}\) Quoted in Zittrain, supra note 32, at 2011.

\(^{206}\) OECD, SHAPING POLICIES FOR THE FUTURE INTERNET ECONOMY (2008), p. 25.
collective action at the international level requires a lot of attention and expertise to be effective. It is questionable to what extent traditional law enforcement agencies are equipped with the expertise and resources necessary to counter the problem.

A different approach has been developed by Stopbadware.org, an independent non-profit organisation that has aligned a number academic institutions, technology industry leaders, and volunteers to protect Internet and computer users from the security threats caused by badware. In contrast to governmental initiatives, StopBadware tries to address the problem through close collaboration with gatekeepers. For example, it has partnered with major search engine providers like Google to issue warnings when a user visits a website that has been classified as potentially harmful. Another element of the strategy are badware alerts that label applications tested and evaluated according to StopBadware’s guidelines.²⁰⁷

8.5 Hate Speech, Child Pornography, and Other Content Considered Harmful

Freedom of speech and freedom of the press are widely recognised to be among the most important fundamental rights in modern democracies. This also applies to speech on the Internet. Article 19 of the Universal Declaration of Human Rights, for example, guarantees freedom to “receive and impart information and ideas through any media regardless of frontiers”. Similar interpretations are common for Article 10 of the European Convention of Human Rights, and a large number of national laws, such as the First Amendment of the U.S. Constitution. However, while free speech is generally protected, not all speech is equally welcome. The standards for what content should be considered harmful differ substantially across cultures and history, and their definition and enforcement is arguably one of the most contentious issues in public policy.

Among the first content-related issues to stir up debate was the distribution of child pornography over the Internet, i.e. sexual or sexualised pictures and video involving children.²⁰⁸ Often invoked and sometimes instrumentalised in public debates as the worst-case scenario of what can happen on the Internet, the extent of the phenomenon is naturally obscure. However, accounts of police operations point to the considerable scale of networks distributing child pornography. For example, in the context of “Operation Ore” it was found that a web portal called Landslide, which gave subscribers access to 300 child pornography sites, had a subscription database with the names and details of 390,000 people around the world in 1999.²⁰⁹ In a similar operation in 1998, a child pornography ring was broken up and 750,000 images seized, with more than 1,200 children involved.²¹⁰

A further category of potentially harmful content comprises representations of violent or sexual behaviour with a potentially harmful impact on certain vulnerable groups such as children. While there is no clear scientific evidence of a causal relationship between the consumption of such materials and any direct physical or psychological harm or harmful behaviour, depictions of certain forms of violence or sexuality tend to be considered as a major risk in most countries.

²⁰⁹ See Wall, supra note 208, at 113.
²¹⁰ See Wall, supra note 208, at 113.
Finally, certain forms of political speech may be considered unacceptable. This is especially true for “hate speech.” While there is controversy about the exact meaning and scope of the concept, hate speech is generally understood as speech that is intended to incite violence or prejudiced action against groups of people on the basis of race, religion, sexual orientation, gender, or ethnicity.\(^{211}\) A recent OSCE report claims that the Internet is “increasingly used to transmit hate-motivated discourse and propaganda”, a special reason for concern being that increasingly personally sensitive data is published on these sites.\(^{212}\) Rather unique in this context are regulations in some countries that have declared specific symbols or statements illegal, often out of a special national history. Under German law, for instance, the public display of symbols of the former Nazi party is equally prohibited as denying the Holocaust.

In all these cases, the key challenge is to strike a delicate balance between the fundamental value of freedom of speech and the exceptional need to protect certain groups of people from the effects of harmful content. How best to handle this process is a difficult question for which different institutions have found different answers.

Democracies and non-democracies alike have established ways of filtering content considered harmful under their respective standards. The locus of such filtering differs across countries. While many countries like the U.S. and the UK have required ISPs to effect state-mandated filtering requirements or target public access points like cyber cafés or public libraries, other countries like China have established private Internet exchange points (IXPs) or explicit state-run clearing points to serve as more direct and pervasive gatekeepers for Internet traffic.\(^{213}\) Targets differ according to the local and cultural priorities of the filtering entities and comprise a broad range of content, ranging from pornography and sex educational materials to political and activist websites and blogs of so-called “cyber-dissidents.”\(^{214}\)

The main problem with such centralised government interventions is that the classification of content as “harmful” is a highly normative and political exercise. As with all filtering approaches, there is a fine line between protection and propaganda. Motivations for filtering are often political, for example, when e-mail communications of anti-government activists are blocked in Burma or foreign news websites like the BBC site are not accessible in China. These cases may seem like clear violations from a human rights perspective, but also bring up the crucial question of what forms of filtering can be considered legitimate under a certain regime and how this is best achieved in a way that is consistent with constitutional protections of freedom of expression and democracy.

Given these problems with government interventions, some commentators have called for a response at the level of industry. Commonly discussed under the rubric of “self-regulation,” it is asked whether and to what extent ISPs, network providers, and platform operators can efficiently bind themselves and deal with the problem. As case studies of self-regulatory regimes in this area have shown these activities can also have some serious disadvantages like a negative impact on competition, failure to

\(^{211}\) See Wall, supra note 208, at 117.
ensure compliance, or a lack of clarity.\textsuperscript{215} At the same time, private corporations tend to depend on the goodwill of the authorities of the countries in which they do business.

While all these approaches have the disadvantage of establishing points of control, which may be abused or misused, a different response focuses on empowering children, parents, and other users to become more literate and protect themselves. This includes child protection controls for browsers, search engines, and major online portals, training and education at schools and the workplace, but also making transparent other parties’ attempts at filtering certain content. Non-profit organisations like the Open Net Initiative have worked for a number of years to uncover filtering on a global scale. Most recently, the organisation launched a distributed, user-driven platform called “Herdict” that aims to provide real-time information on filtering activities worldwide through the feedback of a “global civic network.”\textsuperscript{216} An interesting question here is to what extent such distributed initiatives can help users understand filtering and protect themselves without creating new gatekeepers and points of control.

\textbf{8.6 Cyberwar and Cyberterrorism}

As critical facilities like power grids, industrial control systems and traffic management systems are becoming more and more interdependent and interconnected through IP-based networks, concerns have been raised about how to best to protect these infrastructures against attacks. Especially in recent years, a number of international attacks on critical information infrastructures have been reported in different countries. While physical attacks like the 9/11 planes crashing into the towers of the World Trade Center in New York City can bring down telephone networks, energy supplies, and radio stations, the notion of “cyberwar” is commonly associated with attacks on states that are conducted through information systems on information systems. Similarly, “cyberterrorism” has recently entered the discussions, reflecting the shift in conflicts at the international level.

Among the recent cases reported in the press is a 2007 wave of distributed-denial-of-service (DDoS) attacks on Estonia’s critical information infrastructure. A DDoS attack is conducted through a large number of often hijacked computers that are directed to flood an internet server with seemingly legitimate requests, resulting in the breakdown of the server. Among the targets in Estonia were the online systems of two major banks, which were brought down for several hours. Estonian authorities suspected Russia behind the attacks and linked them to a recent political conflict between the two states, but the actual culprits could never be identified because of the distributed nature of the attacks.\textsuperscript{217}

A similar attack was launched on Georgian government websites in August 2008 in the context of a long-running conflict between Russia and Georgia. Several pro-Russian website offered software and instructions to Internet users for taking part in a DDoS attack, including lists of target websites of the government as well as the American and British embassies in the capital Tbilisi. Compared to the Estonian case, the harm inflicted in Georgia was limited, including disrupted e-mail communications

\textsuperscript{215} See, e.g., Cave & Christopher, supra note 164.
\textsuperscript{217} Id.
and unavailable websites as well as outages in telephone and emergency services, impeding operations of some critical government agencies.\textsuperscript{218} Again, the attacks could not be traced to any particular individual or organisation since potentially any Internet user could have taken part by downloading and running the respective software.

These two recent cases illustrate some of the difficulties in dealing with “cyberwar” attacks. A key challenge is to find out whether an attack is in fact a military matter or the isolated action of a group of malicious hackers. Since the initiators of attacks can rarely be identified, it has been questioned to what extent it is in fact fair to talk of “war,” leading some commentators to speak of a “fog of cyberwar.”\textsuperscript{219} Such questions are not just semantics since international treaties and military alliances like NATO foresee obligations to step in and defend a member of the alliance in case it is “attacked.” The question is therefore to what extent “cyberwar” attacks qualify as “attacks” in the sense of the treaty, triggering the mechanisms of collective defense.

