CHAPTER 7. A DIGITAL FUTURE: REGULATORY CHALLENGES IN A BRAVE NEW WORLD

CHAPTER 7. A DIGITAL FUTURE: REGULATORY CHALLENGES IN A BRAVE NEW WORLD

7.1. Introduction

Human communication has changed immeasurably in less than a generation. Today's children are born into a world in which their means and opportunities to connect with each other and to share information would have been unimaginable to their own grandparents - even their parents. Whether it's called the Digital Age, the Information Society, or the Digital Economy, we are witnessing a fundamental transformation of the most basic relationships among individuals, governments, and cultures. This new era brings with it limitless possibilities for humankind to realize new achievements, harnessing the powers of information and communication for the betterment of the planet. But it also presents new and unfamiliar challenges, and the risk that these technologies of enlightenment could be turned to darker purposes.

In this environment, the role of communications regulation is changing fundamentally as well, but it remains critical to the prospects of realizing the most ambitious goals for ICT-driven development. Indeed, it is due to the strong successes of regulatory authorities, *inter alia*, in their implementation of many of the traditional and innovative practices highlighted in the foregoing chapters of this book, that the current ICT revolution has taken off with such force. As the next generation comes of age in a world saturated with interconnected devices and infinite information resources, their aspirations to take advantage of these media to enhance the fortunes of the global society they will inherit will be heavily influenced by the policy and regulatory landscape that governs them. This chapter thus introduces some of the most prominent new regulatory challenges arising in the context of this transformative digital communications age.

7.2. Convergence, Ubiquity, and Web 2.0

The communications world is vastly different than even a decade ago and continues to evolve rapidly. The greatest forces for change are convergence of media, increasing ubiquity of connections, and the interactive, user-generated nature of the new paradigm.

7.2.1. Convergence of Communications Media: The Future Has Arrived

The concept of "convergence" in the world of communications has been anticipated, forecast, planned, and discussed for several decades - always with the implication that convergence is "on the way" and when it arrives, the traditionally distinct realms of media, technologies and networks will ultimately blend into a seamless and interchangeable whole.[12] As we enter the second decade of the new millennium, it is safe to say that this long-awaited era of convergence has at last arrived in full force.

Over time, the idea of convergence has taken on multiple and overlapping meanings, reflecting different perspectives of the traditional communications landscape. In fact, a variety of interrelated phenomena have been converging at the same time:[13]

- *Computing and Communications*: The merger of IT with C to yield the integrated world of ICT is ultimately at the core of all convergence trends. For more than two decades, the processing power and storage capacity of integrated circuits has been multiplying endlessly, while becoming deeply interwoven with the exponentially growing transmission capabilities of global telecommunications networks. The marriage of the two previously discrete fields is what has made possible the instantaneous sharing of limitless data in any form, in any location around the world.

- *Voice and Data*: Once distinct services and even networks, there is now virtually no distinction as to how most voice and data signals are carried from end-to-end throughout telecommunications links. Not only do nearly all networks now ubiquitously employ digital switching and transmission, but voice calls are also increasingly processed over IP packet-switched systems. In effect, only the end users themselves know whether they are talking or sending data files.

- *Wires and Waves:* Wireline and wireless networks remain separate in only limited ways; most services involve some combination of both. Telecommunications operators deploy terrestrial fixed cables (copper or fiber) where it makes technical and economic sense, and utilize a variety of radio-based connections, from microwave to satellite, for other segments of their networks. This extends all the way to customer premises equipment, where users often prefer cordless handsets attached to wireline public switched networks, as well as in-home or corporate WiFi local area data networks. The chief distinction from a technical and regulatory point of view remains the need to allocate frequencies for wireless segments and minimize interference.

- *Broadcasting and Telecommunications*: Broadcast television and radio developed separately from point-to-point telecommunications, often with separate regulatory regimes. They are increasingly integrated: cable and satellite TV are becoming the dominant media by which audiences receive television signals, and IPTV is right behind them; Internet and satellite radio are also widely utilized. Frequency allocations for broadcasting are being reassigned to allow more efficient use of spectrum for digital broadband transmissions. Ironically, some broadcast signals are returning indirectly to the airwaves in this manner: as they are transmitted from their original source onto the Internet, then accessed by users via wireless mobile devices.

- *Conduit and Content:* The traditional separation of broadcasting from telephony also yielded distinct approaches to regulation of communications content. Television and radio stations were subject to public oversight of their programming, but monitoring the content of voice telephone calls required a special permit to eavesdrop, usually only granted to law enforcement agencies and national security services. Telephone networks were "common carriers," or merely conduit for the signals sent over them. In the converged environment, all networks carry an indistinguishable mix of messages, from voice to data to audio and video.

- *Corporations and Networks:* Convergence is naturally also reflected in the strategic maneuvers of the corporate interests that inevitably vie for control of each new popular manifestation of consumer demand for communications. Both within countries and across national boundaries, media and network ownership is heavily concentrated among a core

of mega-corporations (e.g., AT&T, NTT, Deutsche Telekom, Vodafone, Microsoft, Intel, Samsung, Sony, etc.), which are likely to consolidate further as the industry matures worldwide. Such corporate convergence and market consolidation will be a key trend to watch in the years ahead.

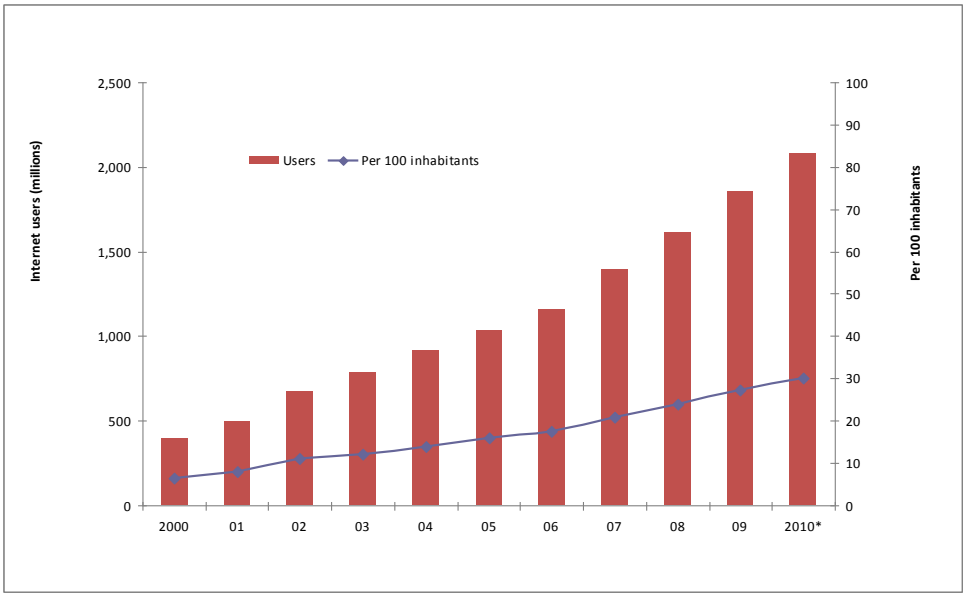
The practical impacts of all these converging trends are limitless, and have created both challenges and opportunities for industry planners, consumers, and governments alike. Today, there are no longer isolated and independent service markets for any and all kinds of communication. Customers can watch television on their MP3 players, access e-mail from their iPads, chat online while playing video games, conduct telephone conversations via their laptops, listen to radio through their cable TV, upload photos and videos directly from their digital cameras. They can do all of the above and more while working, travelling, or sitting in a park. And these options will only continue to expand in the years ahead.

For those concerned with regulation of the increasingly wide ICT universe, convergence implies a certain fundamental realignment of perspective. It means that regimes and rules once applied separately to broadcasters and telephone companies, to mobile networks and landlines, to content providers and common carriers, all must be revisited, and often themselves merged into a new, integrated regulatory framework. Some of the imperatives arising from this new perspective have been noted in the previous chapters of this *Handbook*: on licensing, competition, spectrum regulation, and the like. Looking ahead, it is clear that regulatory functions and objectives will have to take into account a variety of new issues resulting from convergence, as well. This will demand both new resources and new ideas, which recognize that a new communications era is most definitely upon us.

7.2.2. Ubiquity: Mass Communication for the Masses

While communications networks, media, and devices have been converging, they have also been spreading: blanketing nearly the entire planet, multiplying exponentially, finding their way into the homes and hands of millions more people every year. The raw numbers speak for themselves.

Figure 7.1 Global numbers of Internet users, total and per 100 inhabitants 2000-2010



Source: ITU World Telecommunication/ICT Indicators Database.

There are now at least 70 countries, many of them developing ones, in which the number of mobile phones in circulation (or more accurately SIM cards) exceeds the entire population. As at end 2009, more

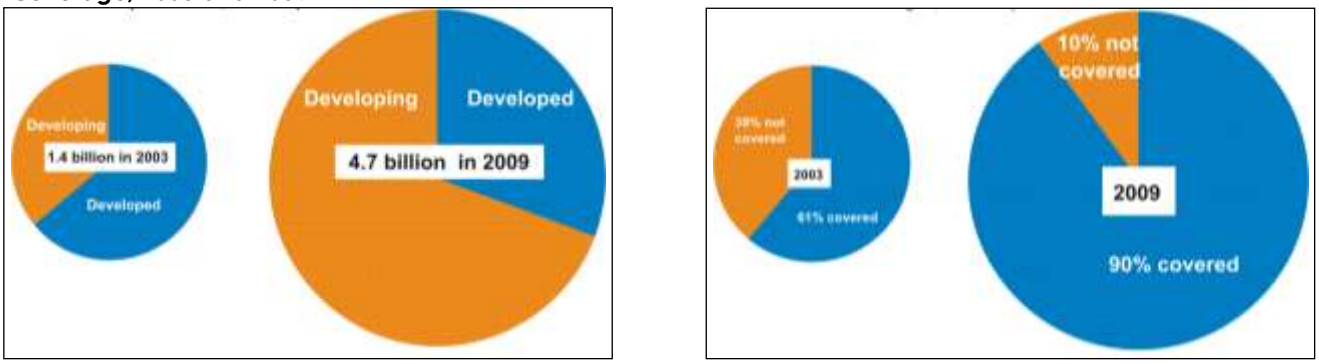
than a quarter of the world's population was using the Internet (see Figure 7.1). There are over 200-million registered domain names, and about 100-million active web sites, containing more than 20-billion individual web pages.[14] The volumes of traffic and data transmitted continue to increase steadily, regardless of economic conditions. The most popular web sites – Google, Yahoo, Facebook, Windows Live/MSN, YouTube, China's Baidu and QQ services – all have users or visitors counted in the hundreds of millions. During the 2010 FIFA World Cup in South Africa, Internet traffic to news-oriented web sites worldwide peaked at over 10 million visits per minute.[15]

Information Wealth

At the high end of the economic scale, in OECD countries and among the wealthier segments of nearly every society, individual citizens are becoming almost permanently connected. They utilize PCs on their office and school networks, while carrying WiFi-enabled laptops to every meeting, classroom, and coffee shop, listening to their iPods and perusing their e-Book readers on the train and bus, or else navigating their cars with smart GPS devices, then returning home to their personal PCs and in-house broadband networks, 500-channel digital television services, online video game systems, and satellite radio receivers, all the while talking, texting, e-mailing, surfing, and posting via their always-on mobile smart phones. The term "ATAWAD" has been coined for this growing trend of digital ubiquity: Any Time, Any Where, Any Device.

But extensive levels of connectivity are penetrating well beyond the elites, to moderate and lower income households, farther and farther out from cosmopolitan centers, and most especially among younger age groups, in nearly every region, country, and culture. Mobile phones have been the leading wave in this rising tide; the combined innovations of pre-paid calling cards, calling-party-pays pricing schemes, and SMS texting, together with the convenience of mobility and shrinking size and cost of handsets, created a perfect industry storm that was largely unanticipated, particularly in the less developed corners of the world. According to the ITU, at the start of 2010, there were over 4.6 billion mobile phones in the world and the overwhelming majority of the growth in recent years has been in developing countries (see Figure 7.2):[16]

Figure 7.2 Global Mobile Cellular Subscriptions by Development Status, and Global Population Mobile Cellular Coverage, 2003 and 2009



Source: ITU World Telecommunications /ICT Indicators database.

Regulators have greatly assisted this growth by opening the newly lucrative cellular markets to multiple independent competitors, who have rushed to invest in infrastructure and networks in even the lowest-end economies, while also bringing in much needed employment and tax revenues. In the process, Universal Service policies and funding (see Chapter 6) have also taken on new significance: rather than merely delivering minimal public phone service to remote villages as emergency connections of last resort, public authorities are now realistically looking to reduce or eliminate altogether the Digital Divide between rich and poor, urban and rural, information saturated and information starved. The widening expectation is that, in the foreseeable future, nearly all humankind will be connected to one another via multiple and ubiquitous electronic communication networks.

Indeed, connections are even extending beyond humans, to include inanimate objects as well. The

emergence of an "Internet of Things" is among the most recent trends.[17] By attaching radio-frequency identification (RFID) tags to virtually any consumer purchase or possession, the nature, location, status of these objects can be tracked and analyzed automatically and in real-time. RFIDs are already used extensively in retail stores for inventory and sales, but this concept implies that objects will remain online permanently. Household appliances can be remotely managed; supplies of home essentials can be monitored and even automatically re-ordered; everything's location and operating status can be tracked; and the history, source, and ownership of objects can be readily identified from its electronic signature. An entire inventory of a person's life might eventually be digitally catalogued for all time.

The Regulatory Imperative

The implications of this immense growth for governments, and especially regulators, are profound. Increasing success in the quest for universal communication means that the scope and impacts of communications services are increasingly significant throughout society. The numbers of people affected by each decision, each new policy, each bold initiative or grave misstep are consistently growing, and the reach of those decisions into their daily lives, their jobs, their social and cultural and political experiences, is ever more extensive.

The role of ICTs in national and local economies naturally has expanded dramatically too, both in terms of the total amounts of money spent on equipment and services, as well as the dependence of companies and employees upon these technologies. Any shift in fees or taxes, any new restriction or prohibition, any investigation or intervention, carries potential consequences that could ripple throughout the economy, for better or worse.