Another key challenge is how to best protect critical information infrastructure against decentralised intrusions. Despite different classifications and definitions, security experts commonly identify four elements: prevention, detection, response and recovery.\textsuperscript{220} The question of how these steps should be operationalised has provoked different approaches. The U.S., for example, have largely adopted a military strategy. One element of this is the creation of new “cybersecurity czar” and “national cybersecurity advisor,” who would have powers to shut down federal networks if they are found to be vulnerable. In addition, U.S. government spending on secure computer networks is expected to rise from $7.4 billion in 2008 to $10.7 billion in 2013.\textsuperscript{221}

NATO has established a Cooperative Cyber Defense Center of Excellence, a think tank tasked with monitoring and analyzing emerging cybersecurity threats.\textsuperscript{222} Estonia has shifted responsibility for “cyberwar” issues from the Department of Defense to the Department of Economic Affairs and Communications. The goal here is to educate citizens, improve the security of selected applications like online banking, and train experts in specialised programs. A key target is to increase the security of individual home computers to prevent them from being hijacked in a DDoS attack.\textsuperscript{223} Other approaches propose a system of insurance to incentivise private investments in cybersecurity while avoiding the inertia of government regulation.\textsuperscript{224}

\textsuperscript{218} See Economist, \textit{Marching Off to Cyberwar}, Dec. 4, 2008.
\textsuperscript{222} See Cooperative Cyber Defense Center of Excellence Website, \url{http://www.ccdcoe.org/} (last visited May 27, 2009).
\textsuperscript{223} See Morozov, supra note 221.
\textsuperscript{224} See Cukier et al., supra note 220, at 5.
9. Economic Impacts: How Big Is the Internet Pie?

How does the Internet affect the performance of the economy and the standard of living of citizens? What are the implications for job markets and employment? What is the role of digitally networked information technologies in fostering productivity, growth, and innovation? While it is virtually impossible to attribute economic transformations to specific technologies, the following data can provide at least a rough indication of the economic implications of networked computing.

9.1 Impacts on GDP

ICT investments have contributed significantly to GDP growth worldwide: over the past decade, the contribution of ICT investments to GDP growth has generally increased (see Figure 9).

![Figure 9: Contributions of ICT Investments to GDP Growth](Source: OECD Productivity Database, September 2005)

A recent study set out to estimate the direct economic value of services provided by the Internet to the U.S. economy. Modelling the Internet as an independent economic unit that exchanges value with the rest of the economy, the study concludes that a net economic value of $175 billion is “exported” from the Internet. According to the authors, this includes $20 billion of advertising services, $85 billion in retail transactions conducted over the Internet, and $70 billion of direct payments to Internet Service Providers. In addition, there is substantial indirect value created through economic activities elsewhere that takes place because of the Internet sector.

9.2 Impact on Productivity and Modernisation

Internet-related technologies are also generally assumed to play an important role for improving productivity. According to the European Commission, ICT was responsible for 50% of overall productivity growth in the EU economy for the ten

---

years up to 2004, while the ICT industry itself drove 20% of the total productivity increase across the economy. Internet retailers, for example, are said to have between 3 and 4 times the labour productivity as brick-and-mortar retailers selling the same type of merchandise.

The impact of ICT on productivity is assumed to work through one of three channels: the ICT-producing sector, ICT investment in ICT-using sectors, and complementary factors, such as organisational capital, firm organisation, skills and human capital. In contrast to these estimates, other studies take a more conservative stance. The European e-Business Report 2008, for instance, diagnoses a so-called “productivity paradox:” while micro-level data shows that ICT are pervasively used in companies, it is difficult to trace this development in macro-level data.

As Figure 10 shows, trade in ICT goods was substantial in 2007. Also in the EU, ICTs are generally seen as a major driver of economic and social modernisation: EU businesses devote 20% of investments to ICTs today.

![Figure 10: Trade in ICT Goods 2007](Source: OECD ICT Outlook 2008)

This trend has not only affected technology-based businesses, but also more traditional industries like the chemical, steel, and furniture sectors as well as a variety of business functions, ranging from sourcing and procurement to logistics and distribution to marketing, sales, and customer service (see Figure 11).

229 Hamilton Consultants Inc. et al., *supra* note 225, at 6.
Figure 11: Relevance of ICT and e-Business for Various Business Functions  
(Source: European e-Business Report 2008, p. 13)

Besides such impacts on more or less traditional industries, ICTs have enabled a whole new range of Internet-based businesses that are primarily built on monetising the attention of users. Sometimes called the “advertising-supported Internet”, this industry comprises all activities on the web intended to promote marketplace exchange of products, services, or information. Consequently, advertising has emerged as an increasingly important funding source for online businesses over the past ten years. A recent study distinguishes 14 different segments of Internet businesses: Internet Service Providers and transport, hardware providers, IT consulting, software companies, web hosting and content management companies, search engines and portals, content sites, software as service, advertising agencies and support services, advertising networks, e-mail marketing and support, enterprise staff and subcontractors, e-commerce services, and B2B e-commerce (see Figure 12).

<table>
<thead>
<tr>
<th>Company</th>
<th>2007 Internet Revs. (Shillions)</th>
<th>2007 U.S. Internet Employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Internet service providers (ISPs) and transport</td>
<td>73.31</td>
<td>181,233</td>
</tr>
<tr>
<td>2. Hardware providers</td>
<td>64.41</td>
<td>65,591</td>
</tr>
<tr>
<td>3. IT consulting and solutions companies</td>
<td>8.15</td>
<td>32,155</td>
</tr>
<tr>
<td>4. Software companies</td>
<td>15.72</td>
<td>27,192</td>
</tr>
<tr>
<td>5. Web hosting and content management companies</td>
<td>5.85</td>
<td>52,835</td>
</tr>
<tr>
<td>6. Search engines/portals</td>
<td>33.84</td>
<td>48,025</td>
</tr>
<tr>
<td>7. Content sites</td>
<td>6.0</td>
<td>59,901</td>
</tr>
<tr>
<td>8. Software as a Service (SaaS)</td>
<td>7.70</td>
<td>31,487</td>
</tr>
<tr>
<td>9. Ad agencies and support services</td>
<td>10.64</td>
<td>29,407</td>
</tr>
<tr>
<td>10. Ad networks</td>
<td>1.19</td>
<td>1,533</td>
</tr>
<tr>
<td>11. E-mail marketing and support**</td>
<td>1.02</td>
<td>10,278</td>
</tr>
<tr>
<td>12. Enterprise staffs and subcontractors responsible for Internet advertising, marketing and web design</td>
<td>15.00</td>
<td>100,000</td>
</tr>
<tr>
<td>13. E-commerce co., including physical delivery</td>
<td>202.78</td>
<td>508,391</td>
</tr>
<tr>
<td>14. B2B e-commerce</td>
<td>1,350.00</td>
<td>44,233</td>
</tr>
</tbody>
</table>

Figure 12: Economic Value of 14 Internet Segments in 2007  
(Source: IAB 2009)

9.3 Impacts on Employment and Labour Markets

The Internet has had a significant impact on employment and job opportunities. A recent study in the U.S. context found that “the Internet employs 1.2 million people directly in jobs that build or maintain the infrastructure, facilitate its use, or conduct advertising and commerce on that infrastructure.” Assuming that every Internet job

---

233 Hamilton Consultants Inc. et al., supra note 225.  
234 Hamilton Consultants Inc. et al., supra note 225, at 5.  
235 Hamilton Consultants Inc. et al., supra note 225, at 4.
supports an additional 1.54 jobs in other parts of the economy, it is further assumed that 3.05 million Americans owe their jobs to the advertising-supported Internet—that amounts to roughly 2% of all employed Americans.\(^{236}\)

This increase can be traced to a number of factors. One is arguably a push for entrepreneurship enabled by the comparatively low barriers to starting a business in networked computing. A recent study estimated that at least 10% of “Internet workers” are based in firms with less than 10 employees—some 20,000 small businesses operate on the Internet, 120,000 people are primarily employed as eBay sellers and 500,000 have part-time businesses on eBay.\(^{237}\) While many of these operations have stayed small, a few developed into major corporations like Google, Amazon, Cisco, or Symantec.

In addition to such entrepreneurial endeavours, ICTs also contributed to the creation of new forms and patterns of work in more traditional jobs such as telecommuting or home office arrangements. The have also affected the way people search and apply for jobs. Over 14% of Internet users in the OECD, on average, have used the Internet for finding a job, rising to 20% in Finland, Denmark and Norway (see Figure 13).

![Figure 13: Percentage of Adults Who Used the Internet for Job Search in 2007](source: OECD, The Future of the Internet Economy: A Statistical Profile (2008), p. 14)

### 9.4 Impacts on Consumption and Individual Uses

The Internet has also had significant impacts on consumption and individual uses. Online shopping has increased steadily. 32% of individuals aged 16-74 in the EU27 bought or ordered goods or services for private use over the Internet at least once in 2008.\(^{238}\) That is an increase from 20% in 2004, 26% in 2006 and 30% in 2007. Most active online shoppers can be found in the age group 25-34, where 47% of individuals qualify.\(^{239}\) Around 30% of individuals aged 16-74 used Internet banking, interacted

---

\(^{236}\) Hamilton Consultants Inc. et al., *supra* note 225, at 4.

\(^{237}\) Hamilton Consultants Inc. et al., *supra* note 225, at 6.