In effect, the role of communications regulatory authorities, whether by design or not, has been elevated into the nerve center of public policy, simply by virtue of the public's insatiable demand for unlimited opportunities to communicate. The pressure on those with day-to-day responsibility to oversee the smooth functioning of the industry has thus increased by orders of magnitude. Any service outages, for example, or perceived poor quality of service, are more likely to galvanize public dissatisfaction with both operators and those that regulate them. Instances of objectionable content or scams or other online controversies will, rightly or wrongly, often be laid at regulators' doorsteps. Moreover, other political powers, as far up as Presidents and Prime Ministers, will be drawn into disputes and crises that might once have stayed well out of their range of vision, simply because of the sheer numbers of citizens affected by ICT developments. The jobs of regulators have never been more challenging, or more important.

7.2.3. The Rise of Social Networking and Web 2.0

One of the overriding features of the digital economy is that it is also an age of democratization: an era in which the masses have a greater voice than ever before in history.

It is sometimes forgotten that the World Wide Web, and even the Internet itself, was not created from the R&D budget of any commercial enterprise. While the technology of the Internet was driven by defense research and public funding, most of the innovations that transformed it from an academic and scientific endeavor into a global communications phenomenon were pioneered by disparate, self-motivated users of the original system. Hypertext transfer protocol (http), hypertext markup language (HTML), and the original Web browsers in the early 1990s, were developed by users for their own experimental (and non-commercial) purposes. That these developments caught on and forged a truly worldwide revolution was as much accidental as intentional.

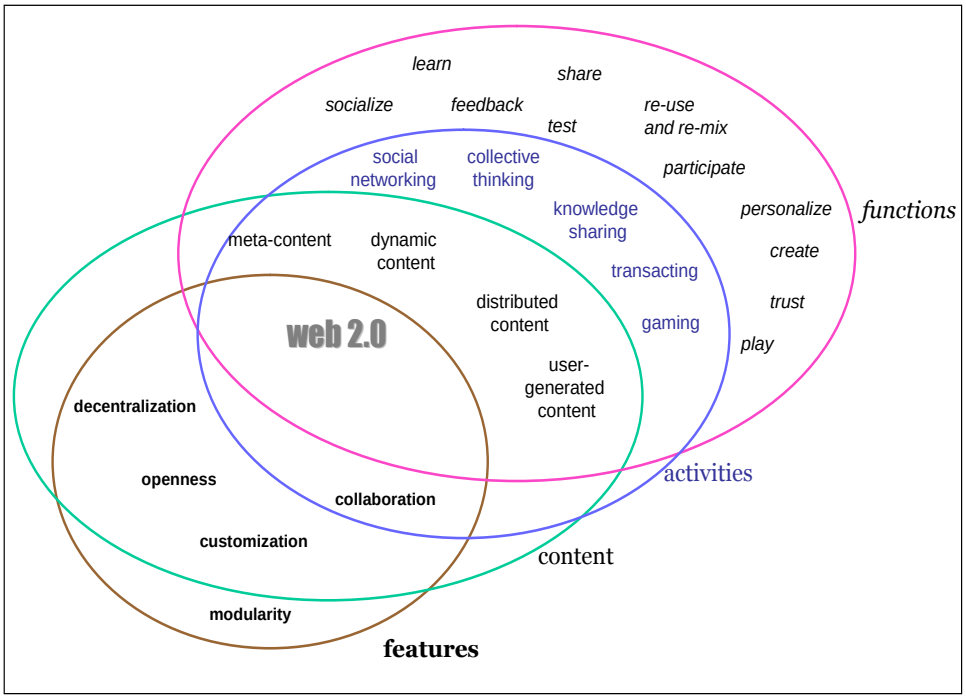
The Next Generation

In recent years, Internet enthusiasts have begun to describe the emergence of "Web 2.0," a term that implies a second generation of the Web's evolution – a more participatory network in which end-users take on a much more important role (See Figure 7.3). In this iteration, the decentralized global Internet has become even more decentralized: peer-to-peer communication and data sharing far outweigh top-down information delivery; the Web is everywhere, and everyone is the Web.

The "killer app" of this latest phase of the Internet is arguably social networking.[18] The core concept involves web-based services that allow individual users to create their own virtual biographies and diaries, and thereby to link themselves electronically with countless digital companions throughout

cyberspace. In just a few years' time, the Internet has become thoroughly dominated by these interactive, user-focused sites. By far the most successful service in this genre – and indeed on the Internet as a whole – is Facebook, the site that claims over a half billion members around the world, who constantly update their status, friends, photos, likes, and interests on a daily, even hourly basis. In terms of traffic generated, it is rivaled by YouTube, in which users themselves are also the main generators (or at least disseminators) of content. Both these applications are now driving mobile Internet traffic as well.

Figure 7.3 The Workings of Web 2.0



Source: Srivastava, 2009.

Among the countless other global sites offering similar services are such leading alternatives as MySpace (allowing multimedia user profiles), Twitter (immensely successful focus on short status messages, or "tweets"), LinkedIn (concentrating on business and job profiles), Ning (a shared web development site), hi5 (very successful in Asia), and several sites competing to dominate the vast Chinese social networking market: QQ, RenRen, 51, Baidu, and others. A special category of social networking sites are dating and marriage services, which abound in nearly every society, helping millions prospective lovers to find one another through photos, text, videos, and chatting features.

The simple concept of having users themselves create the content of an information or entertainment service, thus both minimizing costs and engaging users in the active development of the service, has also expanded far beyond the pure social networking model. There is a wide and growing array of media that now follow the same path of bottom-up, populist content sharing, many of which have risen to be among the most popular features available:

- *Multimedia Sharing:* Sites that allow users to upload and share photos, music, and especially video, showcasing their own creations or interests. By far the leader in this group is YouTube, which hosts over 120-million video clips, from archival to esoteric to amusing to political and even commercial scenes.
- *Weblogs*: Personal and community diaries, universally known as "Blogs", which typically involve commentary and discussion on topics of interest to the blog host, with user feedback and debate. The largest blogs, which cover politics, industry, entertainment, and other popular

subjects, draw thousands of visitors and comments every day from around the world.

- *"Wiki" Media:* A Wiki is a format for interactive user-based editing of online documents. In addition to posting new material, contributors are encouraged to review and revise others' previous posts, in a collective editorial process. The dominant forum of this kind is Wikipedia, the immense non-profit Internet encyclopedia with more than 10-million entries in dozens of languages, all user-generated and user-edited.[19]

- *Chat, Voice, Video:* Some of the most common activity on the Internet involves old-fashioned person-to-person conversations. Chat and Messenger services such as MSN and Yahoo! Messenger allow users to chat together or in small groups in real time. Skype, on of the first successful VoIP services, highlights free PC-to-PC voice telephone calls. All of these services now permit video calling as well, using low cost webcams.

- *Interactive Online Games:* Playing games on the Internet may be the single most popular activity among the younger generation (and many not so young), who represent the largest growth segment of the digital culture. Although most game structures and engines are created by programmers, many of the most successful involve "role playing" by users, who invent their own characters and interact with other online players across the virtual world. The largest community to date of these Massively Multiplayer Online Role Playing Games (MMORPGs) is for *World of Warcraft*, a fantasy game which had reached over 12-million paying subscribers by October 2010.[20]

- *Virtual Selling and Shopping:* Users have also become digital shop owners. The virtual marketplace pioneered by eBay, through which anyone can sell almost anything via a simple auction or direct sale, has been adopted by a variety of other, more traditional Internet retailers such as Amazon.com. This trend of micro e-commerce has encouraged millions of small entrepreneurs in dozens of countries.

- *Reality TV, Talk Radio:* Reflecting the populist trends in cyberspace, traditional broadcast television and radio have also brought users (audience) more into their programming. "Reality" television programs have become a dominant genre, including talent contests among amateur performers, with audiences voting for their favorites, as well as wide variety of other formats which showcase the lives and challenges of "real" people. On radio, the spread of mobile phones has pushed the "talk" format to new heights, as listeners can call to express their views on sports, politics, and current events, wherever and whenever they get the urge to talk.

Network Effects

One significant impact of exploding user demand to produce and display their own content has been exponentially increasing demand for bandwidth and data storage. The most appealing aspects of social networking involve sharing images, sounds, voices, and videos: the full scope of one's virtual identity. As this phenomenon continues to spread via multiple overlapping and converged media networks and devices, worldwide requirements for digital capacity will continue to mushroom without limit, placing recurring pressures upon service providers and technology suppliers to keep pace.

The most fundamental effects of this new era of human interaction, however, will be far more difficult to measure or predict. We have entered an epoch in which physical and authoritative boundaries on information sharing are no longer relevant, in which non-hierarchical knowledge diffusion is becoming the dominant paradigm. In the early 1960s, the father of media analysis, Marshall McLuhan, defined the concept of the "Global Village," to represent the impact of mass media in bringing disparate cultures together into a common worldview. The reach of technological development since McLuhan's time has only intensified this effect, linking the consciousness of billions of individuals, allowing their thoughts, ideas, beliefs, experiences, and collective wisdom to be shared universally, and democratically.

7.2.4. Self-Regulation and Netiquette

In a world where every user is also a provider of information, where does the responsibility fall to regulate, and otherwise oversee all of this multilateral communication? Public authorities, of course, will always have a key role to play in setting boundaries and responding to the most serious and far-reaching challenges, as the further sections of

this chapter describe. But in the most practical sense, a large portion of the converged, ubiquitous, user-dominated communications universe actually functions rather effectively through self-regulation: of the users, by the users.[21]

On one level, self-regulation takes place within the management of the business entities that facilitate unfettered user interaction. Given that commercial success in these realms depends primarily on popularity and reputations, which can spread and change like wildfire in cyberspace, most not operations are acutely sensitive to prevailing customer attitudes, and are often prepared to adjust their practices based upon popular opinion. As huge as it is, Facebook has more than once backtracked on attempted policy changes regarding customer privacy in response to outcry from users. Service providers also may work voluntarily with law enforcement and regulatory authorities to address public interest concerns, even if they are not legally bound to do so. Several U.S. telephone operators controversially cooperated with Bush administration wiretapping and data access requests in the post-9/11 period. And the large online classified advertising service Craigslist agreed to cut back on "erotic services" (i.e. prostitution) ads, following high-profile abuse and murder cases.

Netiquette

Even more prevalent, however, has been the emergence of unofficial, collective standards of conduct, and mechanisms for enforcing them, throughout broad segments of the user-dominated online world. In effect, a form of frontier democracy has taken hold, defined and constantly modified by the implied consensus of countless millions of activist users, for their own self-interest: to enhance the quality of their virtual lives. Sometimes known as "netiquette," or community moderation, the terms and methods of this self-governance may vary from site to site depending on the nature of the service and its most enthusiastic participants.[22] One generally common feature is to allow participants to rate or vote on each others' contributions, which yields relatively democratic rankings of the most appealing inputs, while downgrading and even censoring the most disapproved content. This type of rating system is used by all kinds of blogs, movie and book review sites, travel and tourism portals, as well as a preponderance of news media, which invite commentary on published stories from virtually any reader (often with a result of thousands of flame-filled epithets). The Internet has sometimes been compared with the "wild west", and it is nowhere more vigilante than in the shootouts over community rated online content.

Just the FAQs

The Internet has also evolved an unprecedented system for distilling facts from fiction, or at least for giving users the greatest possible basis for deciding for themselves what to accept as "truth". It is the ultimate realization of the concept of the "marketplace of ideas," which has motivated philosophers from Socrates to John Milton to Thomas Jefferson and John Stuart Mill. Although the Internet is overflowing with wild claims, conspiracy theories, and unending debates on virtually every subject, no assertion of any interest goes unchallenged by other, competing viewpoints. In all serious forums, there is a general requirement to substantiate most factual claims with supporting documentation (typically in the form of hyperlinks to outside, trusted sources), and a broad philosophy prevails that, as Carl Sagan once said, "extraordinary claims require extraordinary evidence". For every urban legend, for every persistent "meme" (an idea that takes on a life of its own), there are innumerable investigations seeking to verify or debunk the underlying myths.

By the same token, the Web offers limitless sources of information for those in search of answers or advice, again with the aid of self-regulation to help the most useful data to rise to the top. There are innumerable web sites whose mission is to provide information on every conceivable topic, typically for no charge. In addition to the intelligent search functions of Google and other search engines, and the rigorously moderated fact mine of Wikipedia, there are How To, Ask, Answer, How Things Work, Infoplease, AskMe, AskDeb, Mahalo, and hundreds of other locations where users both ask the questions and provide the answers to a limitless range of factual, self-help, research, trivia, and basic knowledge queries. At a somewhat more professional level, numerous sites also invite lawyers, doctors, designers, tax accountants, and other specialists to provide advice (albeit without liability) on generic and user-specific topics in their fields. In nearly all cases, users have the opportunity to rate, rank, and respond to the information given through these channels, again allowing the most effective and valuable (usually) to penetrate to the surface.

New Gatekeepers?

Despite the decentralized, populist self-regulation of the Web 2.0 era, there are nevertheless reasons to remain vigilant against the emergence of new types of bottlenecks and gatekeepers, which could skew the control of information away from the user masses. As some Internet business models prove overwhelmingly successful, their ability to dictate the means by which users can access and share information could rise above those users' ability to maintain control even of their own virtual identities. A Facebook or a Google, for example, could systematically promote or exclude certain viewpoints, vested interests, or especially competitors, with little recourse beyond vociferous protest for their dependent customers. Similarly, technology and network gateways may re-emerge, in the form of those who dominate the development of operating systems, programming code, even end-user equipment. The debate over net neutrality (see Chapter 7.5) represents one legitimate area of concern about vertical integration, even in this era of decentralization.

Self-regulation, therefore, will always need to be complemented and reinforced by public sector regulation: not to reclaim dominance by the state from the will of the masses, but to ensure that the masses are continually able to express their will as robustly as possible.

7.3. Regulating Digital Content

Regulation of content in the digital world is a new challenge not typically part of the traditional telecommunications regulator's role, typically limited to broadcasting and print in the past. Most agree that some limits are necessary, but defining and enforcing them are huge challenges.

7.3.1. First Principles: How Much Freedom of Expression?

In the case of the fundamental practices of human communication, the world's governments have long acknowledged that free expression and access to information are among the most basic rights that all societies and persons should share. Article 19 of the United Nations *Universal Declaration of Human Rights* states:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.

The World Summit on the Information Society reaffirmed these rights in 2003 and 2005, and added further principles relevant to modern digital communications:

> Communication is a fundamental social process, a basic human need and the foundation of all social organization. It is central to the Information Society. Everyone, everywhere should have the opportunity to participate and no one should be excluded from the benefits the Information Society offers.