\(^{239}\) *Id.*
with public authorities or searched for health-related information in the second quarter of 2008; nearly a third of these individuals used the Internet for travel and accommodation services, and about a quarter read online news.\footnote{Id.}

As far as communication is concerned, on average 57\% of adult users in OECD countries used the Internet to send e-mail or make a phone call in 2007 (see Figure 14). While VOIP use is still relatively low, it is growing quickly with the uptake of broadband. For example, the number of registered Skype users increased by over 50 times between 2004 and 2007 to reach 276 million worldwide.\footnote{OECD, THE FUTURE OF THE INTERNET ECONOMY: A STATISTICAL PROFILE (2008), p. 13 [hereinafter Future Internet].}

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{individual_internet_use_for_communication.png}
\caption{Figure 14: Individual Internet Use for Communication (Source: OECD, The Future of the Internet Economy: A Statistical Profile (2008), p. 13) }
\end{figure}

Further, one out of four adults downloaded music or played games on the Internet in OECD countries in 2007 (see Figure 15). On average, 17\% of European Internet users in the EU15 used peer-to-peer file-sharing technologies in 2007 to exchange music, movies and other information goods; with over 35\%, the percentage is about twice as high as the European average in Spain.\footnote{OECD, FUTURE INTERNET, supra note 241, at 15.}
9.5 Impacts on the Organisation of Enterprises

Enterprises have made increasing use of Internet-related technologies. 93% of enterprises of ten or more persons employed in the EU27 had Internet access in January 2008; 81% had a broadband Internet connection. On average, 64% of enterprises in EU27 had a website in January 2008 with online presence being highest in the Netherlands and Finland with almost 100% penetration and lowest in Romania, Lithuania and Poland with less than 60% penetration. Only about 1 in 4 enterprises have Internet access via mobile connections (see Figure 16).

Figure 16: Internet Connectivity in EU27, 2007-2008 (%)  
(Source: Eurostat, Data in Focus 48/2008, p. 1)

---


244 Id.
About 68% of enterprises used Internet for interacting with public authorities in 2007, such as obtaining and submitting forms or obtaining information (see Figure 17).

Figure 17: Enterprise interaction with public authorities by purpose in 2007 (%)  
(Source: Eurostat, Data in Focus 48/2008, p. 2)

Further, 40% of all enterprises engaged in a form of automated exchange of standardised data with other entities.

9.6 EU Policy Initiatives

The European Commission has fostered these developments with its i2010 strategy, an EU policy framework introduced in June 2005. The aim of the initiative is to establish a single European information space in the sense of a single market for the digital economy, strengthen innovation and investment in ICT research, promote inclusion, public services, and quality of life.246 Currently, research and innovation are at the top of the EU agenda for economic reform: EU spends only half as much as the U.S. on ICT research and development and tends to specialise in sub-sectors of the ICT industry with low research intensity. This gap between the EU and its competitors is regarded a problem for innovation and future competitiveness and is being countered with a number of measures, including the emphasis on ICTs in the seventh research framework programme, the pioneering of public-private partnerships, or the targeted support of so-called “lead markets” with appropriate policy actions.247

9.7 Economic Costs of Networked Computing

Besides its unquestionable benefits, the Internet also causes costs for the economy. One example are the losses suffered as a consequence of criminal activities.248 Generally, data on the economic impacts of cybercrime are difficult to collect—partly because much of the activity takes place out of public view, partly because companies and organisations do not want to reveal the true losses they suffer. For example, while there is only little data available on the economic impact of malware, an association of banks in the UK estimated the direct losses caused by malware to its member organisations to be at £ 12.2 million in 2004, £ 23.2 million in 2005, and £ 33.5

248 See Section 8 for a more detailed discussion of cybercrime.
million in 2006, an increase of 90% from 2004 and 44% from 2005.\textsuperscript{249} Also the cost to individual consumers is likely to be significant. In the U.S., for example, consumers paid as much $7.8 billion over two years to repair or replace information systems infected with viruses and spyware.\textsuperscript{250}

\begin{itemize}
\item\textsuperscript{249} OECD, \textit{A Threat to the Internet Economy, Computer Viruses and Other Malicious Software} (2009), p. 68.
\end{itemize}
10. Social Implications: The Individual and Society

Besides the economic implications sketched above, digitally networked environments also have profound social implications. New forms of communication and interaction transform and challenge the daily routines and habits of millions of people. Documents that took days to be delivered are now crossing large distances at a split second. A wealth of information is created to support or subvert individual decision making. And new forms of mediated communication like social networking sites challenge common understandings of what “friendship” is and how we present ourselves to others.

While diagnoses of “revolutionary” change and “fundamental” transformations are popular among contemporary analysts, it is important to notice that the social implications of technologies are usually too complex, messy and contingent to be easily singled out. The reason is that both “technology” and “the social” are in a dynamic relationship and consequently co-evolve. While some uses like microblogging have reached critical mass and taken off rather unexpectedly, others have been carried by high hopes and resulted in disappointments. For example, while many had predicted significant reductions in travel because of increased use of teleconferencing technologies, researchers have not found any noticeable decrease in travel – in some cases, just the opposite.\(^\text{251}\) Hence, we have to be careful to understand the role of networked computing in everyday life and to avoid singling out isolated “impacts.”

10.1 Scope of Internet Use Today

Today, the Internet has found its way into the everyday lives of people around the world and is becoming increasingly embedded in a variety of socio-technical networks. As Figure 18 illustrates, the Internet has implications for how hundreds of millions of people around the world claim to make decisions. In the U.S., for example, 45% of Internet users say that they used the Internet for a significant decision over the last two years, while 17 million resorted to the Internet to help someone with a major illness and 21 million used it for career training.

The Internet now impacts everyday life for hundreds of millions

Figure 18: Impact of the Internet on Everyday Life

The increasing importance of the Internet for all kinds of decision-making is also reflected in the information-seeking behaviour of users. In the UK, the Internet has become a key medium for seeking information of all kinds. In 2007, 47% of respondents to a nationwide survey said that they would go to the Internet first if they were looking for a book, 54% if they were planning a trip, 40% if they were looking for information about a local school, and 39% if they were looking for information on taxes.252 Users rate the Internet as an important source for gathering information just after talking to other people, ahead of television, radio or newspapers. In addition, the Internet is playing an increasingly important role in work environments, allowing new forms of teleworking and collaboration across distances.253

---

253 See Section 13 for further details.
Especially, but not exclusively, among younger users, social networking sites have become integral parts of individuals’ communication environments. While general-purpose social networking sites like MySpace, Facebook, or StudiVZ allow users to create a personal profile and publicly display their connections with others, content-based platforms like YouTube or Flickr provide spaces for users to share videos or photos with a broader audience. Other forms of social networking sites include business-oriented networks like LinkedIn or Xing and networks for children like Club Penguin and Barbiegirls. In addition, micro-blogging sites like Twitter or virtual environments like Second Life or Habbo Hotel are sometimes included in the definition.

The European Commission has noted a massive increase in the popularity and use of these platforms. According to a study, more than 56% of the European online population visited social networking sites in 2007; from 2007 to 2008, there was a 35% increase in visits to European social networking sites.\(^{254}\) What all these services have in common is that they allow users to connect and interact through digital representations of each other, share information and creative works like music and video at comparatively low costs, and stay informed about trends in business, culture, and their local neighbourhoods. With the recent advent of mobile technologies, it is often argued that many of these phenomena will further intensify and become even more pervasive.

10.2 Digital Divide and Inequality

While there have been worries over the last decade of a “digital divide” between Internet users and non-users, more recent discussion has focused on notions of “digital inequality” to analyse the social implications of differential access to

---

Traditionally, concerns about a “digital divide” and “digital inequality” have consisted of two mutually reinforcing arguments. In a first analytic step, it is suggested that differences among people like socio-economic status, gender, or age lead to different uses of digital media, often only specified in terms of the most extreme cases “use” and “non-use.” In a second step, it is assumed that these differences lead to social inequalities in terms of access to information and resources. In as far as these resulting inequalities affect characteristics like socio-economic status, this perspective usually results in the assumption of a self-reinforcing feedback loop, further exacerbating existing social and economic inequalities.

Many studies attempt to understand the digital divide on a global scale. An example can be found in Figure 20, which illustrates a considerable gap between Internet use in “developed” vs. “developing” countries.

![Internet users per 100 inhabitants 1997-2007 (Source: ITU)](source)

Figure 20: Internet Users per 100 Inhabitants 1997-2007 (Source: ITU)

However, other studies have looked at differential Internet access and use to demonstrate inequalities among different segments of the population with particular attention to education, rural residence, race, gender, age, or income. Recent studies show that use and non-use of the Internet are shaped by a variety of factors. Besides access to socio-economic resources, it has been found that there are significant differences in Internet use between students, employed, and retired people as well as

---


gender, age, income, and ability gaps. Other scholars have pointed out that a binary classification of people into users and non-users may not be sufficient to understand the problem and proposed more differentiated perspectives, for example, by focusing on different levels of media skills.

In the same vein, it has been noted that many of the gaps may not be as clear-cut as they are sometimes portrayed and that the interplay of many variables needs to be taken into account. For example, with regard to the age gap, it has been argued that factors like gender, education and socio–economic status still play an important role for Internet use; while the diffusion rate among the elderly will continue to lag behind that among young people, the elderly could also make use of latecomer advantages with matured technologies.

More generally, whether and under what conditions these inequalities actually exacerbate or mitigate further inequalities has been contested among policymakers and academics. While some argue that digital exclusion will deepen existing differences in access to social and economic resources, others suggest that the more ubiquitous the Internet becomes, the more it will help closing the existing gaps by offering new forms of engagement. Overall, it is therefore still an open question what exactly the role of the Internet will be in overcoming or reproducing inequalities.

10.3 Digital Self and Community

A further set of issues revolves around questions of self, identity and community. While these concepts may seem rather abstract and elusive, they point to the possibility of some fundamental transformations of how we conceive of ourselves, form identities as well as build and maintain relationships, networks and organisations.

It has been argued that individuals face an Internet identity paradox. On the one hand, it is assumed that in digitally networked environments individuals have a rich set of controls that let them design or “stage” different identities in different contexts. Usually, people need to create some form of representation of themselves in order to appear as someone or something with a certain identity. This may be something as trivial as a username, e-mail address, or signed comment on a message board or a graphical avatar or a full-scale personal profile on a social networking site. On the other hand, once these representations are “inscribed” as data, they can travel across contexts and evade the control of the individual. While this tension raises obvious concerns over privacy and informational self-determination, it also points to potential implications for how users manage their selves and identities in digitally networked environments. For example, it has been noted that “impression management” or “reputation” plays an increasingly important role in socio-technical networks.

257 Dutton & Helsper, supra note 252, at 11.
Closely related are questions about what kinds of imagined audiences users operate with and how these audiences affect their decisions to disclose or hide certain information. Another aspect of computer-mediated communication is the increasingly blurred boundary between public and private spheres. Conventionally, many aspects of our social life had relied on a more or less clear-cut separation of these two realms. This applies to the definition of “personal data” but also more broadly to distinctions between public and private law. However, with interactions moving from face-to-face encounters to computer-mediated exchanges, it is increasingly difficult to separate these spheres. Against this backdrop, it can be asked whether increased fragmentation of communication and identity should lead to a lack of awareness of self or a breakdown of individual identity, purpose and self-worth. Is everyone potentially an Internet celebrity? Does everyone wish to be, and why? What are the consequences of this for our understanding of identity and audience?

Any change in the digital self is inevitably connected to changes in social relationships. It has been asked, for instance, whether there is a difference between real and virtual “friends” and how the meaning of “friendship” changes on social networking sites. The same can be said for a variety of other relationships at work, in the family, or among friends. Other researchers have claimed the rise of so-called “networked individualism.” The idea is that in a personalised and wireless world people increasingly switch between ties and networks: “People remain connected, but as individuals rather than being rooted in the home bases of work unit and household. Individuals switch rapidly between their social networks. Each person separately operates his networks to obtain information, collaboration, orders, support, sociability, and a sense of belonging.”

10.4 Implications for Families

Such developments also challenge existing institutions, most importantly the family as a fundamental social unit. It has been argued that ICTs have played an important role in shaping the structure of the family itself, relationships between family members, work-life relationships and entertainments. A key question here is whether an ICT-based culture strengthens or weakens the family unit.

On the one hand, ICTs may lead to a more private and separated everyday life within families. For example, children in wealthier families may have their own Internet-connected computers in their rooms and consequently spend less time with other family members, given that computers are still mostly designed for single users and increasingly offer personalised services. A rare exception is the phenomenon of jointly created and maintained family websites. In addition, if devices for Internet access are becoming increasingly mobile, family members may pursue their activities

outside the home. On the other hand, it has been argued that increased Internet use in families reduces time spent viewing TV, talking on the telephone, or reading a newspaper. However, it is not clear whether this in fact represents a significant shift with regard to family life.

Further, the widespread use of mobile phones may facilitate communication within the family and foster cohesion and security. For example, in a survey of 4,500 families with Internet access across 16 countries worldwide, more than half of respondents aged 18 to 34 said that technology is not just helpful, but necessary to stay in touch with family. At the same time, it has been reported that especially children may perceive such increased connectivity as an invasion of privacy if parents use the technology for greater control and surveillance. Another aspect concerns the use of the Internet in family-related contexts. For example, it has been argued that the Internet may represent a promising opportunity for fostering family–school communication for the benefit of the children. A special case are families that have been geographically divided because some family members migrated to another country. The Internet provides an affordable medium for staying in touch, exchanging photos and experiences, chatting, e-mailing, and video-conferencing across long distances. It has also been suggested that digitally networked technologies may enable new forms of telemedicine, which would allow families to care for their elderly members at home.

Thus, as already these few observations indicate, existing studies paint a highly complex picture of the implications of the Internet for the family. It is widely agreed that there are no easy answers and that more research is needed. This includes understanding how, by whom, and for what purpose digitally networked technologies are actually used inside and outside the family home, and how these new forms of interaction relate to existing ones. In addition, it would be interesting to understand how these implications and dynamics differ across social, economic and cultural backgrounds.

10.5 Political and Civic Engagement

Particularly in the US and Europe, the Internet has had a strong impact on political and civic engagement. In the UK, for example, Internet users have been found to be more active socially than non-users. In 2007, a survey showed that 28% of users attended meetings while only 22% of non-users did. 9% of Internet users have

---


272 See Forge & Blackman, supra note 265, at 44-55.

undertaken at least one civic action on the Internet, compared to 36% of users who have done this offline (see Figure 21).

![Figure 21: Number of Civic Activities Undertaken Online and Offline (Source: OxIS 2007)](image)

These observations have given rise to the idea of a networked public sphere. As Yochai Benkler writes, this new form of a public sphere “will have no obvious points of control or exertion of influence—either by fiat or by purchase [and] promises to offer a platform for engaged citizens to cooperate and provide observations and opinions, and to serve as a watchdog over society on a peer-production model”.\(^{274}\)

While such new communicative spaces tend to be received rather enthusiastically, there have also been more critical views on this development. For example, it has been argued that greater choice of media may lead to polarisation and group think instead of diversity and deliberation.\(^{275}\) Power law distributions may lead to concentration of attention on a few websites rather than a truly diverse information environment.\(^{276}\) Others have pointed to tension between traditional political structures and processes and the new Internet-enabled forms of widespread political participation and how the former may maintain dominance over the latter for the moment.\(^{277}\)

**10.6 Negative Implications and Dangers**

From a public policy perspective, it further seems appropriate to draw special attention to a selected number of potentially negative consequences of digitally

---

\(^{274}\) Benkler, *supra* note 86, p. 177.


networked technologies. While qualifying consequences as “negative” usually involves substantial value judgments and thus depends on the worldview and individual preferences of the analyst, a number of issues have been repeatedly discussed.

One prominent example is the concern over addiction to certain forms of media consumption like online gaming or pornography, which is sometimes said to become more common with the spread of networked computing. Yet, while it is sometimes feared that increasing use of networked computing may alienate users from each other, it is virtually impossible to find conclusive evidence for that claim. Also the effects of increased media use on children have gained considerable attention. While some studies claim that there is no causal link between violence in computer games and aggression in real life, others have suggested that video game violence is a risk factor for aggressive behaviour.

Further, the proliferation of increasingly immersive virtual environments poses a number of social and ethical challenges. Besides the already mentioned issues of privacy and security and their implications for personal development and identity, there is likely to be an increasing need to bridge people’s experiences of the real and the virtual and ease transitions between the two. While distractions through networked devices while driving a car have long been on the agenda of regulators, new virtual reality applications may increasingly challenge our ability to manage coexisting and potentially conflicting realities.

Finally, instant information access and the always-on environment we live in can create an illusion of control. For instance, a teenager may feel confident and knowledgeable about a subject, such as sex, by simply doing a Google search; people may feel like they know each other even though they have never met and many of the subtle cues of human interaction are missing. Essentially, the Internet may foster the illusion of being factually accurate, but it may not always be – for instance, playing what seems to be a physically active game online does not mean that an individual’s own body is getting exercise. Someone on the Internet is not necessarily who they claim.

---


281 See Ralph Schroeder, Malte Ziewitz & Eric Meyer, Social, Legal, and Ethical Implications of Presence Technologies, Peach FP6 Coordination Action No 33909, May 2009.

11.1 Electronic Government and Citizen Participation

While modern bureaucracies have always depended on technologies of representation and communication, the Internet has the potential to transform the relationship between citizens and governments.

Initially, the term “electronic government” has been used to describe the online provision of public services. Following the example of “electronic commerce”, the main focus of many governments in the late 1990s was on translating offline procedures and interactions into online ones, substituting paper trails and face-to-face meetings with online forms and web-based interfaces. A key concern of most consulting and benchmarking studies at that time was with creating web presences for government agencies, through which citizens could communicate with public servants, fill in forms electronically and apply for building permits online from their living rooms. The transformation of the public sector was depicted in a number of stages, driven by a technological interface between citizens and government. In other words, the initial view of “electronic government” was largely transaction-based, focusing on transposing administrative procedures into online settings via web-based interfaces.