These principles actually imply several related practical rights for citizens:

- Freedom to speak what they believe, publicly, without fear of reprisal;
- Freedom to write and publish their opinions without censorship;
- Freedom to communicate with anyone, by any means, anytime;
- Opportunity and ability to access any information, to learn and gain knowledge from any source;
- Right to know: access to government information files.

Nevertheless, all societies place some limits on citizens' rights to free expression and information, and the challenge to define the proper place for those limits is one of the critical issues of the new communications era.

Technologies of Freedom

One of the most prominent early analysts of social transformations in the information society, Ithiel de Sola Pool (who first coined the term "convergence"), raised important concerns about the regulatory limitations that might be placed on new communications technologies:

> The onus is on us to determine whether free societies in the twenty-first century will conduct electronic communication under the conditions of freedom established for the domain of print through centuries of struggle, or whether that great achievement will become lost in a confusion about new technologies.[23]

The revolution in ICT since the early 1990s has dramatically surpassed anything that even de Sola Pool anticipated, and the potential effects on social and political freedom and democracy are proving vastly more significant. In many respects, the forces

unleashed by the Internet and other new media have allowed greater freedom of expression across a wider expanse of human society than was ever possible in previous eras.

From another perspective, it is also clear that openness, free expression, and democratic choice have a strongly positive impact on economic and social opportunity and development, including development of the ICT sector itself. In countries where the ICT industry has been encouraged to grow and diversify through relatively unrestrained competition and open-ended market entry, the industry and the national economy have thrived. The examples of Facebook, Google, Yahoo, and other open forums that encourage nearly all forms of expression demonstrate the economic value and social popularity of limitless communication in virtually any society. The explosion of mobile phone usage – voice, text, and images – and the revenues generated by these services, reinforce the fundamental observation that communication has tremendous value to all people, everywhere. The more they are able to take advantage of the technologies of freedom, the more they seek and embrace them.

Freedom of Information

Beyond freedom to express oneself and to access all forms of information and communication, there is a particular class of freedom of information that is centrally important to civil liberties advocates. This is the citizens' "right to know" about information obtained and held by their own government in a democratic society. This right implies several obligations on the part of governments: that they maintain and make available all relevant information (aside from that classified for legitimate national security or privacy purposes); that they provide such information upon request to citizens, journalists, and other interested parties, in formats and within time frames that are reasonable; and that they take pro-active measures to inform and assist citizens with obtaining such information. Numerous governments and international bodies have endorsed this principle of information access by citizens. The United Nations Special Rapporteur on Freedom of Opinion and Expression, for example, issued a report expressing the view that the human rights provision "imposes a positive obligation on States to ensure access to information, particularly with regard to information held by Government in all types of storage and retrieval systems - including film, microfiche, electronic capacities, video and photographs…".[24]

A highly controversial recent example of this issue occurred in 2010 when the self-designated international "whistle-blower" organization, Wikileaks, which takes an aggressive stance in favor of full disclosure of government secrets, managed to obtain thousands of pages of classified U.S. Pentagon documents concerning the conflict in Afghanistan. The U.S. government and many of its allies denounced the leak of these materials in terms as strong as were used during the Vietnam era, when publication of the Pentagon Papers raised some of the same vital questions. Defenders of the revelations of government secrets during wartime, then and now, claimed that citizens' right to know is, if anything, more essential with respect to decisions about war and peace than any other subject. In practical terms, the documents' publication mainly served to refuel the already intense global debate, across all media forums, concerning the war, the clash of cultures, democracy, and technology.

7.3.2. The New Age of Broadcasting: The End of Scarcity?

Broadcasting of information and entertainment via radio and television has been the foundation of modern mass communication for nearly a century – and often the center of controversy over content regulation. For much of the broadcasting era, the majority of countries tended to tightly control messages and images sent over the public airwaves. This was most often accomplished through direct state ownership of broadcast stations, whose programming was either implicitly or explicitly guided by political considerations above all else. Such state-run broadcasting services, many of which continue their mission to this day, may be quasi-independent in their editorial discretion and essentially benevolent in operating philosophy, but it is difficult to escape perceptions, and often reality, of propaganda when a government ultimately monopolizes the mass media.

Spectrum as a Scarce Resource

Still, even in those societies where private commercial broadcast outlets are allowed and encouraged, regulations governing radio and TV content have been commonplace throughout the history of the medium. Such regulation has been justified by physics. The scarce resource of the spectrum has been widely considered to belong to all

the people of each society, to be utilized for their collective benefit (See Chapter 4). Calculating this benefit is a matter of balancing socio-political and economic considerations. In practice, it has meant everything from children's educational programming to scientific documentaries to international news reporting to daily prayer recitals, depending upon the country. At the same time, governments have sought to restrict broadcasting of what they view as undesirable content, recognizing that anything sent over the airwaves can be received by anyone, including impressionable children, disgruntled citizens, and influential power-brokers.

The key question for the new world of converged and unlimited media is whether broadcasting still merits its special regulatory status. The laws of physics haven't changed. However, the unique role of broadcast signals is rapidly disappearing amidst the deluge of alternative content sources and transmission media. This is especially true of television, since radio broadcasting retains a somewhat more unique place as the primary (but not exclusive) mobile mass medium, particularly for hundreds of millions of automobile drivers. Broadcast TV stations, however, are becoming indistinguishable from – and often integrated with – countless other video-based media sources. The number of viewers who still rely solely or primarily upon over-the-air signals for their electronic information and entertainment is dwindling fast: already a small minority in most of the developed world, and limited mainly to rural audiences in most developing countries. This lifeline status for rural broadcasting certainly merits maintaining support to continue sending signals to these communities, but may not justify an entirely distinct regulatory structure, especially regarding broadcasting content.

Harmonizing Broadcasting Regulation

If broadcast programming should no longer be subject to separate regulation, the key question is: should traditional regulation of TV and radio stations be extended to audio-visual content on other media, or should existing regulations be removed or streamlined to fit broadcasters within the more open-ended regimes applied to other 21st century networks?

Some relics of the broadcasting era would be difficult or impossible to apply to the Internet, cable and satellite TV, etc. These include, for example, "fairness and equal time" provisions, which try to mandate balanced coverage of alternative political views: there is no way to measure or otherwise evaluate the infinite mix of political expression in cyberspace. Similarly, TV and radio have often been subject to diversity and domestic content obligations: neither is practical, nor necessary, in the digital content world, although there should be nothing wrong, in principle, with a government helping to support production of material that it views as socially desirable. Restrictions on "indecent" or other objectionable content may also be next to impossible to apply outside of the traditional broadcasting realm.

On the other hand, it is possible to consider developing a standardized regime to apply across all forms of audio-visual media that are distributed to the public, regardless of the source of transmission or means of access. This is what the European Union has introduced, through its *Audio-Visual Media Services Directive* (AVMSD),[25] which provides for coordinated legislation throughout the EU on a range of AV media issues, applying both to traditional broadcasting as well as to AV signals distributed through other means (See Box 7.1).

7.3.3. What to Regulate: The Dark Side of the Web

Every leap forward in our ability to communicate with each other, to share information and ideas, has inevitably been accompanied by advanced methods of deception, exploitation, and abuse, pioneered by the darker elements of every society. One glaring drawback of the ubiquity and dominance of digital ICTs is that the newest waves of such unfortunate practices are vastly easier to create and disseminate, and vastly more difficult to hide from the most vulnerable targets (see Figure 7.4).

Some of the most destructive digital content is unique to the cyber world: viruses and worms and spam and malware, which infest and depend upon the digital code itself; these are addressed in Chapter 7.7.3. Other nefarious content, however, is as old as papyrus. Societies have been wrestling with the challenge of drawing boundaries and enforcing collective standards of morality and propriety around various forms of human indulgence for millennia. Now in the digital era, it increasingly falls to regulators to carry on this often futile quest.

Box 7.1 Key Provisions of EU Audio-Visual Media Services Directive

Technological neutrality: Applies to all AV content regardless of medium, but distinguishes between *linear* (broadcast) and *non-linear* (on-demand) programming.

Prohibition of incitement to hatred: Authorities must ensure that AV content does not contain incitements to hatred toward persons based on race, sex, religion or nationality; this applies to content provided within the EU as well as delivered from outside, such as via satellite.

Commercial communications: There are a variety of protections regarding commercial advertising within AV content, such as requirements that actions such a product placement and sponsorship be recognizable and not subliminal or surreptitious, not promote discrimination or unhealthy behavior (tobacco and prescription medications are specifically forbidden).

Protection of minors: Differential rules regarding content which might "seriously impair the physical, mental or moral development" of children (banned from broadcast, restricted with on-demand services), and which is "likely to impair" minors (restricted on broadcast, not regulated in on-demand). Programming which falls into these categories expressly includes pornography and gratuitous violence.

Accessibility for people with disabilities: AV services must take measures to ensure their programming is accessible by visually and hearing impaired persons.

Major events: Broadcasters generally cannot obtain exclusive control over transmission of "major events" (sport championships, coronations, inaugurations, etc.), which would prevent large segments of the public from watching them.

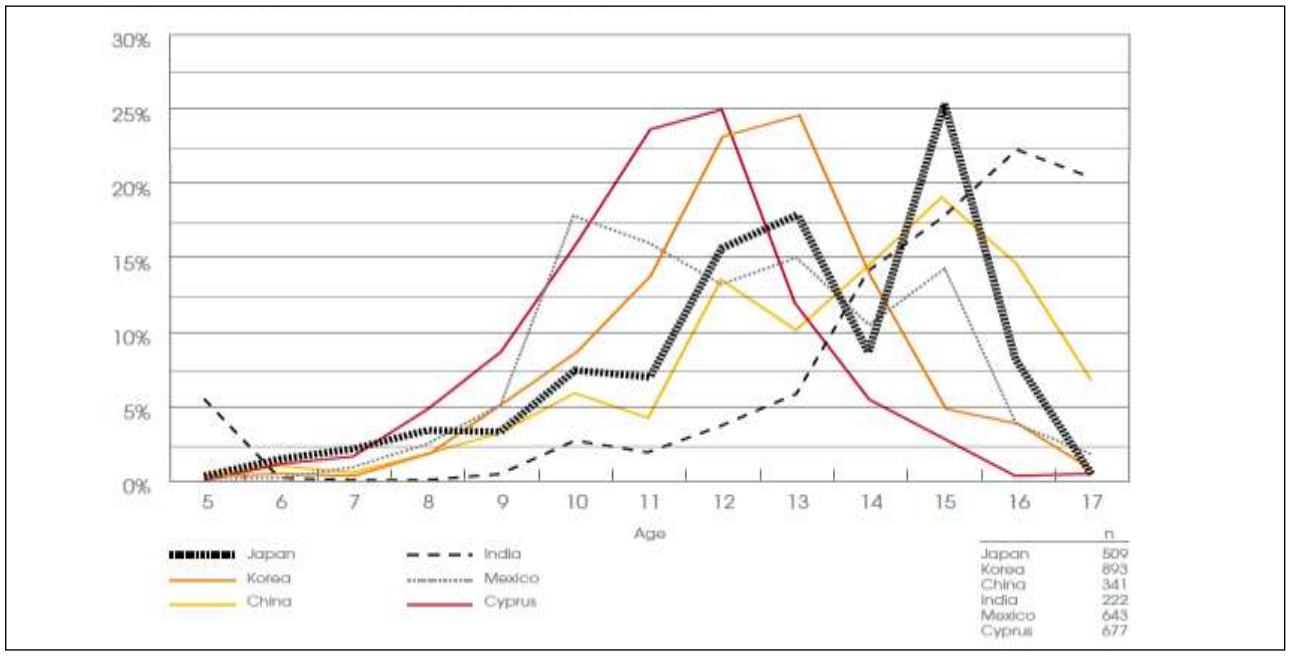
Promotion and distribution of European Works: EU broadcasters and other AV media outlets must help promote and distribute European Works, i.e. programming developed by Europeans, through various proactive means.

Source ICT Regulation Toolkit.

This is an area, however, where it is extremely difficult to define any kind of international consensus as to the appropriate limits of free expression. Different cultures, and hence different governments, exhibit widely varying degrees of sensitivity to certain types of dubious activities. It is safe to say, however, that large segments of most populations are at least uncomfortable with some of the most extreme examples of disreputable digital content. Among the most widespread of these challenges are the following:

- *Pornography, Cyber Sex:* Absolutely forbidden in some countries, utterly unrestricted in others, controversial regardless, the vast digital sex industry somehow generates many billions of dollars in revenue worldwide each year. Measures to at least quarantine online porn – e.g., through a .xxx top-level domain – have to date proven ineffective, leaving government authorities, school administrators, and parents to resort to filtering and monitoring techniques (see 7.3.4), also with limited effectiveness.
- *Hate Speech, Incitement to Violence:* Even more difficult to define and problematic to restrict in a democratic society, there are nevertheless myriad cases where governments have determined that various forms of hate-mongering, incitements to violence, conspiracy and criminal or gang related communications should be restrained by law. This category can also include incitements to rebellion or sedition against the state, an area that is difficult to segregate from legitimate political dissent.
- *Gambling:* Another highly controversial, and popular, online pastime, Internet-based gambling is banned or heavily regulated in many countries as either immoral, potentially corrupt, and/or economically damaging. Off-shore gambling sites continue to thrive, however, through hosts that are based in countries with less to lose and much to gain (in tax revenues) from the practice. Although it is technically illegal for citizens of many countries to utilize these foreign digital casinos, this is another area that is virtually impossible to police effectively.
- *Child Exploitation:* Virtually every civilized society agrees that abuse and exploitation of children is unacceptable and should generally not be protected even by free speech principles. This includes child pornography, even where adult pornography is tolerated, and any other coercion or misuse of children's images or identities that may compromise their safety, development, or innocence. In the Internet world, further protections are also needed to shield children from predators who may contact them through deceptive enticements in online forums. For many governments and law enforcement agencies, this area may represent the highest priority of prevention, investigation, and prosecution, given the vulnerability of the victims and the scope of the perceived risk they face.

Figure 7.4 Starting Ages of Having a Mobile Phone



Source: GSMA and NTTDOCOMO, 2010.