Examples of such initiatives can be found all over the world. While Singapore integrated its public services into a web portal, the U.S. post office tasked a private company with developing a one-stop website for people moving home. According to a recent study, over 30% of citizens in OECD countries used the Internet for interacting with public authorities in 2007 (see Figure 22). For example, online tax declaration have increased dramatically such as in France, where the number of electronically submitted tax declarations has increased from about 500,000 in 2003 to more than 5 million in 2006. About 43% of EU15 enterprises returned forms to public authorities via the Internet in 2007. Electronic government of this kind is assumed to lower the cost of citizen-government interactions and contribute to economic competitiveness. As a consequences of these early transaction-based approaches, the main challenges lay in motivating citizens to actually use the new service and addressing the resulting inequities following from the digital divide between routine computer users and the digitally illiterate.

---

282 See, e.g., Irina Netchaeva, E-Government and E-Democracy, 64 THE INTERNATIONAL JOURNAL FOR COMMUNICATION STUDIES 467 (2002);
285 OECD, FUTURE INTERNET, supra note 241, p. 18.
286 Id.
287 Id.
In contrast to this rather narrow, transaction-based approach, it has been suggested to draw the circle much wider and include more generally the use of information and communication technologies in the public sector. In this tradition, electronic government is regarded as the logical extension of other technologies of representation and information processing that characterise bureaucratic organisations. Digitally networked information technologies allow new forms of public administration. Electronic government is therefore regarded as a way to improve government more generally and realise efficiency gains not just in citizen-government relations, but also within government. As such, it is closely related to new forms of public management and the goal of achieving public policy objectives in a fair and cost-efficient way. The analytic focus consequently shifts to institutional structures and change or the role of hierarchies. An recent example of this more comprehensive approach is the work on “Digital Era Governance” by Patrick Dunleavy et al. A central idea here is that government needs to reclaim the long-outsourced expertise in IT matters by “reintegrating functions into the governmental

---

290 See, e.g., Davy Janssen, Sabine Rothtier & Kris Snijkers, If You Measure It They Will Score: An Assessment of International eGovernment Benchmarking, 9 INFORMATION POLITY 124–125 (2004); Mayer-Schoenberger & Lazer, supra note 284, at 4
sphere, adopting holistic and needs-oriented structures, and progressing digitalisation of administrative processes.”

A final approach adopts an even broader view and looks at the role of the Internet in democratic processes of deliberation and representation more generally. The focus here is neither on technical citizen-government transactions nor the internal organisation of government itself, but the processes of participation and deliberation in the “networked public sphere” that characterises democracies in the information age. While the state is still the main point of reference, the emphasis shifts to citizen involvement in policy-making and more generally civic engagement with issues of public concern. Major questions here are, for example, how digitally networked technologies can be used to improve citizen participation in government and policymaking or how new technologies may deepen or overcome existing biases and divides in public policy. This approach to electronic government has gained currency over the past five years with the advent of web 2.0 applications and attempts to make them useful for the public sector.

A case in point is the British non-profit organisation mySociety, which builds “websites that give people simple, tangible benefits in the civic and community aspects of their lives.” A few examples from their portfolio illustrates the range of projects that are currently being developed:

- **WriteToThem.com**: Launched in 2001 under the name of “FaxYourMP,” this website allows UK citizens to find their representatives at the local, regional, national, and European level via a postcode search and send them private messages online. With about 100,000 users and 180,000 messages counted in 2008, about two thirds of all requests receive a reply.

- **TheyWorkForYou.com**: Visited about 2 million times in 2007, TheyWorkForYou.com provides users with a range of information about their politicians. Among other things, citizens can find out who their Members of Parliament (MP) are, how they have voted, what they said in parliament, what written questions they submitted to government departments and what answers they got back, and what other users said or commented on regarding a specific MP. In addition, users can sign up for e-mail alerts when a specific MP speaks in parliament or watch video of an MP’s speeches.

- **FixMyStreet.com**: The website was launched in February 2007 and is supposed “to help people report, view, or discuss local problems they’ve

---

294 See Benkler, supra note 86, at 212 ff.
295 See, e.g., Kevin Esterling, Michael Neblo & David Lazer, Home (Page) Style: Determinates of the Quality of House Members’ Websites, 1 INTERNATIONAL JOURNAL OF ELECTRONIC GOVERNMENT RESEARCH 50–63 (2005); Victor Bekkers, E-Government and the Emergence of Virtual Organizations in the Public Sector, 8 INFORMATION POLICY 89, 90 (2003).
found to their local council by simply locating them on a map.” Issues like graffiti, unlit lampposts, abandoned beds, or broken glass on a cycle path are reported to the responsible council via e-mail and may be solved by officials or groups of local volunteers who take matters in their own hands.

Similar web-based projects aimed at fostering transparency and accountability of government vis-à-vis civil society are currently emerging in many other European countries. Overall, it seems fair to assume that these examples indicate a new trend in “electronic government.” The Internet has adopted a role far beyond the initial transaction-based and institutional approaches and enabled new forms of citizen participation and interaction that partially bypass the established procedural and organisational structures of democratic. Consequently, it has been argued that these phenomena are more adequately described as a new form of “information government.”

11.2 Education and Technologically-enhanced Learning

What started out as “e-learning” and later became “technology-enhanced learning” is largely based on the idea that digitally networked technologies can improve the ways in which we learn and study. Examples range from the use of PCs, data projectors and interactive whiteboards in classrooms to web-based distance-learning programs, large-scale virtual learning environments, and the use of mobile phones in teacher-student interactions. While the focus of these discussions is mostly on learning in schools and higher education, the field could be drawn much wider, including institutions for lifelong learning or Internet-based training programs in companies.

Recent OECD statistics indicate a broad uptake of new information technologies in education sectors across Europe. For example, in 2006, more than 20% of Internet users used the Internet for formalised educational activities in the UK, Turkey, Greece, Hungary and the Netherlands; in Finland it was more than 30%. Broadband access has increased significantly in primary and secondary schools (see Figure 23). And in most OECD countries, over 25% of enterprises use e-learning applications for training their employees.

---

300 See, e.g., the project Abgeordnetenwatch in Germany, http://www.abgeordnetenwatch.de/ (last visited July 31, 2009).
302 OECD, FUTURE INTERNET, supra note 241, at 17.
While the beginning of Internet-based e-learning applications was characterised by a general enthusiasm for large-scale information systems and integrated virtual learning environments, educators and practitioners currently refocus the debate towards more fundamental questions about the role and purpose of technology in different forms of learning. A review of the available literature and discussions yields four major themes that are likely to shape the future of education in relation to the Internet:

- A key lever for any educational policy are school curricula. The main question here is what pupils should learn in the future to be prepared for an increasingly digitally networked work and life environment. Attempts to increase “digital literacy” or improve technical and media skills can be seen in this context. The same is true for initiatives to foster “creativity” among students.

- There is a widespread concern with new forms of distributed intelligence. Educators increasingly wonder what difference it makes when people work as “networked individuals”, i.e. as parts of networks and teams, instead of all on their own. Should, for instance, performance be assessed on a team basis rather an individual basis?

- Educators have discussed various topics around spaces of learning. They are beginning to experiment with different teaching models, trying to integrate technology in everyday educational practices beyond installing “computer

---

303 The UK’s “Schools for the Future” program is a good example, see Teachernet, Schools for the Future, http://www.teachernet.gov.uk/management/resourcesfinanceandbuilding/schoolbuildings/innovativedesign/sbschoolsforthefuture/ (last visited July 31, 2009).
labs.” For example, it is still far from clear to which uses mobile devices can be put, what the implications of laptop use in lectures and classes are, and to what extent activities outside school could be integrated into the curriculum through digitally networked technologies.\(^\text{304}\)

- Finally, education experts increasingly attend to matters of **personalisation**. While the concept is used rather vaguely, it has featured prominently in recent debates. The idea here is to join up lots of information about the student and use the existing data to support and control learning.

As these issues show, it is impossible to discuss the potential of technology-enhanced learning with an exclusive focus on technology or information systems. As in many other areas, the possibilities opened up by the Internet challenge us to revisit many of the defining, yet unanswered questions of the field—or in this case: what is education for? It seems that too many initiatives have started out without laying out a clear idea of what can reasonably be achieved to what ends. In one way or the other, the field of education will be a key issue not just for those immediately affected, but also for European society and a competitive economy more generally.

**11.3 e-Health, Patient Records, and Telemedicine**

At the core of most eHealth initiatives is the idea of systematically gathering and storing electronic patient records with up-to-date historical health information about an identifiable patient and making these available to authorised individuals via dedicated health information networks.\(^\text{305}\) Such records are thought to improve the informational basis on which physicians make decisions, increase patient safety, save costs and allow for easy and timely access to a person’s medical history. Also other healthcare professionals like pharmacists or insurance companies are likely to have an interest in accessing individualised health information to make their services more efficient and target specific customers. In addition, electronic patient records may provide a valuable and cost-efficient resource for researchers, who could extract large-scale data sets from them without having to conduct expensive surveys or studies themselves. Yet, while patient records are already kept in most countries (e.g. in the UK by the National Health Service (NHS)), the idea here is to go one step further and make the decentralised patient records accessible via dedicated electronic health networks.