- *Cyber Stalking:* Many authorities have begun to recognize cyber stalking as a new and very real threat to Internet users, especially the young, the mentally ill, and other vulnerable groups. Cyber stalking occurs when one or more antagonists deliberately and aggressively harasses a victim through a combination of public media, for purposes of intimidation, vengeance, outright hatred, or mere amusement. Actions can include continuously posting abusive comments on social networks; posting compromising photographs (real or altered); circulating SMS and images; sending repeated insulting or threatening e-mails and voice messages; and spreading malicious rumors through a variety of media, among many other examples. There have been several high-profile cases of cyber stalking victims committing suicide, and other grave effects, sufficient to compel legislators and regulators to identify this new form of harassment as needing special attention.
- *Fraud, Scams:* The realm of e-commerce requires its own set of extensive legal and regulatory requirements, adapting the complex systems developed over centuries for traditional commerce. One area of particular concern is the proliferation of outright fraudulent practices and scams perpetrated on the Internet, via e-mail, and even through telephone services. There are countless examples of false web sites set up to sell non-existent products and services to unsuspecting customers, as well as other schemes such as pyramid or Ponzi style multi-level, get-rich-quick deceptions. Ubiquitous spam, of course, is a worldwide scourge (see Chapter 7.7.3). In many cases, these scams may be difficult to identify until after people have been defrauded, and the international nature of the Internet makes it vastly more difficult to track down perpetrators. At least in some cases, however – such as the ever-present and painfully obvious Nigerian 419 scam[26] – it would seem that more aggressive cooperation and intervention on an international scale should be able to clamp down strongly on these most predatory and ultimately amateur of swindles.

Each of these areas of potential abuse can require an entire body of legislation, case law, regulations, enforcement standards, and intervention criteria, and there will always be countless borderline cases that

test the underlying assumptions and objectives of such rules. Attempting to draw fine lines around human behavior has never been an easy task.

7.3.4. How (and Whom) to Regulate: Challenges of Policing Cyberspace

When policy makers decide that restrictions, obligations, and sanctions should be established relative to various forms of digital content, they need to take into account the practical options for enforcing these mandates. The truth is that, in the highly advanced technological landscape of computer software and telecommunications networking, there are few effective options for restraining certain specific types of transmissions, and none that can be even close to 100% reliable. Not only are these measures seeking to identify and segregate a tiny fraction of bytes out of trillions being sent and received every day, but they are seeking to penetrate the messages, web surfing, and communication habits of potentially millions of private citizens, to modify and inhibit their personal behaviors. The more successful the communications revolution in a given society, the harder it is for government, or anyone, to control how that revolution plays out in the lives and perceptions of the people, for better or worse.

Prior Restraint, Censorship

In societies with strong free expression rights, the practice of "prior restraint" represents the most extreme form of intervention against any potential speech or publication, and most the difficult to justify legally. Prior restraint is tantamount to outright censorship, before the fact: i.e. preventing a speaker from speaking at all, when the subject matter is anticipated to be prohibited.

In the case of the Internet, it may be impossible to literally prevent the creation of objectionable content, but the closest equivalent of prior restraint is to block users from accessing such content. This can only be accomplished by a system of filtering web access, which requires placing such filters strategically within the network of web servers that connect a given group of users to the Internet. Such a system is relatively straightforward, for example, for a school or a business or government office, which utilizes a local area network and a single server behind a firewall, through which all connections must pass. The filtering system can be installed on this server, containing algorithms for preventing access to designated web sites, e.g., those with obscene or hate-filled content. The difficulty, of course, is defining and identifying the prohibited content, and maintaining up-to-date registers of URLs that are to be censored.

When applied at a country-wide level, this challenge is far greater, as the filters must be applied simultaneously to all web servers of all Internet Service Providers. This requires a degree of state control over the country's entire Internet industry, whether through enforced cooperation of commercial ISPs, or even direct state monopoly ownership of the ISP sector. While such a policy can be relatively effective in limiting public access to outlawed web content, much of the material will still inevitably slip through – while some inoffensive content will be accidentally blocked as well – and the required development, maintenance, and control of ISP web filtering imposes substantial costs on the industry. Nevertheless, this method of Internet censorship is applied with considerable effect in many countries, especially to restrict access to pornographic sites, among other objectives.

Investigation, Deletion, Prosecution

An alternative to prior restraint and filtering is for authorities to approach the problem of illicit digital content in the same manner as other lawbreaking activity: investigate alleged violations, intervene and stop (delete) the prohibited action, arrest and prosecute the perpetrators. Although this approach will undoubtedly allow a much larger amount of unwanted content to be accessible, ideally the threat of prosecution will deter most potential violators.

A critical aspect of this form of enforcement is to identify the appropriate persons or companies to hold accountable for the offensive material. Should ISPs that host web sites which contain illegal content be responsible for policing their servers? Should open forum and social networking services exercise censorship over their users? Or should only the individual poster or commenter, possibly likely hiding behind an anonymous ID, be liable for his or her words and actions? And should ISPs and providers of services such as Facebook be obligated to help law enforcement root out offenders, by providing access to identifying source code and addresses?

The greatest difficulty with this method, however, is that there are no national jurisdictional boundaries, and much of the most objectionable material is likely to be hosted on servers outside of the countries

whose laws prohibit it. International cooperation can help with the most egregious abuses, but there is unlikely to be a strong consensus on banning and eradicating most categories of purportedly offensive content, because national definitions of what constitutes offensive content differ and are often culturally specific.

Cooperation

Another alternative approach, and preferable where possible, is to encourage cooperation between information service providers, government authorities, and citizens themselves, to police and uncover illicit and harmful media content. In some cases, this may require a degree of public pressure and negotiation. This was the case with the classified advertising service Craigslist, which finally agreed to remove its "erotic services" listings, which had become a *de facto* forum for prostitution, only after extensive negative publicity and pressure from police and politicians. In the case of cyber stalking, some jurisdictions have passed legislation to require authorities, such as school administrations, to report and investigate allegations of harassment and stalking when they learn of them. In all cases, however, the challenge remains difficult, both to identify where the line should be drawn between acceptable and unacceptable content in a free and democratic society, and to devise effective and non-excessive means to prevent and eradicate the worst offenses. Again, the international nature of these networks requires global cooperation on the most egregious and widespread abuses, which implies participation among governments, law enforcement, corporations, and even users themselves.

7.4. Balancing Intellectual Property Rights

"Intellectual Property" (IP) refers to the intangible value of products that emerge from the creative human mind. Governments have recognized a need to protect the rights of those who create from those who merely copy or steal for more than a century. In the digital age, there are difficult balances to strike between ensuring those rights when electronic copying is easy, while many of the owners of IP are among the most powerful corporations in the world.

7.4.1. Copyright Protection: Combating Piracy on the Digital Seas

The global markets for computer software, film and television recordings, computer and video games, and recorded music are almost immeasurably vast. Estimates vary widely as to the overall size of these markets, but annual global revenues are at least in the range of $300-billion for software, $50-billion (and growing) for electronic games, $25-billion for home video, and $15-billion (and shrinking) for recorded music (CDs plus downloads), or close to $400-billion worldwide each year. [27] Such a huge treasure chest would not likely escape the notice of thieves and pirates in any era, but in the digital age, the opportunities to steal and profit from these forms of intellectual property are unprecedented.

Throughout modern commercial history, the creative segments of society – those who write books, compose music, and produce original designs of all kinds – have been protected under the legal principles attached to intellectual property: copyright, patents, trademarks, etc. These principles state that creators own their original works, and are allowed to sell and market them exclusively as they see fit, and that unauthorized parties cannot reproduce or forge and sell copies of such works without compensating the original source. In the computer era, these protections extend to authors of software programs and operating systems, as well as to the electronic versions of all traditional and new media. Unfortunately, in a world where the technology to make virtual exact copies of any digital file is within the hands of the simplest computer user, maintaining these principles has become one of the most difficult challenges of all.

Losses due to Piracy

The value of industry losses resulting from digital piracy is itself a matter of considerable controversy, but by any measure the sums are immense. While it is possible to estimate the order of magnitude of unlicensed software and unauthorized copies of media in use in various countries, it is far more difficult to determine how many of these pirate versions would actually have been sold if the users had to pay full retail prices. This is especially the case with the lowest income countries, where piracy is most widespread in terms of the percentage of illicit versus authentic uses. Unless rights owners were to offer their products for a fraction of their prevailing international prices, it is likely that most private users, and even most companies and governments in these countries (which also frequently use pirated software) would be unable to purchase more than a fraction of the material that they currently obtain through the black market.

With these caveats in mind, the international software industry estimates that the value of its losses from digital piracy are in the range of $50-billion per year.[28] According to industry claims, there are more than 25 countries in which over 80% of the software in use is unlicensed or unauthorized, and in countries such as Bangladesh, Georgia, Moldova, and Zimbabwe, the proportion is claimed to be over 90%. Clearly, the incentives and resources needed to enforce the copyright laws that are usually on the books in many of these countries are not very high, especially in comparison with the perceived value that many users and governments receive from not paying market prices for software. Even in the most developed countries, however, illegal software copying is commonplace, and the economic impacts can be greater, as manufacturers and retail sales outlets lose customers to pirates. Estimates of losses for other media such as DVDs and video games are even harder to come by; by one measure, there are 600-million pirated DVDs in circulation in India alone.[29] There is no other illicit enterprise in the world of anywhere near the same magnitude.

Critics of the software giants such as Microsoft, IBM, and Oracle, as well as game makers Nintendo, Electronic Arts, and others, claim that these companies drastically overprice their products and thereby drive users toward piracy. Some activists have taken strong political stands against the increasing global dominance of such firms, highlighted by the formation of the Pirate Party in Sweden in 2006, and similar parties in other countries, which favor extensive reform of copyright and patent laws to allow more widespread (non-commercial) sharing of copyrighted material, as well as strong measures to protect citizen privacy and open access to government files. In 2009, the Swedish Pirate Party had gained such prominence that it gained two seats in the European Parliament elections. It also became the host site for the servers of Wikileaks, the international group dedicated to exposing government secrets.

International Law

Piracy has always been fundamentally an international challenge, far more so in today's information society. All software markets are global in nature, and the Internet permits instant access to and transfer of any files, anywhere. In theory, a cartel of digital thieves, decoders, copiers, and distributors could be based across dozens of countries, and could conduct most of their operations without ever meeting in person. Indeed, a large amount of illicit software exchange does take place through services such as Warez and a variety of BitTorrent and peer-to-peer sharing sites. Many of these services tend to be driven less by profit motives than by the ideologies behind electronic file sharing and open source software (see next section). On the other hand, there are also many subscription and purchase-based sites that will provide low-priced downloads of pirated software.

A large portion of the for-profit piracy market, however, involves sales of physical media: counterfeit copies of DVDs, packaged operating system and applications software, video game discs, and the like. Often these are produced by small distributors in open "grey market" shops in locations where enforcement of IPR laws is lax at best: retail customers may browse catalogues of movies, music, and software, place an order, and simply wait while the illegal copies are burned to discs from the master files. Those master copies, however, and many thousands of mass-produced counterfeit discs, are made in a smaller number of major pirating factory locations, run by well-organized and sophisticated operations, unknown to or left alone by authorities in discreet locations in Brazil, China, India and the Russian Federation, and a number of other countries.

Governments and international organizations have developed strong agreements as to the need to address intellectual property rights violations, and these have been embodied in a series of treaties as well as national legislation around the world. These agreements date as far back as 1886, when the Berne Convention first established reciprocal copyright protection among major European nations; this was followed by a wider agreement in 1952, including the United States and most of Latin America, known as the Universal Copyright Convention. In 1967, the United Nations established the World Intellectual Property Organization (WIPO) as a specialized agency to coordinate international policies on IPR.

WIPO's stated mission is to develop "a balanced and accessible international intellectual property system, which rewards creativity, stimulates innovation and contributes to economic development while safeguarding the public interest." It is responsible for administering dozens of international treaties, and has taken the lead in drafting legislative language and proposals for

national governments to adopt in pursuing a standardized global approach to copyright issues, among others, including the WIPO Copyright Treaty. This treaty has been reinforced through global trade negotiations under the World Trade Organization (WTO), resulting in the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), which provides a detailed set of conditions and responsibilities for member states to adopt to protect copyright and other intellectual property within their borders, and cooperatively across borders.

Many governments have thus adopted, in whole or in part, the main provisions of the WIPO and TRIPS directives, creating an increasingly harmonized international regime for defining and protecting intellectual property rights. In some countries, legislation has expanded upon the WIPO standards to add further clarity and specificity of rights and obligations. The United States Digital Millennium Copyright Act, for example, incorporates liability limitations on ISPs and online service providers, allowing them to block suspected copyright infringements upon demand by rights holders, and granting immunity if they follow the law's provisions, even where violations ultimately occur.

The EU has adopted the WIPO standards in its *Copyright Directive*, and similar liability protection in its *Electronic Commerce Directive*. However, there have been strong differences of opinion among members of the European Parliament over how to strengthen anti-piracy laws and regulations. The more stringent proposals would adopt a so-called "Three Strikes" rule, which has already been controversially passed in France.[30] This approach calls for cutting off the Internet connections of users who are caught illegally downloading copyrighted content three times, for as much as a year. Opponents have argued that such disconnection is extreme, and that in the current era Internet access is a fundamental human right. Alternative proposals would focus on web sites from which such downloading occurs, allowing judges to shut them down if they are proven to facilitate copyright violations.

Industry Policing Efforts

To a great extent, the private software and entertainment industries themselves have taken the lead in trying to control and reduce digital piracy, using both technology and litigation, including financial and investigative resources that most government enforcement authorities would never be able to allocate to this type of crime. Technological barriers to illegal copying have included various forms of encryption and Digital Rights Management (DRM) mechanisms, which can prevent at least the most widespread and amateur attempts at piracy, but have often been easily bypassed by organized media copying experts.

Across the industry, all of the major corporate players have taken strong steps and allocated substantial funds to press the fight against piracy losses. Several industry associations have taken lead roles in this quest at the national and global levels:

- The Business Software Alliance (BSA) is the largest and most international IT industry group, with policy, legal and/or educational programs in 80 countries. While several of BSA's initiatives are global in scope, most of its policy, legal, and educational efforts are led and conducted at the national level, with a growing emphasis on emerging economies. The BSA employs a range of programs to further the anti-piracy objectives of its members, including:
  - Investigation and enforcement of allegations of copyright violation and software piracy, including filing lawsuits;
  - Online tracking of Internet sites containing pirated software;
  - Software Asset Management (SAM), which assists companies in complying with software licenses;
  - Education initiatives to publicize and raise awareness concerning software piracy.
- Business Action to Stop Counterfeiting and Piracy (BASCAP), an agency of the International Chamber of Commerce. BASCAP takes international initiatives to connect companies and pool resources to address counterfeiting and piracy issues in multiple industries. It also lobbies governments to establish and enforce intellectual property rights laws.
- The Recording Industry Association of America (RIAA), which has taken the lead role in combating unauthorized digital music downloads and file sharing (see Chapter 7.4.2).

These and other industry enforcers, out of their own self interest and of necessity given the scope and complexity of the digital piracy problem, will have to remain on the front lines of this struggle, and themselves become vulnerable to hacking or denial of service attacks. It is their profits that are mostly at stake, while governments are in the uncomfortable position, in many cases, of seeking to balance the need to enforce the law with the cold realities of a very widespread set of practices that often arguably benefit their own populations more than they may harm the domestic economy.

7.4.2. Digital File Sharing: Peer-to-Peer Rights and Wrongs

The objections to outright theft and resale of copyrighted material are relatively easy to grasp, and the economic harm to rights holders, while debatable in magnitude, is certainly very real. The realm of digital file sharing, by comparison, is not so easily navigated.

Copying and sharing of popular media, especially music recordings, has been a common practice since the introduction of cassette tape recorders. With the introduction of digital audio tape (DAT), the U.S. recording industry persuaded its Congress to adopt the *Audio Home Recording Act* in 1992, which established a number of legal precedents for the copyright issues of the emerging digital era. Among other provisions, the law required manufacturers of DAT devices to include specific copy protection technology, and also mandated an implicit royalty payment be charged for each DAT tape sold, with funds going to the recording industry, on the presumption that at least some of the purchases were being used in place of new recording sales. The Act also included new protections, however, for private users who record audio tapes for their own, non-commercial purposes.

The File Sharing Boom

The practice of digital file sharing is also well established, dating to the earliest days of the Internet, when BBS and UseNet bulletin board users would post digital copies of their music collections for free download by like-minded fans. With the arrival of the iPod and MP3 formats of digital music, together with the spread of home PCs and broadband Internet connections, this fringe activity became mainstream, and created huge new challenges for the recording industry. Since a peak of almost $40-billion worldwide in 1999, recorded music sales declined by nearly 50%, with much of the loss ostensibly attributed to file sharing and/or direct piracy.[31] In the U.S., revenue from music sales and licensing dropped to $6.3 billion in 2009, from a total of $14.6 billion a decade earlier.

When first introduced, peer-to-peer digital music sharing was a uniquely imaginative invention, expressly designed to circumvent any claim of outright piracy by any organization, i.e. direct copying and distribution (for profit) of CDs and song files. The original service, Napster, in 1999 pioneered the innovative concept of facilitating direct sharing of MP3 music files by linking individual users' PCs to each other over the Napster network. Napster's main function was simply to permit members to search among the song lists of other members for recordings they wanted, then make the connection between the two for the duration of the download. In effect, each song transfer was a private non-paying transaction between two anonymous fans.

Immediately in Napster's wake, a number of other peer-to-peer file sharing services sprang up – Kazaa (which went on to become the foundation of Skype), Gnutella, Grokster, Morpheus, LimeWire, BitTorrent, Vuze, The Pirate Bay and many others – sending shock waves through the music recording industry, as hundreds of millions of users suddenly began exchanging digital music recordings for free, and revenues from CD sales plummeted. The ambiguous legal status of these unprecedented services has made it difficult for regulators, legislators, lawyers and courts to determine exactly how to respond: technically, individual users were simply trading personally owned files, and in many cases they were merely downloading digital copies of songs that they had already purchased in other formats (see Figure 7.5). But the reality was that a worldwide wave of free music access had been unleashed, with uncounted millions of copyrighted recordings landing on the hard drives and MP3 players of millions of users, and none of them paying royalties to artists or the music industry.

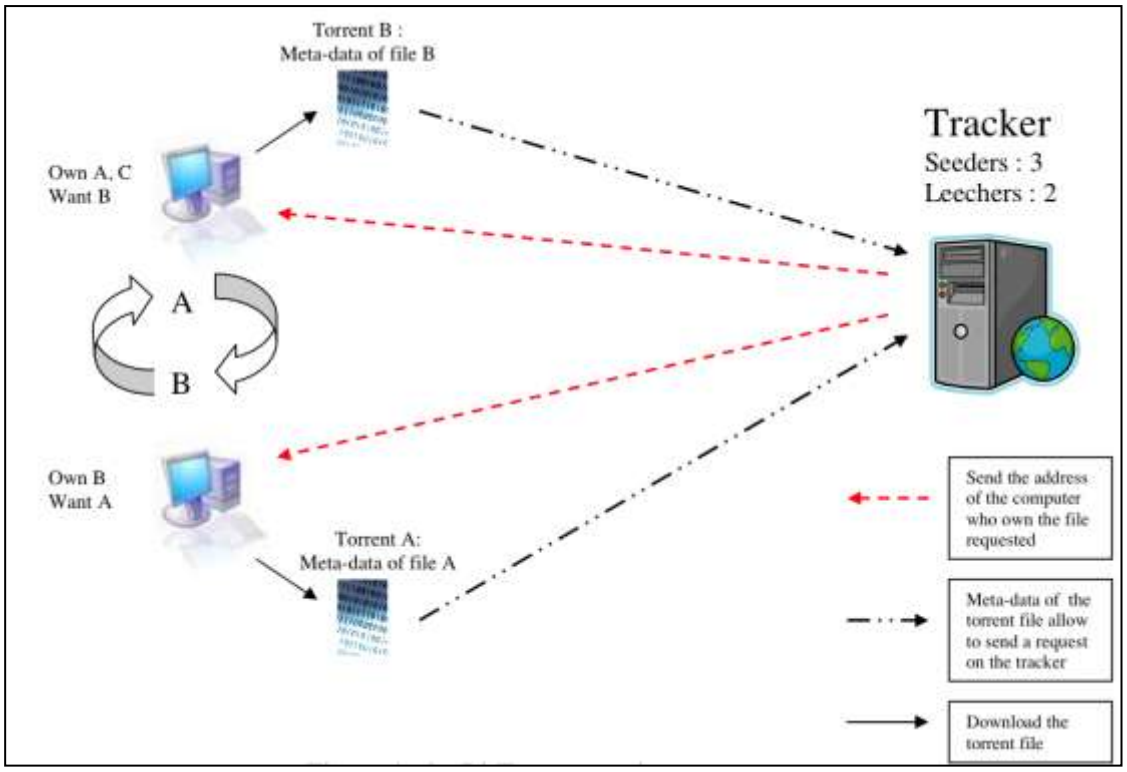
Industry Responses to File Sharing

As file sharing became a global phenomenon among music enthusiasts (and began spreading further, to sharing television shows, movies, and software as well), its methods and principles came under closer scrutiny. Ultimately, the established music business fought back, notably the Recording Industry

Association of America (RIAA) and its member recording companies. Beginning in 2001, the industry chose to file suit under existing copyright laws in the U.S., the U.K., Australia, and other jurisdictions against file sharing operations, and court rulings ultimately supported the contention that peer-to-peer file sharing, even where no money changes hands, is illegal and that services that actively encourage and facilitate such sharing can be liable for substantial damages. As a result of these lawsuits, Napster and other peer-to-peer networks were forced to cease operations, or transform themselves into paid subscription, royalty-paying online music services.

The problem of digital file sharing, however, was not at all eradicated as a result of these initial high-profile lawsuits, as new services continued to come online, not always in jurisdictions where the industry could readily shut them down. The RIAA introduced a second, more controversial tactic of pursuing individual users who had downloaded unauthorized recordings, winning and negotiating a number of litigations that resulted in fines of tens or hundreds of thousands of dollars. The industry's goal has been to intimidate illicit file downloaders, although critics have argued that the punishments are out of proportion to the crime, and have not had a material effect on sharing as a whole.

Figure 7.5 The BitTorrent Environment



Source: Dejean, Penard and Suire, 2010.

The industry's efforts are also hampered by disparities in laws and enforcement across different countries, which have created a safe haven for many digital sharing sites and users. In Spain, for example, a court ruled in early 2010 that file sharing peer-to-peer networks do not violate the country's IP laws, [32]effectively legalizing file sharing that had already been widespread; not coincidentally, Spain's market for official music sales, including opportunities for new recording artists, has plunged. Mexico, Italy, and other countries with less aggressive or non-existent file-sharing restrictions have seen similar declines in revenue from authorized music sales.

The Ongoing Challenge

Ultimately, the shifting trends in the music industry, and across electronic entertainment in general, imply that an entirely new paradigm for marketing, sales, and business strategy is emerging, which amounts to a philosophy of "if you can't beat them, join them". In February 2010, Apple reached the ten billionth legal, paid-for download from its iTunes Store, a

service which generated about U.S.$ 1 billion in 2009.[33] Still, file sharing and illicit copying and downloading remain rampant, as the music industry seeks to adapt to a new business model, which will undoubtedly involve continuing battles over copyright violation.

For governments, regulators, and law enforcement, the ongoing peer-to-peer sharing challenge represents a headache and a question about priorities. With industry forces taking the lead to try to disable the practice through litigation and their own investigations, public authorities with limited resources have to assess how much attention they should pay to this form of illicit activity. Some newer laws and regulations have attempted to place added responsibility on intermediary operators, such as Internet Service Providers. France and Ireland have sought to adopt the "Three Strikes" provisions that would go as far as to disconnect the Internet connections of repeat offenders of digital file sharing restrictions, and the European Parliament has wrestled with similar proposal. The Republic of Korea and other countries have adopted similar policies in recent years. Regulators can augment these provisions by establishing fines and other sanctions for licensed telecommunications operators and service providers that knowingly permit the hosting of illegal file transfer services, and potentially requiring disclosure of traffic data in instances of alleged abuses. But to date all measures have taken barely a small bite out of a worldwide practice that shows few signs of subsiding in the foreseeable future.

7.4.3. Consumer as Creator: Fair Use, Creative Commons

The flip side of defining boundaries and mechanisms to prevent harmful copyright violation is determining what constitutes acceptable, even beneficial, re-use of protected content. If the purpose of IPR restrictions is to ensure that creators – artists, authors, programmers, and the companies that back them – are appropriately compensated for their original works, then it generally follows that uses of those works which don't harm the learning potential of creators – and which may even actually help them – should not be unduly prohibited.

User-Created Content

Such may be the case with a wide variety of popular, creative activities that imaginative individuals in the digital age have introduced, spawning whole new forms of derivative art and entertainment (see Figure 7.6). One of the earliest examples was in the early hip-hop music movement of the 1980s, wherein artists included "samples" of others' recordings for background and rhythm effects; this was done on a fairly unrestricted basis until hip-hop and rap music gained mainstream popularity, whereupon recording industry attorneys began to require copyright compensation for music sampling.

With the proliferation of broadband Internet and user-originated content, new forms of sampling and adaptation of existing content are rampant. YouTube, for example, is overflowing with home-made videos that utilize technically copyrighted background music or video clips as creative fodder (notwithstanding the site's stated rules against copyright infringement). Parodies and re-imagination of popular books, movies, and other works are a favorite hobby of innumerable amateur authors and artists. The site FanFiction.net, for example, hosts several million fan-created stories based on thousands of well-known novels, films, television series, and *manga/anime* cartoons – there are nearly 500,000 variations on the Harry Potter books alone.[34] Moreover, virtually every successful production of popular entertainment soon generates multiple unofficial fan web sites (sometimes before the work is even released), which incorporate imagery, video and sound clips, text, character names, and all manner of original material copied from official sources.

Technically, nearly all of these activities constitute unauthorized use of protected material. In a few exceptional cases, authors and rights holders have in fact chosen to shut down sites that they deemed might be encroaching upon potential earnings from their own online projects, or that they perceived detracted from or demeaned their original work. But in the many cases, artists have recognized that these types of creative imitation often represent the highest form of flattery, and provide favorable publicity as well.

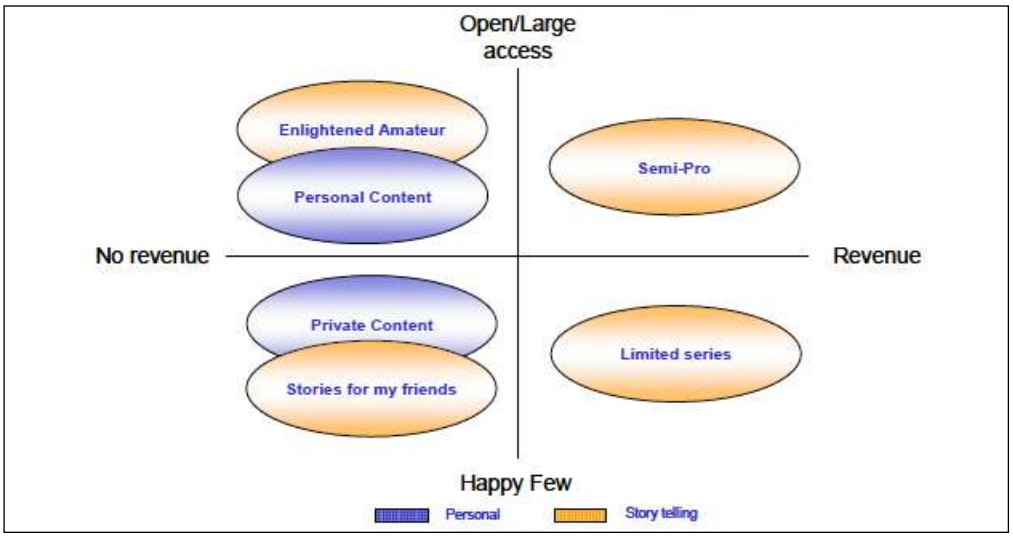
Fair Use Principles

In general, over the history of copyright law, the concept of "fair use" has evolved, to define the boundaries between acceptable adaptation or citation of protected works and copyright violation. Standards adopted under U.S. law and court rulings, which have been mirrored in a number of other countries, embrace the principle that portions of

copyrighted works may be reproduced for a variety of legitimate reasons, including criticism, comment, news reporting, teaching, scholarship, and research.

There is a four-part general test to help determine what constitutes fair use:

Figure 7.6 Main Characteristics of User Created Content Categories



Source: EU, User-Created-Content: Supporting a Participative Information Society, 2008.

1. The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes;
2. The nature of the copyrighted work (e.g., fact vs. fiction);
3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole;
4. The effect of the use upon the potential market for, or value of, the copyrighted work.

On the Internet, the fair use doctrine has become problematic for some news reporting organizations, for example: when unaffiliated sites can quote even small headlines and highlights of news reports, this may be all the information that rapidly surfing users need to keep up with current events. Hence, they may not "click through" the link to the original source, which will thus receive less traffic (and advertising revenue) for its original content.