From a technical point of view, this requires most basically making the existing information systems deployed by general practitioners, hospitals, pharmacies and insurance companies interoperable. As far as primary care is concerned, a recent survey of general practitioners across the EU27 in 2007 showed that over 87% are using computers while 70% use the Internet with still only about half of all practices connected through broadband.\(^\text{306}\) The idea here is not only to connect these primary healthcare providers so that they can easily access critical health information about specific patients, but also to include secondary healthcare providers like hospitals and

\(304\) See the University of Nottingham’s project on mobile learning as an example, [http://www.nottingham.ac.uk/splint/mlearning/index.php](http://www.nottingham.ac.uk/splint/mlearning/index.php) (last visited July 31, 2009).


related actors like insurance companies, health authorities or even pharmacies. Often these systems include functionality for electronic prescriptions.

While the medical and economic benefits of such integrated health information systems may be substantial, the usual public policy concerns associated with large-scale information systems apply. Given the extraordinary sensitivity of personal health data, some authors have argued that special attention must be given to issues of privacy and IT security, for example, when it comes to access to centrally stored electronic records for research purposes when there is only little room for effective anonymisation. As an alternative to central databases, France and Slovenia have introduced personal electronic health cards that are carried by the patients and can be read by doctors in practices, hospitals and potentially pharmacies.

Besides electronic health networks, Internet technologies may also facilitate healthcare in other ways. For example, general practitioners (GPs) and medical personnel in primary and secondary care can make use of digitally networked technologies to tap each other’s expertise, get a second opinion on difficult cases with the consent of the patient, and share best practices with peers. A case in point is the online community Sermo, where physicians can share their latest insights and collaborate on challenging cases. The hope is that such collaboration improves the quality of treatment at marginal costs and reduces the probability of error.

Further, patients and their families increasingly use the Internet to find information about symptoms, diseases, and treatments. In OECD countries, about 25% of all adults have used the Internet on average to seek health information in 2007 (see Figure 24). While it is not always clear from the data what “information seeking behaviour” exactly comprises, it involves at least searching for health-related information on the web or sharing one’s experience with other patients via e-mails, bulletin board systems, or social networking sites specialised in health topics (e.g. patientslikeme.com). Public health portals can provide support and information regarding disease prevention, treatment and management of healthy lifestyles.

---

307 Commission of the European Communities, supra note 306, at 41.
309 Other countries like Germany are currently testing the concept.
Further, digitally networked information technologies can be employed as part of the treatment itself. One example is telemonitoring of long-term care patients. Currently, researchers are exploring the potential and practicability of so-called personal health systems (PHS). Key technologies like biosensors or secure communications may be built into smart clothes and implants in order to help patients and their doctors to continuously monitor and manage their health status. For example, telemonitoring of heart conditions is reported to reduce mortality by an estimated 20%, while telemonitoring of patients who would otherwise be kept in hospitals could save between 30-60% and 40-70% of health professionals’ time.\textsuperscript{312} Another innovation currently discussed is telermicine services, which allow treatment at a distance. Commonly defined as “the delivery of healthcare through the use of Information and Communication Technologies (ICT) in a situation where the actors are not in the same location,” telermicine services can be deployed both between two health professionals and between a health professional and a patient. Examples of such practices are teleradiology or telesurgery, but also telepsychiatry in the case of mentally ill patients.\textsuperscript{313}

A critical component of every public service infrastructure, healthcare has been up on the agendas of national and supranational policy-makers for a while now. While initiatives have been launched in many EU member states, the efforts have remained fragmented with often-incompatible systems implemented by doctors or hospitals across the continent. Given the goal of providing EU citizens with the highest standards of healthcare wherever they go, the EU initiated—among other things—an eHealth Action Plan in 2004 as part of its i2010 policy framework to facilitate a harmonious and complementary European approach to health.\textsuperscript{314} The plan sets out a


number of steps towards a widespread adoption of eHealth technologies across Europe by 2010 and covers a broad range of service from electronic prescriptions to health cards and IT systems that reduce waiting times. The European Commission also issued a recommendation for cross-border interoperability of eHealth systems in 2008\textsuperscript{315} and launched a Lead Market Initiative for the deployment of “eHealth services” in 2007, putting the EU in a leading position in the area of regional and national health information networks.\textsuperscript{316} As mentioned above, a key challenge will be to make the best possible use of eHealth technologies for the benefit of the patient while complying with European privacy and security regulations.

11.4 Digital Activism

Besides the abovementioned new forms of citizen participation in public service, the Internet has also been discovered as a medium for activism more generally.\textsuperscript{317} Already in the 1990s, researchers and practitioners started discussing Internet activism and the question of how new media has been used by a variety of political movements. Among the earliest cases that received wider attention was the use of the Internet by the indigenous Zapatista movement in the Chiapas region of Mexico\textsuperscript{318} or a “laptop campaign” that resulted in the Landmine Ban treaty\textsuperscript{319}. Consequent analyses focused—among other things—on the role of online media in the anti-globalisation movement\textsuperscript{320} and more recently the use of the social web in the context of grassroots initiatives like Moveon.org, a non-profit organisation that aims to involve citizens in political advocacy and fundraising. Most recently, Internet-based technologies like Twitter have gained

Most basically, it is argued that advances in increasingly personalised and mobile information technologies afford new forms of resistance and political organisation. The costs of communication are assumed to be reduced substantially, and the scope of communication has increased across the geographical and temporal boundaries associated with previous communication technologies. It is claimed that the Internet enables individuals to gather around topics of interest and form dynamic and highly-informed virtual communities.\textsuperscript{321} This is thought to support and facilitate all kinds of cause-related activities like fundraising, lobbying, community building, and the recruitment and motivation of volunteers.

\textsuperscript{318} See David Ronfeldt et al., THE ZAPATISTA “SOCIAL NETWAR” IN MEXICO (1998).
\textsuperscript{319} See Maxwell Cameron et al., TO WALK WITHOUT FEAR: THE GLOBAL MOVEMENT TO BAN LANDMINES (1998).
\textsuperscript{321} See Howard Rheingold, SMART MOBS: THE NEXT SOCIAL REVOLUTION (2002).
However, while these new forms of Internet-based activism are often regarded as desirable developments to foster civic engagement and democratic participation, it is important to also keep in mind that many of the same techniques have been employed for destructive causes, for example, in the context of international terrorist networks like al Qaeda. One challenge could therefore be to find ways to foster cyberactivism as a welcome form of non-governmental engagement in politics while containing new forms of cyberterrorism.  

See Section 8.6 for further discussions of the phenomenon of cyberterrorism.
12. Business on, through and with the Internet

Over the last decade Internet technologies have played an increasingly important role for the way business is done on a local and global scale. An increasing number of transactions are now computer-mediated, transforming value chains on every level. Not surprisingly, this transformation has had profound consequences for existing business models and opened up space for new ones.

12.1 The Rise of Computer-mediated Transactions

Networked computers are involved at some point in the value chain of virtually every transaction today. With the uptake of the web in the mid-1990s, businesses started to realise the potential of initiating and coordinating transactions online, i.e. across time and space without any face-to-face contact, and started to engage in what came to be known as “e-commerce”. The most obvious cases from a consumer’s perspective are Internet-based trading platforms and online retailers like eBay and Amazon as well as businesses selling insurance and financial products, groceries, video cameras, vacation packages, and cars. Price comparison sites and search engines allowed users to search for the best deal, compare, and order items from faraway merchants, who in turn had to draw on complex supply chains and logistics companies to get the goods to consumers on time.

Communication services are increasingly provided online. For example, Voice over Internet Protocol (VoIP) services offer voice communications over IP-based networks, also known as “Internet telephony”. Among the best known VoIP services is arguably the software Skype, which offers free calls to other Skype accounts and fee-based calls to landlines and mobile phones. It is also possible to receive calls on one’s computer from regular phones against a fee. Other providers like Vonage offer VoIP services to consumers through dedicated hardware.

These new online businesses also required new forms of electronic payment that were efficient and secure enough to be trusted and used on the Internet. While consumers initially had to use their credit cards for computer-mediated transactions, soon new systems like Smartcard, Electronic Bill Payment, or PayPal became available.

According to recent studies, the percentage of individuals who ordered goods or services over the Internet for private use in the past year in the EU25 rose significantly between 2004 and 2008, from 22% to 34%; in 2008, 32% of individuals in the EU27 had ordered online in the last year (cf. Figure 25). Market research institutes estimated the European e-commerce market at €106 billion in 2006 with 70% of turnover being concentrated in the United Kingdom, Germany, and France.