Lawmakers have attempted to define the boundaries of fair use, and liability, for borrowed online content, with some difficulty. The U.S. *Digital Millennium Copyright Act* was amended to include a key *Online Copyright Infringement Liability Limitation Act*, which created what has become known as "safe harbor" for web intermediaries that allow others to post material which may be found to violate copyright. Under this provision, user-focused sites such as YouTube, Wikipedia, and Facebook are not liable for the postings of their members where copyrights may be infringed. The giant media conglomerate Viacom attempted to sue YouTube for $1-billion in damages due to countless unauthorized postings of Viacom-held intellectual property (video clips from TV shows, etc.) on the site, but lost the case (pending appeal) due to this safe harbor provision.[35]

Another significant response to the challenge of balancing IPR with the public's creative and imitative impulses is the non-profit organization Creative Commons. Founded in 2001, its purpose is to provide creators and would-be imitators with alternative licenses allowing free use of copyrighted works. Creative Commons licenses can be adopted by rights holders according to their preferred degree of permissible use: e.g., allowing any use with attribution, allowing only non-commercial use, or allowing only exact replicas without derivative uses. Wikipedia, for example, offers all of its content under a blanket Creative Commons license.

7.5. Neutrality of Access

The principle of "neutrality" has begun to take on central importance in the constant evolving and expanding ICT world. It is linked to the notions of democracy, populism, and decentralization that are hallmarks of the digital era: the idea that neither governments, companies, nor other gatekeepers should be able to dictate how anyone utilizes these technologies.

7.5.1. Net Neutrality: Clash of the Titans

The inevitable tendency among corporate strategists to seek competitive advantage and financial gain through market manipulation has raised alarm among a wide coalition of advocates for consumer rights, free speech, and Information Society principles of openness and equity. The ideal that proponents collectively advocate has been labeled "net neutrality". The basic concept is that the Internet should remain free of any discrimination or barriers among classes of users, or of information stored and transmitted on the Internet. In practice, this implies that all Internet users should be allowed to access all online sites and data and services, with no differences in quality or pricing dependent on their choices. Network operators that connect customers to the Internet would be treated the same as traditional Common Carriers, with no right to impose differential treatment for various forms of usage or content.

Opposing Views

Neutrality is not only a slogan of free speech philosophers and consumer representatives, however, it is also the preferred policy of many large corporate interests, especially software and applications providers, from Yahoo! and Amazon to eBay and Microsoft. These content providers share the concerns of net neutrality advocates that their services could be discriminated against by large access network providers, which may have affiliations with competing content services.

Aligned against this coalition, however, are many of the largest network operators, including telecommunications giants, cable TV providers, and some ISPs. These companies want to maintain maximum flexibility to configure their services to their greatest competitive and financial advantage. Also, given the high growth rates for bandwidth heavy applications, network providers argue that they have a legitimate need to manage their capacity, especially on wireless broadband networks where traffic congestion, particularly in high-demand urban areas, is a very real concern. There is also an ideological component to opposition to net neutrality regulations, a sense of rights of ownership, and resentment that companies which have not invested directly in network infrastructure should not be able to benefit so liberally from others' investment. There is also a basic principle concerning freedom from government interference in the marketplace which guides many political opponents.

Some of the prospective alterations in established Internet business practices that net neutrality advocates oppose, and that have been at least contemplated among some network operators, include various forms of multi-tiered, usage-based pricing, in which user payments would be roughly linked to the amount of data they download and upload, as many cell phone data plans already charge. Also, vertically integrated or affiliated network and media corporations could institute preferential pricing and/or differential access speed and quality, for web sites and services they control and profit from, as compared with competitors' sites and the broad Internet as a whole. More ominous still, and the worst fear of free speech advocates, some corporations that may have certain political leanings and vested interests, could attempt to skew the information content received by their subscribers, in direct contravention of the basic principles of free exchange of ideas.

A different business model that has also been proposed by some providers would involve the establishment of separate, proprietary access networks for certain types of customers. For example, larger corporate users might pay premium prices to receive the highest speed connections, both at the customer premises and in terms of server capacity and throughput. The corollary to such a plan, however, would imply that the lowest paying, average consumer would receive the poorest quality connections, resulting in a de facto tiered, price discrimination scheme.

Policy Initiatives

The most prominent policy issues arising from this debate tend to fall into two main categories. One is whether network operators should be able to introduce pricing schemes that are linked to customer usage levels in general: i.e. to charge more

for higher bandwidth consumption, which would seem to have a basis in the economics of network operations. The second set of issues relate to whether operators can discriminate among different classes of content on their networks, apart from the capacity that such content consumes. Although both issues raise a range of concerns and debate, it is the second, content discrimination, which has been the primary focus of net neutrality policy initiatives to date.

In 2008, the U.S. Federal Communications Commission attempted to order Comcast, a cable TV and Internet access provider, to cease blocking or downgrading certain users' access to some high capacity peer-to-peer download services. There was no attempt to impose capacity charges or separate pricing tiers, and other high capacity usage, such as video streaming or VoIP, was not treated similarly. On the surface, it appeared that Comcast was simply trying to discourage peer-to-peer file sharing itself, although it had no specific policy to do so. The FCC's ruling, however, was subsequently struck down on appeal in court, leaving U.S. law undecided as to the FCC's authority to implement net neutrality regulations.[36]

In mid-2010, two major U.S.-based players, Verizon Communications, a network operator, and Google, an applications provider and Net neutrality supporter, collaborated on a proposed "compromise" policy on certain aspects of the Net neutrality issue. Their proposal would endorse basic non-discrimination principles as proposed by the FCC, preventing carriers from favoring or degrading certain classes of user or content. However, these principles would apply to existing Internet access and content, but would permit access providers to develop "new" services, which could be priced differently from basic access. This approach would also allow operators to sell dedicated network capacity to high priority users, for purposes of accessing these new service offerings. Also, the joint proposal would not apply to wireless broadband networks, which the companies asserted were still evolving and should not be constrained by these principles, other than transparency. As of late 2010, the FCC and the Congress had wrestled with the issue for several years, and continued its efforts to balance competing corporate and political pressures, without clear resolution.

The European Commission has suggested a number of policy distinctions to clarify the degree of neutrality required of network operators and ISPs. For example, traffic management and product differentiation by operators and ISPs, are considered acceptable practices, but customers should be informed in advance of any limitations or distinctions in the level of service they will receive. On the other hand, the Commission has indicated that unequal discrimination between similarly situated customers or services should not be allowed. As of mid-2010, the European Commission had launched consultations to obtain wider input on these and other issues, before considering whether to adopt specific net neutrality related regulations.[37]

Several other governments have also wrestled with this issue, but few have codified rules that formally guarantee – or not – any particular model of net neutrality. On the other hand, outside of various isolated disputes, there have not to date been major re-pricing initiatives by broadband access networks to introduce tiered or measured services, nor substantial anti-competitive quality of service discrimination. But the debate has become a central issue in Internet regulation and even political campaigns, and promises to gain force as network capacity usage and related competitive interests continue to grow.

The issue may be of particular concern in relatively smaller, emerging economies where Internet access and usage are still low, but likely to grow substantially in the coming years. In many of these countries, there will not be a wide scope of competition among either network operators or content providers, and other interests may also seek to gain a stake in controlling the gateways to the online world. As the debates among industry giants play out on the world stage, regulators in these developing economies should follow them closely.

7.5.2. Technology and Service Neutrality: Avoiding Picking Winners

Neutrality also arises as an issue in a variety of other contexts where governments and regulators have important roles to play. In such a highly competitive and lucrative industry as ICT, each decision by a public authority carries the potential to help or harm major stakeholders.

The goal of government should be to ensure that all participants in the sector have an equal and unbiased opportunity to succeed on the merits of their products and services, with a minimum of

favoritism. This is especially important to prevent any perception (or reality) of corruption influencing public policy toward the industry. The fast changing nature of ICT technology and markets also suggests that regulators should avoid, to the extent possible, trying to dictate which specific technical platforms or architectures should be deployed, and allowing the greatest possible flexibility for industry innovation and evolution.

Public Choices

Government decisions can influence ICT industry competitive outcomes in several different areas. These include the following:

- *State Ownership:* In countries where at least some national telecommunications operators remain under state ownership, even though the may be managed autonomously, it is almost inevitable that these operators will receive favorable treatment in many cases. While the rationale for such preference may be that the state operators serve the public interest, the inefficiencies and market distortions that arise are quite likely to outweigh the net benefits, especially when compared with the positive impacts of open competition and innovation. While this justification for private, open market entry in telecommunications has prevailed for several decades, it is even stronger in the broadband digital era, when competing forces are driving rapid change throughout the industry, and no single dominant operator is likely to be able to be able to stay out in front of every trend.

- *Licensing:* Licensing decisions almost by definition involve choosing winners among potentially competing players, especially where a limited number of licenses are granted to provide, say, cellular mobile services, or to utilize scarce spectrum. In the era of convergence, however, there is less reason to retain traditional distinctions between types of licenses (mobile, fixed, etc.), and more reason to allow unrestrained market entry by a significant number of integrated, multi-service telecommunications operators. As discussed in Chapter 3, many countries are moving to provide unified licenses, which permit licensees to offer a full range of services, via any technology platform. The main limitation involves the need to allocate finite spectrum among different uses in a rational manner, but even with this constraint it is possible to support a growing number of market participants without direct specification of their technology or market focus.

- *Subsidies:* Where public policies determine that certain ICT services or user groups merit subsidy funding support – for example, universal service programs, or stimulus type investment – the principle of technological neutrality is again critical. In some countries, subsidies are available to promote ICT access, and they are often distributed through a form of competitive tender (see Chapter 6). When specifying the services and facilities to be delivered under such mechanisms, it is important to allow maximum flexibility among competing technologies: for example, satellite, landline, WiMax, or 3G, all of which might be capable of bringing adequate network access to remote areas. If subsidy administrators were to design projects so that only one type of network could comply with the requirements, this could again constrain market development and potentially lock in outdated technologies for many users and geographic areas.

- *Procurement:* Governments utilize extensive amount of information technology resources and IT-enabled services for their own day-to-day operations, especially as widespread e-government systems come online. This requires public procurement of equipment and software which must meet detailed and standardized specifications, and which can amount to huge sales for any IT supplier. Ideally, such procurements will maintain competitive balance between multiple vendors and systems, especially for computer hardware that may be relatively interchangeable among multiple brand names. However, in the case of software operating systems, application packages, and custom solutions, strict interoperability and ease of use are vital requirements. Again, given the size of typical purchases, governments have been forced into the position of influencing industry outcomes through their decisions.

  In some countries, advocates of free and open-source software have succeeded in persuading national governments to promote the cause of

unlicensed open source software by establishing this standard throughout public offices. Partly in response to this trend, market leaders such as Microsoft have in some cases offered highly discounted government-wide licenses for their own product packages. Ultimately, effective and convenient operability and value for cost should probably be the primary motivation behind public IT procurements, but in this sector it is always difficult to avoid getting in the middle of competitive and even ideological battles.

- *Public Networks:* Beyond IT software and equipment, e-government policies also usually involve establishing physical or virtual networks, connecting schools, health facilities, government offices, and the like. Operation of these networks is typically outsourced to established or specialized telecom providers. When developing these contracts, public authorities should focus on their functional needs as opposed to specific technical solutions (e.g., by specifying minimum transmission capacity rather than, say a fiber optic network). Competitive bids for these public networks that are based on maximum technological neutrality are likely to be most cost-effective, and will encourage more creative solutions, while avoiding favoritism toward specific vendors.

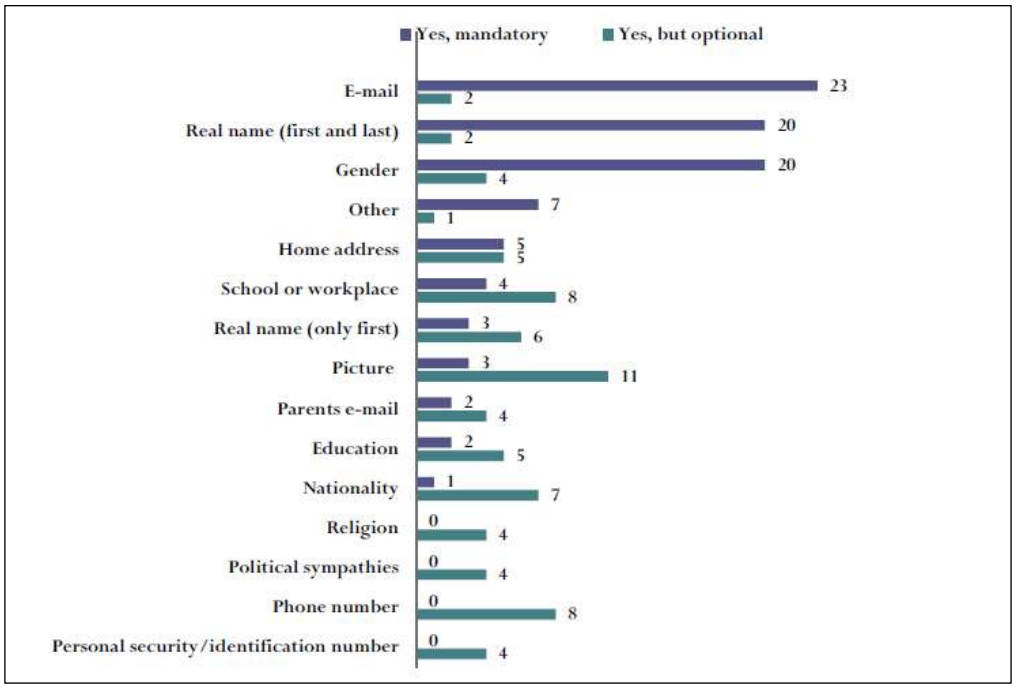
7.6. Protecting Privacy

The digital age has created massive new challenges to protect individual privacy and personal as well as commercial proprietary information. Regulators are now coming to terms with the magnitude of the problem and trying to forge workable solutions.

7.6.1. Protecting consumers in the commercial digital space

Protection of consumer privacy in the context of commercial relationships in the digital world is an extremely difficult issue. By the nature of electronic networks, it is a simple, virtually automatic task for operators of any web site or ISP to track and compile endless amounts of data on users of their systems: who visits what web sites, what people search for, what they purchase, how much they spend, and of course inordinate amounts of personal details, names, addresses, credit card numbers, etc (see Figure 7.7). From a business point of view, such information is a gold mine, which can help to refine marketing campaigns, target potential customers, and save costs at the same time.

Figure 7.7 Personal Information Typically Requested When Creating a Profile



Source: EU, Evaluation of the Implementation of the Safer Social Networking Principles for the EU, 2010.

For consumers, however, the idea that faceless corporations are collecting detailed databases on their identities and online activities is, in most societies, a disturbing prospect at best. Most people don't want to be bothered, targeted, or especially spammed by commercial interests, and they are usually sensitive to the possibility of anyone knowing their most intimate habits, interests, and secrets. This has given rise to new levels of privacy concerns and risks in the digital environment.

Vulnerability of Personal Data

There are a wide range of situations and practices that can raise commercial privacy concerns for consumers. Some may be more problematic in terms of risks and the degree of exposure that users may face, while others may primarily be annoying or time-consuming. Depending on circumstances, some instances of companies utilizing private consumer data for commercial purposes may not be entirely objectionable to many citizens, especially where this is done in a transparent and approved manner. The following examples highlight some of the many categories of privacy concerns in the digital era.

- *Online:* Wandering through the Internet, one leaves digital tracks virtually everywhere, some more obvious than others. True privacy online is probably impossible, but some situations are especially risky for unsuspecting users. Entering one's credit card number to make an online purchase places some of the most sensitive data into the infinite depths of the Internet. Countless web services request identifying information from their users. Some companies utilize "opt-in" practices, which require users to actively agree to have their data shared with others, while many will only safeguard such data if users explicitly ask. Many web sites also install "cookies" on one's personal computer, which retain identifying data for each site visited. Both social networking and even e-mail expose one's personal data to unlimited outside locations.
- *Telephone:* Use of the fixed-line telephone, as well as newer mobile and smart phones, also invokes a great many privacy concerns, some new and some which have been troubling consumers and lawmakers for decades. Telemarketing is both well established, and widely disliked. Many governments have introduced mandatory "do not call" lists, which certified telemarketers must respect or face legal damages. Millions of people depend on mobile and smart phones for much more than calls: they are address books, appointment calendars, cameras, repositories of hundreds of text messages, and links to social networks, e-mail, even GPS locations. They are also very easy to lose or to steal. Moreover, cell phone signals are far easier than landlines to monitor and trace, by both legal and illegal electronic eavesdropping. Most telephone systems now routinely deliver the Caller ID of each caller, and policies are often required to allow for blocking this information.
- *Workplace:* Privacy issues relating to use of ICTs in places of employment raise a unique set of concerns, requiring a delicate balance between employer and employee rights. When hiring new personnel or reviewing employee performance, employers often seek revealing background information, through a variety of channels. When on the job, many workers utilize office computers to access the Internet and send personal e-mail. In general, there is no presumption of personal privacy for employee communications conducted via company computers and networks.
- *Daily Life:* There are countless other situations in the average daily lives of citizens in which they may provide sensitive data that could well end up in compromised databases. The widespread use of credit and debit cards, together with digital cash registers, RFID scanners, and computerized inventories, allows stores and banks to track nearly every purchase a person makes. Health and medical records are potentially accessible through a diverse number of channels: doctors' offices, hospitals, health and life insurance companies, public health offices, and more. Joining a political or hobby club, getting a library card, signing up for a contest or promotion, volunteering for charity work: all are likely to add to one's electronic profile, for better or worse.

Privacy Protection Policies

There are widely varying legal approaches to privacy and data protection in different countries and regions, and this is an area of law and regulation that

continues to evolve as the challenges and conditions of data use and international communications evolve. Possibly the most extensive policy regime on these issues has been developed by the European Union, through its Data Protection Directive (1998). These Directives are critically important because they affect not only all Member States of the EU, but by law they also extend to all countries and companies that do business with Europeans. The key elements of the EU Data Protection Directive are set out in Box 7.2.

By contrast, data privacy protection policies in the United States have been considerably less comprehensive and coherent. Although privacy law has a long history in the U.S., it has evolved through a patchwork of separate legislation and court rulings addressing specific areas of concern, such as financial services, credit and debt records, health information, and a variety of more recent mandates in the context of the Internet and data communications. No single authority or set of rules uniformly applies to all personal data processing, as with the EU. This has led to conflicts between the U.S. and the EU, given the strict rules in the *Data Protection Directive* concerning transfer of data to countries with fewer protections, as the U.S. regime has been considered to be less protective in some cases.

Box 7.2 Key Elements of EU Data Protection Directive

Definitions: Defines "Data Controllers" (anyone who has control over any person's private data); "Data Subjects" (anyone whose personal data is utilized); and "data processing" (collection, storage, and disclosure of data).

Principles: Data must be collected only for explicit and legitimate purposes; must be relevant and not excessive, accurate and up to date; data subjects must be aware of and able to obtain any data about them, and to correct errors. Each state must establish a supervisory authority to oversee data protection.

Limitations: Data controllers can only process data under certain conditions: if the data subject has unambiguously given consent; if it is necessary under a contract, required by legal obligation, or where other legitimate interests are involved.

Sensitive Data: Especially sensitive data about persons include their race or ethnic origin, political or religious views, health, sexual preference, and union membership. More strict rules apply to processing such sensitive data, which must normally require the subject's consent.

Data Transfers: Companies are not allowed to transfer data outside of the EU to any country where data protections are not equivalent to those in the Directive; however, foreign companies can go beyond their country's laws by signing binding contracts with EU companies that incorporate stricter data protection standards.

Source: European Commission.

Numerous other countries have enacted privacy laws, many of them predating the explosion of digital and online databases and transactions, which have been subject to review and potential updating. The Australian Law Reform Commission, for example, recommended in 2008 a comprehensive overhaul of Australia's existing *Privacy Act,* and the government accepted and began work on implementing most of these reforms in 2009. Many countries, however, especially in the developing world, have very few legislative or regulatory protections of consumer privacy rights, and even fewer resources to enforce whatever rules they do have. As a result, many such countries are likely to encounter problems in international trade relations, for example with companies in the EU, as well as with their own citizens, as ICTs and e-commerce continue to expand and diversify.

Identity Theft

One of the greatest concerns in the area of privacy protection and international cooperation on cybercrime involves identity theft. Quite simply, identity theft is a form of virtual impersonation, in which one party utilizes the personal data of another, without knowledge or authorization, to obtain benefits or information that should only be available to the original person. The most common and harmful actions of identity thieves are typically to access financial information, funds, and credit through stolen credit card numbers, bank accounts, and other highly sensitive and valuable data. By far the most common recognized instances of identity

theft have involved illicit use of stolen or unauthorized credit cards.

Although financial motives are likely the most prevalent, there can be others motivations for identity theft, which rely upon different types of personal information. For example, a person may steal another's medical records in order to obtain prescription drugs; illegal immigrants may use black market ID materials to enter a country or gain employment; and spies and terrorists may advance their causes by utilizing innocents' identifying data in a variety of circumstances. In all cases, the impact on victims whose data may be compromised can be devastating, and may required very costly and time-consuming efforts to regain their good name and standing.

Identity thieves may obtain critical information on others through a host of methods, from simple to highly sophisticated. Some may involve intercepting people's mail or digging through their trash to obtain identifying information and credit card or bank numbers. In the online world, a prevalent practice is known as "phishing," in which unknowing consumers are enticed to visit a deceptive website, which asks them to fill in personal information under false pretenses – e.g., replicating the website of a bank or store with which the person may have an account, and requesting that he or she "verify" personal data. Some of these techniques can be highly effective, by employing virtually identical web pages and convincing communications methods, such as personalized e-mails. To combat phishing, many organizations inform their customers that they will never ask for such data in e-mail or other correspondence, and also send out alerts when fraudulent initiatives are discovered.

Box 7.3 Google Street View: Are Public Streets Private?

One indication of the fast changing nature of technology and privacy involves Google's "Street View" service. In connection with Google Maps, the company's popular mapping and GPS service, Google has also included street level photographs of major routes in countless cities, to help with navigation. To some citizens and governments, these often close-up views of private homes and streets offer too much of a peak into personal and private lives. It also emerged that Google obtained a vast amount of WiFi data from WiFi receivers in its Street View vehicles. Google also admitted that it intercepted and stored WiFi transmission data, including email passwords and email content.

Governments in Greece and the Czech Republic have imposed bans on Street View photos, while at least 18 other countries have launched investigations into the service, e.g.:

- Connecticut Attorney General Richard Blumenthal announced in July 2010 that 38 states and the District of Columbia are seeking additional information about Google's collection of WiFi data from private, residential computer networks. Blumenthal also sent a letter to Google, asking for information about Google's packet-sniffing software, the testing and review procedures, and the internal investigation of the code that "accidentally" recorded unencrypted WiFi traffic in 30 countries over a three-year period.
- In the U.K., London's Metropolitan Police Service is reviewing a criminal complaint filed against Google. The complaint was brought by London-based Privacy International under two U.K. laws: the Regulation of Investigatory Powers Act and the Wireless Telegraphy Act.
- The French National Commission on Computing and Liberty (CNIL) released preliminary results of the Google Street View investigation in France. According to the CNIL, Google "saved passwords for access to mailboxes" and obtained content of electronic messages. The CNIL is pursuing the investigation to determine whether Google engaged in "unfair and unlawful collection of data" as well as "invasion of privacy and individual liberties."
- The Chief of the FCC's Consumer and Governmental Affairs Bureau warned consumers that Google's "behavior" raises important privacy concerns and said that the collection of WiFi data, "whether intentional or not . . . clearly infringes on consumer privacy."

Source: Electronic Privacy Information Center.

In many countries, identity theft for purposes of defrauding another or gaining illicit financial benefits are covered under traditional criminal fraud statutes, but such crimes are also being taken into consideration under data protection laws as well. The United States passed the *Identity Theft Deterrence Act* in 2003, which makes the possession of any "means of identification" to "knowingly transfer, possess, or use without lawful authority" a federal crime, as well as unlawful possession of identification documents. The government has also directed financial institutions to collaborate in developing identity theft detection and prevention measures.

Another key question that needs to be addressed by such laws is the liability for financial losses that may

result, for example if funds are fraudulently withdrawn from a bank account or if a stolen credit card is used for a purchase. In Sweden, for example, where banks and stores are obligated to verify the identity of a customer, if they fail to do so these institutions are liable for the cost of any fraudulent transactions. In other cases, credit card companies may bear limited liability, but this may depend upon the customer notifying the card issuer of the lost or stolen card within a certain time period. For consumers in some jurisdictions, however, nearly all the risk is on the individual, and victims of identity theft can potentially lose most or all of their assets without recompense.

Aside from stopping these crimes and restoring victims' privacy and reputations, another important goal of law enforcement is to monitor and expose organized rings of data thieves, by tracing individual cases to their source. Because these criminals can be based anywhere in the world, and identity theft is an inherently global problem, international cooperation among governments, institutions, and law enforcement is crucial to reducing the scope and impact of these practices.

7.6.2. Curtailing Big Brother: Protecting Citizen Privacy

In many countries, citizens may have as much reason to be concerned about government intrusion on their privacy as from commercial entities. Rights and laws relating to basic principles of privacy differ widely among societies (e.g., the "right to be left alone"). This is partly due to differing state interests in monitoring and maintaining information about citizens. This debate then spills over into policies on national security. In the ubiquitous digital age, this long-standing conflict between civil liberties and government scrutiny takes on even greater urgency.

Government Databases

Governments have always inevitably gathered vast amounts of information about all their citizens. In the digital age, this information can be stored, sorted, distributed, examined, cross-referenced, and utilized in countless ways that are far more extensive than was ever possible in the era of paper, typewriters, and photocopies (let alone pen and ink). Democratic societies that may have, in the past, established reasonable protections and limitations on use and misuse of private citizen information by government authorities have been forced to revisit the principles and practices of nearly all public agencies, to adopt new rules of behavior for everyone from senior administrators to filing (or data entry) clerks.

To some extent, government databases do require sharing and cross-referencing of certain private information, to help improve efficiency of numerous bureaucratic processes. It makes sense, for example, for automobile registries to be linked with traffic enforcement databases, for real estate deeds and property tax records to be connected, and so forth. In the United States, where access to firearms is widely available, considerable controversy arose over the introduction of "background checks" on gun purchasers, requiring both a brief waiting period and a mandatory check of national criminal databases before guns can be sold. Shared access to public database records is especially needed for criminal investigations, and most national data privacy laws include a variety of exceptions and exemptions for law enforcement and national security.

But there are also important limitations in many laws regarding the scope of government access to and use of the private personal data of citizens without their knowledge and consent. Many countries issue national identification numbers (e.g., social security numbers) to each citizen at birth or upon legal immigration, and these ID numbers may be tied to dozens of records stored within disparate databases of various national or provincial/state authorities. As a general principle, most of these records must typically remain private and for the internal use of each agency that maintains them, and may not be shared or disclosed to outsiders without the subject's consent. Also, disclosure laws typically require that citizens be able to obtain copies of virtually all information that is kept about them, from public school records to tax files. There are, however, a number of areas where information is routinely made available for public access by anyone, especially those records which involve public proceedings such as court hearings, as well as information such as birth, death, and marriage certificates and property ownership deeds.

The EU *Data Protection Directive* applies to government agencies in most respects as well as commercial enterprises. Government agencies are "data controllers" with respect to the information that they obtain from citizens for any purpose, and so are similarly restricted from misusing, disclosing, or sharing such data according to the mandates of the Directive.

Electronic Democracy

Data protection and other privacy (and disclosure) issues also arise in connection with the increasing digitalization of democratic political processes and activities Politics requires an extensive degree of communication between candidates and voters, and the new era of technology is becoming fertile ground for innovative fund raising, public relations, advertising, activism, polling, and numerous other communications-intensive political endeavors. As with government's role in general, however, citizens in most democratic societies have a right and an expectation to be shielded from excessive invasions of their personal privacy by politicians, to know what is going on behind the scenes, and most of all to be sure that their personal electronic choices are safe, fair, and private.

Some of the most important privacy and data protection issues relating to electronic democracy policies fall into the following categories:

- *Campaigning:* In tight campaigns, candidates have been known to utilize technology to virtually harass potential voters: by placing automated telephone calls to every known number, for example, multiple times per day. Unlike commercial telemarketing, these may not be subject to strict limitations, due to free speech concerns. The same may be true of excessive e-mails, not to mention advertisements, as well as endless polling of public opinion. Of greater concern is the need to ensure openness and honesty in all communications, especially where information may be circulated that can include false rumors or unproven claims. Wherever official campaign staff and affiliates are involved in publicity or information dissemination, either in favor of one candidate or against another, laws should require strict disclosure of the source and support for any such activities. This is distinct from the unaffiliated activism of private citizens, who should have more freedom to express their views without interference or restraint.