Consumers are on average more satisfied with shopping on the Internet than with retailing in general. For example, 80% of consumers who bought entertainment and leisure goods on the Internet thought that their retailer’s prices offered reasonable value for money, compared to an average of 67% for all retail channels. Overall, the retail market over the web has grown considerably and gained importance in a

---

325 Id.
326 Id., at 10.
variety of areas from shopping to insurance and gaming, producing a new customer interface.

Figure 25: Percentage of Individuals Who Ordered Online for the Last Year (2008) (Source: Eurostat Information Society Statistics, quoted in EU eCommerce Report 2009)

More conventional businesses have been transformed by networked computing without necessarily being classified as e-commerce. While accounting systems were among the earliest applications, digitally networked technologies now pervade many aspects of the value chain. In supermarkets, for instance, cash registers are basically networked computers with specialised interfaces, directly connected to databases that allow retailers to monitor transactions on a large scale and transmit orders directly to wholesalers. Shipping companies like UPS utilise online networks to optimise delivery routes, reportedly saving 12 million litres of fuel in 2006 from nearly 100,000 trucks.  

In 2007, on average, 33% of all businesses with 10 or more employees in OECD countries used the Internet for purchasing and 17% for selling goods or services (see Figure 26).  

Since the early days of the Internet, procurement packages for both commercial off-the-shelf and bespoke goods have been equipped with Internet access features, allowing buyers to compare prices quickly and efficiently across markets.  

Industrial sourcing increasingly takes places via online reverse auctions, in which sellers compete for business by offering their products and services for lower prices than their competitors; such auction mechanisms have already been used to procure billions in parts and services in both the public sector and virtually every major industry. 

328 OECD, FUTURE INTERNET, supra note 241, at 25.  
This extensive use of networked computing both inside and outside enterprises has transformed existing business models and paved the way for new ones. Some general features can usefully be distinguished. It has been argued that computer-mediated transactions allow for more intensive monitoring and performance measurement of contracts, behavioural data can be extracted and analysed on a large scale, and goods and services can be increasingly customised and personalised to optimise transactions for individuals and organisations.\textsuperscript{331} New concepts like “the long tail” have been discussed, claiming that business strategies can be built on selling small amounts of obscure products.\textsuperscript{332} At the same time it has been argued that despite more products being available for purchase the main revenue sources will remain in the head of the tail, following a power law distribution.\textsuperscript{333} 

\textsuperscript{331} See James Manyika, \textit{Hal Varian on How the Web Challenges Managers}, MCKINSEY QUARTERLY, January 2009, p. 4-5.
12.2 Monetising Web-based Businesses: Online Advertising and Attention Economies

Web-based businesses face a number of specific challenges. The first is how widespread user interaction on and participation in online platforms can best be monetised. An early idea was to charge users small amounts of money (so-called “micropayments”) for consuming certain content or having access to a website. However, that strategy did not take off since users were not willing to pay for content they could get for free in similar quality from other sources. The cognitive load of making many such small purchasing decisions also deters users, which has led more widely to the use of “bundling” strategies that also support hidden price discrimination.

From the standpoint of economic theory, social welfare is maximised when price is equal to the marginal cost of production. So if the marginal costs of production are effectively zero and the use of the information good cannot be perfectly controlled, it follows that there will always likely be a competitor with a similar offering for free.

In view of these problems, it is not surprising that Internet platforms and content providers have developed alternative ways of monetising their popularity. Besides the option of charging for extra or “premium” services, online advertising has turned out to be the largest revenue source. Advertisers are charged by impressions, targeted views, click-through rates, or even completed transactions. In addition, ads can be targeted based on the context or certain features of the user in the case of personalised services. According to the Interactive Advertising Bureau (IAB) Europe, the European market for online advertising was worth €12.9 billion in 2008, still lagging behind the U.S. as the biggest online advertising market with €16.6 billion (see Figure 27).

![Figure 27: Total Online Advertising Europe 2006-2008](Source: IAB Europe, AdEx2009, Presentation at Interact Congress, June 10, 2009, p. 5)

A key feature of contemporary web-based communication platforms is therefore the emergence of so-called “attention economies.” In mediated communication systems the scarce commodity is not any material resource or access to technology, but people’s eyeballs. Attention is considered crucial for facilitating further transactions and directing people to specific products, services, or content.

Many recent businesses and start-ups have tried to capitalise on this idea. Most prominently and successfully, Google has developed a business model that is largely based on capturing the focused attention of users and monetising it through targeted

---

334 See Carl Shapiro & Hal R. Varian, INFORMATION RULES (1999), pp. 73-78, 103 ff.
advertising on search results. Major web services like Gmail, Google Search, Google Calendar, or Google Book Search are offered for free in order to create attractive and user-friendly environments that attract the attention of as many users as possible. In the case of Google, digitally networked technologies are also used to manage the transactions with its advertisers. For example, keywords for search queries are auctioned in real-time.

12.3 ICTs in Organisations and the Workplace

Information and communication technologies have also had a substantial impact on how organisations and individuals work. In many businesses, networked technologies are already deeply embedded in day-to-day operations. For example, companies like Vonage offer complete alternative VoIP services to the standard voice carriers, cutting costs considerable while increasing dependence on the Internet. Such new technologies do not only allow for efficiency gains, but also new forms of monitoring, accountability, and performance measurement. For example, networked cash registers at supermarkets allow local supervisors to track their employees’ performance in real time and intervene accordingly if deemed necessary. Intranets and large-scale IT systems in large corporations often record e-mail and instant messaging communications by default—a potentially useful data set for regulators as the Enron case has shown. In 2007, the average rate of usage of the Internet in companies of 10 and more employees was 95% across OECD countries (see Figure 28).

![Figure 28: Proportion of OECD Businesses Using the Internet](source: OECD, The Future Internet Economy: A Statistical Profile (2008), p. 6)

One implication of the increasing use of these technologies is the geographical distribution of work. Teams do not have to be in the same building to effectively work together. While early discussion focused on issues of teleconferencing, other applications of information technologies in the workplace may be even more illustrative. A good example are call centres. Orders at drive-through counters at McDonald’s restaurants across the U.S. are not taken by the local staff, but a central call centre that records the customer’s choices and instantaneously submits them to
the local restaurant for preparation and delivery.\footnote{Matt Richterl, \textit{The Long-Distance Journey of a Fast-Food Order}, N.Y.TIMES, Apr. 11, 2006, available at http://www.nytimes.com/2006/04/11/technology/11fast.html (last visited June 24, 2009).} Other call centres are organised in a decentralised fashion themselves. The company Live Ops, for instance, offers services that are not provided from traditional brick-and-mortar offices, but through a virtual community of over 20,000 remote agents that offer on-demand call centre services as independent contractors, connected through cloud computing.\footnote{LiveOps Website, http://www.liveops.com/index.html (last visited June 24, 2009).} Even the application process for becoming a remote agent is largely virtual, involving tests for reading comprehensions and voice auditions.\footnote{LiveOps, \textit{Frequently Asked Independent Agent Questions}, http://www.liveops.com/become-agent/faq.html (last visited June 24, 2009).} A related model is pursued by Amazon’s Mechanical Turk, a crowdsourcing platform, on which computer software coordinates so-called “human intelligence tasks” (HITs), which interested users can complete for a monetary payment remotely in front of their screens.\footnote{See Amazon Mechanical Turk, https://www.mturk.com/mturk/welcome (last visited July 31, 2009).} Some authors have pointed to the social and ethical implications of such arrangements and expressed concern over alienation and privacy invasions.\footnote{Jonathan Zittrain, \textit{Ubiquitous Human Computing}, Oxford Legal Studies Research Paper No. 22/2008, available at http://ssrn.com/abstract=1140445 (last visited July 31, 2009).}

While in the past many business models have been predicated on control, it has been argued that in the future more emphasis will be put on group decision-making and consensus. Small groups are often seen as critical for the success of an organisation. Again, Google Inc. is often mentioned as an example. The company allows engineers to dedicate 20% of their time to work on a personal project. A related strategy would be to acquire small companies and start-ups to incorporate small group expertise and creativity.

\section*{12.4 Trends in the ICT Industry}

At 32\% of global ICT spending, Europe is the world's largest ICT market.\footnote{Viviane Reding, \textit{The Digital Dividend: A Unique Opportunity for Europe's Wireless Economy}, ComReg Conference "How Ireland Can Best Benefit from Its Digital Dividend", Dublin, Oct. 1, 2008, p. 4.} On a global scale, more than half of the estimated 2007 ICT spend was on communications services and hardware, 21\% on computer services, 14\% on computer hardware and 9\% on software (see Figure 29).
Some current trends can be identified in the ICT industry. Open source software has been remarkably successful and has developed into a major commercial force. Examples are the Apache web server software, JAVA, the MySQL Community, or Mozilla Firefox. Another trend is cloud computing. The increasing availability of fast and affordable web access has enabled new forms of computing that do not depend on local data centres, but run applications remotely from a central server or “cloud”.

Major Internet companies like Amazon, Google, or Salesforce already offer cloud-based web services to companies, including e-mail, computer storage, and software for managing relationships with customers, suppliers and business partners. Cloud computing thus enables “software as a service,” a trend which has been discussed among software vendors and CIOs for some time. The underlying idea is to deliver software services online: businesses sign up to use software hosted by a third party instead of buying a license and installing it on individual machines.\(^{341}\) While cloud computing and software as a service promise significant cost-savings and an increase in flexibility, many major corporations hesitate because of concerns over data security, reliability, and regulatory compliance.\(^{342}\)

Traditional telecommunications incumbents are currently in search of new revenue streams and—at least in the U.S.—have recently attempted to introduce differential pricing models for data traffic. This had led to passionate debates about “network neutrality”, which have also started in Europe with some variations.\(^{343}\) Mobile network operators have been looking for ways to expand their data services to compensate for falling profits from voice and text messaging—mobile broadband


Internet access is a particularly attractive service that requires a combination of new technologies and spectrum capacities.
13. From Wired to Wireless

The commercial success and functionality of mobile multimedia devices like the iPhone in combination with faster and more reliable wireless networks has led to a significant recent increase in market penetration for the mobile Internet. According to the last PEW Internet Survey, “mobile phones will be the dominant connection tool” by 2020.\(^{344}\) In January 2009, the number of mobile phone subscribers surpassed 4 billion globally.\(^{345}\) This section therefore briefly describes the development of the mobile Internet and maps some of its key opportunities and challenges.

13.1 How the Internet Went Mobile

The rise of the mobile Internet can be understood in terms of two separate developments: the increasing technological capacity of mobile phones and the increasing portability of personal computers. Both lines of development faced essentially similar constraints: limited user interfaces or mobile use and limited capacities and coverage of wireless networks that would allow large-scale exchange of multimedia data.

The first line of development started when mobile phone manufacturers were considering the possibility of integrating Internet connectivity into mobile phones. The first mobile devices with PC functionalities were introduced in the early 1990s. An example of an early Smartphone was the IBM Simon Personal Communicator from 1992, which combined a mobile phone with applications like a calendar, address book, world clock, calculator, and e-mail. A pioneer on the European continent was Nokia, who launched their Communicator 9000 in Finland in 1996, a mobile device with Internet connectivity.

In Japan, South Korea, and Taiwan, NTT DoCoMo’s wireless Internet service “i-mode” became widely popular and consecutively spread from Asia into the rest of the world. Introduced in February 1999 in Japan, i-mode could be accessed directly from the handheld device through a special i-mode button with navigation sites to the handset interface. The service allowed users to access Internet services like e-mail, games, financial services, weather forecasts and other services typically offered by the respective mobile carrier. Technically, i-mode was built upon Internet standards such as C-HTML as well as proprietary protocols. The success of i-mode is sometimes attributed to its business model that integrates “equipment manufacturers, content providers, and other platforms to ensure that wireless technology, content quality, and user experience evolve jointly.”\(^{346}\) Given i-mode’s success in Asia and its by now more than ten years of experience in mobile Internet markets, it may offer some lessons for the design of other services in the future.

At around the same time, the competing Wireless Application Protocol (WAP) standard started to be promoted by a number of mobile carriers. WAP is based on Wireless Markup Language (WML) and allowed users to access content in the appropriate format via a WAP browser on the go. In 2002, the first BlackBerry smartphone was released, which combined mobile phone capabilities with a push e-mail service and web connectivity, reaching 28.5 million subscriber accounts in

---

The development of devices and standards went hand in hand. Obviously, the growth of mobile services depended on both devices and networks. Currently, the third generation (3G) of mobile telephony standards as defined by the International Telecommunications Union (ITU) is in use all over the world, including standards like DECT, WIMAX, the UMTS family or CDMA2000.

However, despite these efforts and innovations, it was only in 2008 that a mobile device became widely popular in Europe. Running on mobile phone and wifi networks, Apple’s iPhone was introduced in late 2007 and widely regarded a success story in terms of uptake of the mobile Internet. Operating on the existing fast 3G networks, the iPhone offers an easy-to-navigate user interface with a touch screen and colour display. By the beginning of 2009, the iPhone reached total sales numbers of 21.17 millions worldwide (see Figure 30) and made the mobile Internet accessible through a broad range of applications by both Apple and a large number of third-party providers.

![Total iPhone Sales Chart](source: Wikipedia, based on Apple Company Reports)

Besides the increasing Internet connectivity of mobile phones and their respective networks, a parallel development allowed more location-independent Internet uses by increasing the portability of personal computers. While laptops had been around since the early 1970s it was only in the 1980s that wireless networking started. With wireless LAN networks like wi-fi, laptop PCs and PDAs were increasingly able to connect to the Internet with comparatively low effort and costs. Many wifi-enabled locations have developed into popular hot spots that have attracted users, such as in coffee shops. So while laptops and netbooks are becoming smaller and smaller, smartphones like the iPhone are becoming more and more powerful—with the result that portable PCs and mobile devices increasingly converge. Sophisticated electronic interfaces and the availability of wireless network capacities have made the mobile Internet a social and commercial reality.

### 13.2 Opportunities and Challenges of a Mobile Internet

The mobile Internet presents a number of opportunities and challenges. From an economic point of view, wireless technologies are already a major driver of the EU

---


The economic value created through wireless technologies is estimated at €250 billion or 2-3% of GDP and rising already today.\textsuperscript{349}

This growth is likely to be both direct and indirect. Direct growth is expected in mobile data traffic. Wireless broadband is already taking off with nearly 500 million 3G subscribers globally, and also the fast uptake of ultralight portable netbooks is likely to increase that trend. As EU commissioner Viviane Reding noted, wireless services are growing at 10% per year and will have surpassed fixed networks by 2010 to achieve 55% of worldwide telecoms revenues.\textsuperscript{350}

Potentially even more important, indirect effects are likely to set in when mobile technologies have reached critical mass and networks effects can materialise. New services and applications are likely to emerge and provide access to the conventional web and integrate these with mobile-specific feature like mobile payments, geo-targeting and mobile social networking. At the same time, these services can provide the basis for a range of location-based secondary services like traffic control or environmental sensing networks. For 2009, it is expected that 5 billion or three quarters of the planet's population will have access to a mobile handset.

It has been noted that the further uptake of mobile Internet connectivity will depend on costs. For consumers, the cost of connectivity makes a significant difference for the uptake of fixed lines and mobile phones.\textsuperscript{351} When costs for connectivity drops, time-intensive uses will become more affordable and common. This may include browsing, streaming music, participating in social networking sites, playing games, and new forms of instant messaging and communication. A key target group in this regard are young people and children, who are traditionally among the earliest adopters of new communications technologies.

However, the mobile Internet and especially mobile broadband also face a number of challenges. These include the network infrastructure necessary for mobile devices to connect. For example, high-speed mobile broadband requires additional bandwidth, should it become a real alternative to fixed broadband.\textsuperscript{352} A key issue here is the availability of spectrum, which is a core public policy issue at the European level. A fourth generation (4G) wireless network would require additional spectrum, which would need to be freed up for wireless applications. One option is this regard is to allow mobile phone companies to "re-farm" 2G spectrum bands for more advanced 3G services such as mobile Internet access by releasing them from existing license restrictions.\textsuperscript{353}

Another aspect to consider regarding network infrastructure is that the main target for 3G architectures is to make use of core IP networks. This would mean that all IP traffic would be carried directly through the existing IP networks so that mobile devices could fully access the Internet, including VoIP applications. While this could


\textsuperscript{350} See Reding, supra note 340, at 2.

\textsuperscript{351} Leslie Haddon, \textit{Mobile Communications, the Internet and Society}, Policy Forum at the Oxford Internet Institute, March 20, 2009.

\textsuperscript{352} See Reding, supra note 340, at 3.

also be achieved through the conversion of non-IP protocols to IP higher up the application stack, there is resistance from operators due to the potential impact on revenues. However, it can help new market entrants to grow rapidly, as can be seen for example with the UK operator “3”, which has opened up direct access to the Skype VoIP network. IP architecture in the core network is also behind the “dongles” for mobile data transmission on 3G networks across Europe.

A second set of challenges revolves around the need for investments in open infrastructures. The growth of mobile networks over the past decade has only been possible because of substantial investments in wireless broadband services. Important trade-offs here concern the benefits vs. the burden imposed by regulation. But also business models need to be developed that offer users with attractive and transparent pricing models that can compete with fixed broadband data plans and flat rates. Another issue is that existing mobile phone networks are almost exclusively closed systems with the consequences that start-up costs for new entrants are considerable. This, in turn, inhibits the scaling-up of the mobile Internet, which may or may not be overcome with the emergence of open operating systems.

A further set of challenges concerns the risks mobile Internet services pose to fundamental rights as well as their implications for the social welfare of citizens and users. Most importantly, location-based services inevitably process personal data by tracing and tracking individual movements. While this may provide an opportunity for new business models, it could equally be abused for generating behavioural profiles and become a threat to individual privacy. In addition, it has been noted that affordable mobile connectivity may also make it harder for parents to monitor their children’s Internet use. Child protection lobbyists have therefore pointed to the need for adequate measures to protect children in their use of mobile devices at both the national and EU level. Mobile uses of the Internet may also interfere with other potentially dangerous activities like driving.

Finally, it has been argued that mobile platforms have the serious potential to be set up as “walled gardens” that only let certified applications run on their infrastructure. Consequently, the European Commission has emphasised the need to ensure open platforms for mobile services.

---

354 Cf. Zittrain, supra note 152, ch. 5.
355 See Reding, supra note 340, at 4.