- *Financing:* Strong campaign finance disclosure and limitation laws have been introduced in a number of countries, although many other democratic regimes have far less protection or openness with respect to the funding of political activities. The most open requirements obligate any citizens, organizations, or companies that donate to or otherwise financially support a candidate to reveal their support clearly, and for candidates to file regular reports that are available to the public for easy review. There is generally no right, in these circumstances, to privately or secretly underwrite a political campaign.

- *Voting:* Perhaps the greatest fear among privacy advocates in relation to electronic democracy involves the risk that electronic voting itself may be subject to corruption. More and more governments are adopting advanced, computerized voting machines, which expedite the voting and vote-counting process, but have created strong concerns that the resulting databases could be manipulated by hackers or infiltrators, rendering results suspect. Voters also need to be certain that their private selections in the voting booth will remain secret: one of the most fundamental tenets of electoral democracy, which could be at greater risk where electronic processing of votes predominates.

7.7. Cybersecurity Concerns

The digital age has brought with it an entirely new class of security concerns, for governments, companies, and individuals. Our growing dependence on ICTs has meant that our public and private networks have become critical and increasingly vulnerable infrastructure. The reality is that any weakness or attack, no matter how small, can have large global consequences. And the interests of security must be weighed against the liberty of citizens and the need for reasonable restraints on interference with private communications.[38]

7.7.1. Virtual Vulnerability: Security of Networks and Infrastructure

The technological revolutions of the digital age have arrived at a time when historical patterns of international conflict and rivalries have also undergone dramatic changes. While the prospect of all-out military battles between massive national armies has diminished greatly since the end of the Cold War, a new era has emerged in which malicious terrorism is becoming the leading worldwide threat to peace. At the same time, there continue to be numerous regional conflicts and hostile regimes, requiring the world community to be continuously alert for potential trouble. These developments

have placed ICT infrastructure and services at the very core of national security concerns, requiring a re-assessment of the scope of defense and intelligence policies.

Emerging security threats

The role of digital communications in both fostering and preventing security threats in this environment is extensive. Virtually all actors, from state security systems to terrorist organizations employ the full range of advanced networked technologies to collect and share intelligence, to conduct espionage, to maintain contact among personnel, and to spread their messages. From the point of view of threat prevention and response, however, one of the greatest concerns is the vulnerability these very communications resources to attack and disruption. It is an immeasurable challenge, as a virtual assault could come from anywhere at any time, from invisible sources, aimed at any of a million at-risk and critical targets.

The areas of virtual vulnerability are many. In the months leading up to January 1, 2000, there were widespread concerns that the so-called "Y2K bug" would disable essential systems that depended upon computers throughout the world; while those fears proved overblown, they highlighted the vast interdependence of computerized infrastructure and facilities, which could be harmed through targeted cyberattack. These could include electrical grids, telecommunications networks, government and commercial databases, financial institutions, and military networks, among others. One of the most common forms of cyber assault is a "distributed denial of service" (DDOS) attack, in which hundreds or thousands of computers under the control of the infiltrator transmit uninterrupted signals toward a web site or other online network; the resulting overload of traffic effectively crashes the site, making it unable to function properly. Similar attacks can employ specialized viruses, or even direct takeover of the command functions of a targeted system.

The level of threat in all of these areas is very real, and to some extent not even very new. Various forms of electronic espionage and sabotage have been attempted since the dawn of computers and modern telecommunications. In some way, cyber espionage is the ideal form of infiltration, since classified information and national security can be compromised by foreign entities over a long distance, without spies in harm's way. There have been a number of clandestine incidents that have come to light over the years, raising alarms that even greater risks may be forthcoming.

As for true cyberterrorism, i.e. destructive acts by non-state actors on a large scale aimed at core infrastructure, there have been fewer significant publicized incidents to date. One prominent case occurred in 2007, numerous sites in Estonia came under large-scale distributed denial-of-service attacks, which resulted in the temporary disabling of most Estonian government ministry networks as well as those of two major banks.[39]

Responses. Whether defending against organized cyber terrorists, state-sponsored cyber warfare attacks, or rogue hackers, governments are recognizing the need to devote substantial resources to this evolving area of threats. A range of responses have been attempted and suggested. Until recently, the most common deterrent for cyber attacks has been "passive defenses", such as firewalls and other physical and virtual blocks against electronic intrusion. These approaches, however, can be increasingly vulnerable as they do not typically evolve as quickly as expert hackers are able to thwart them.

Another potential strategy in reflects the Cold War tactic of nuclear deterrence, by developing a response capability which can turn cyber attacks back on the attacking party. The main problem here, however, is not determining where a cyber attack comes from, but specifically whether it was the work of a government, a military organization, a corporation, terrorists, or individual hackers. In fact, governments may employ private proxies, even based in different countries, to carry out attacks. Without the ability to accurately identify the source, cyber retaliation could be fruitless or counter-productive.

Recently, more focus has been placed on developing multilateral international approaches to deterring cyber warfare or terrorism. Several key states, including Russia, China, the United States, and India, have entered into negotiations through the United Nations to develop an international treaty on cyber security, based on Russian proposals to establish common principles and standards for such the use of electronic "weapons" and protection of critical infrastructure from infiltration and attack. There have even been proposals that Russia and the North Atlantic Treaty Organization (NATO) should

engage in joint simulated "cyber war games", to help plan for responses to potential emergencies or misunderstandings, among other potential cooperative actions. The International Telecommunication Union has also taken a leading role through its *Global Cybersecurity Agenda* (GCA) (see Box 7.5).

Box 7.4 The ITU Global Cybersecurity Agenda (GCA)

Launched in 2007, the ITU Global Cybersecurity Agenda is a framework for international cooperation aimed at enhancing confidence and security in the information society. GCA focuses on building partnership and collaboration involved in detecting, preventing, and overcoming cyber threats.

GCA has established five "pillars" or Work Areas of cooperation and initiatives:

1. Legal Measures
2. Technical and Procedural Measures
3. Organizational Structures
4. Capacity Building
5. International Cooperation

The GCA has fostered initiatives such as Child Online Protection and through its partnership with IMPACT and with the support of leading global players is currently deploying cybersecurity solutions to countries around the world.

Source: ITU.

The most critical component of any response to cyber threats, however, is human resources. Dealing with this class of highly sophisticated and constantly evolving electronic interaction requires trained specialists, and many of them, focusing their efforts on different types of risks and scenarios. By some estimates, national security teams require a force the equivalent of an entire army regiment, some 20,000 to 30,000 specialists, to mount a comprehensive cyber defense.[40] Yet most governments employ a small fraction of such a force, and training in cyber security is a field that has yet to reach levels adequate to meet the risks of the 21st century.

7.7.2. National Security and Civil Rights: What Should be the Boundaries?

Rising fears concerning both cyber attacks and many other forms of security risks have led many governments to revisit their options for investigating their own citizens and non-citizen residents. In the wake of the 9/11 attacks on the United States and multiple other terror incidents around the world, a very intense debate over the delicate balance between civil liberties and national security has been engaged among nearly all democratic societies. The magnitude of potential threats is matched by the scope of potential government intrusion into private lives, and each country must decide how much risk versus how much infringement on freedom it is willing to tolerate.

Electronic Surveillance

Since the earliest use of telegraph and telephone communications, regimes have sought to intercept such connections to eavesdrop upon enemies, spies, criminals, and nefarious conspiracies of all kinds. With much more widespread use of both landline and mobile telephones, including massive growth in international telephony, this avenue of surveillance has only increased in importance. There are two general ways, in theory, in which security officials can seek to identify threats and obtain intelligence through real-time monitoring of electronic communications: (1) by randomly monitoring large volumes of voice traffic in hopes of catching snippets of suspicious conversations; or (2) through targeted eavesdropping of selected suspects (or profiled persons). Both approaches are widely utilized, and both are controversial.

As a general rule, most countries' surveillance laws require officials to obtain a court warrant or similar authorization, based on some degree of probably cause, to institute targeted wiretapping or electronic eavesdropping against individuals or groups. The key questions involve what scope such authorizations should be able to encompass, with what limitations? Some of the important details to be resolved include:

- What evidence authorities must present to justify establish cause for a surveillance warrant?
- How long the warrant should be in force?
- How easily, and on what basis, a warrant should be renewable?
- How much time should be allowed for a warrant request to be reviewed?
- How many persons, or how wide a scope of an organization, can be covered based on uncertain evidence?

- And perhaps most important: under what special, emergency circumstances can authorities proceed with electronic surveillance *without* a warrant?

The U.S. Patriot Act, signed into law scarcely one month after the Sept. 11, 2001 terror attacks, resulting in fewer restrictions on American law enforcement agencies' authority to conduct investigations of a wide range of potential suspects. It specifically amended the existing Foreign Intelligence Surveillance Act (FISA), which addresses how electronic surveillance may be conducted on foreign powers or their agents, but not domestic citizens. Although FISA still required warrants for such eavesdropping, a scandal arose in 2005 when it was learned that the Bush Administration had secretly authorized extensive interception of both foreign and domestic communications for several years, without obtaining warrants. Although the program was subsequently stopped, in reauthorizing the Act in 2008, the U.S. Congress granted retroactive immunity to telecommunications companies that had cooperated with the illegal warrantless wiretapping activities, adding to public displeasure among many citizens.

Box 7.5 Mobile SIM Card Registration

Another recent step taken by many governments has been to require that all cellular mobile telephone users register their SIM cards in a national database. Countries such as Ghana, Nigeria, Zimbabwe, and others where these policies have been instituted have far more mobile phone users than landline subscribers, but standard pre-paid mobile services don't normally require any form of identification or registration. Government security officials have proposed SIM card registration as a means to reinforce their investigatory and research functions, by associating names, addresses, and other information with each cell phone. Implementation of these policies has proven difficult, however, and governments have had to postpone shut-off deadlines for mobile customers that failed to register, while the logistics of the system have been ironed out. Many customers have objected to having to provide their personal information under such programs, and have expressed concern that the registration is part of a broader government goal to eavesdrop on private citizens.

Source: AudienceScapes, 2010.

A different objection arose in Italy in 2010, when the government actually proposed cutting back on the uses of wiretapping. Italy has had one of the less restrictive regimes governing wiretaps and eavesdropping by both police and private entities, which has led to as many as 100,000 wiretaps per year, compared with only a few thousand in the U.S. and Britain. As both law enforcement and the national media had come to rely upon this particular method of discreet information gathering, proposals to curtail wiretapping warrants met with protests by both groups, including a general strike in which nearly all national media shut themselves down for a day.

Access to Data

In an era where a large and growing proportion of global communication involves means other than voice conversations, where myriad forms of information can be exchanged across limitless electronic data channels, security authorities confront an expanding scope of targets to investigate for evidence of crimes and threats. The bulk of contacts among many subversive or criminal organizations most likely involve some combination of e-mail, SMS or text messages, chat rooms, coded web postings, and other modern innovations. Such surreptitious uses of multiple digital channels are all the more necessary, and convenient, for organizations that operate across borders and among many discreet locations.

The need to locate, uncover, monitor, decipher, and evaluate all the varied possible communications mechanisms of potential adversaries places law enforcement and national security forces squarely in the center of the debates over civil liberties in the information society. Almost any form of cyber investigation will inevitably involve accessing private data of entirely innocent average citizens. Again, the challenge is to determine the appropriate balance: the most reasonable, effective, and practical limitations on officials' authority to obtain and examine private data, and the rights of all citizens to expect that their personal information and communications will remain out of reach, by even the police or security apparatus.

The most common manner for officials to obtain access to data communications requires ISPs and other network and service providers to grant access to actual server databases, either through direct transmission links or through copies of data files. Either step is a serious intrusion and one that many companies are reluctant to accept. Again, the challenge becomes the scope of the government's case as to the urgency and value of such an investigation, as against the rights of both the data owner or controller, and its customers. At a minimum, court warrants authorizing such access

need to be narrowly tailored to protect innocents' data, and to avoid massive increases in public control of private information.

Box 7.6 The Blackberry Controversy

In 2010, several governments, including the United Arab Emirates, India, and Saudi Arabia, threatened to block use of the secure network of Canada's Research in Motion (RIM), the company that produced the popular Blackberry smart phones, widely utilized by corporate customers in particular. Security officials in these countries, where perceived threats of subversive and terrorist activities are very high, insisted upon gaining the ability to obtain access to encrypted Blackberry-originated e-mails, calls, text messages, and the like. While offering to cooperate, RIM objected that its entire business model depends upon offer secure communications to corporate customers, and even the company itself was not able to access and decode its customers' encrypted transmissions.

This standoff led to threats that the governments would block all transmissions utilizing the Blackberry system, potentially eliminating their service altogether and forcing hundreds of thousands of customers to switch to different service providers and/or new, non-encrypted devices. As of late 2010, the parties were seeking to negotiate a mutual agreement, while the security officials were looking at expanding their access demands to Google, Yahoo, and other multinational providers of personal e-mail services. The problem with this type of conflict between security and civil liberties lies partly in the nature of modern communication technologies themselves.

While it is theoretically possible for any network to capture and retain virtually all digital messages that pass through its servers, most operators do not actively monitor and retain such information willingly. For one thing, the storage capacity required to keep indefinitely all data files transmitted through a broadband network with millions of users would soon become astronomical, especially as users send more multimedia messages, and the costs of such capacity could become prohibitive. Also, the nature of encryption protocols is such that, as RIM indicated, they are not intended to be accessible by intermediary parties, and these might have to be entirely rewritten, or abandoned, to comply fully with security access demands. These problems are of course compounded by the objections of users over having their private messages exposed to government scrutiny. The impact of such policies could therefore be as significant in commercial and economic terms as in the political and civil liberties realms.

Source: England, 2010.

7.7.3. The War Against Malware

As networks expand, the volumes of malicious, destructive, and exploitative uses of ICTs are also multiplying exponentially. Regulatory authorities are on the front line of the battle against these abuses, which are among the most pervasive and potentially damaging challenges of the digital era. The risks are especially great for the most vulnerable victims - new and inexperienced users, children and teenagers.

The Danger of Viruses

Computer viruses represent a unique and unprecedented form of malevolent activity. A virus is a software program designed to invade and infect computers, servers, or networks, causing whatever harmful or innocuous effects its designer chooses, while replicating itself and traveling over the Internet or any private networks it infiltrates by attaching to e-mails or other transmission vehicles, unbeknownst to the users who receive and re-send it. These are typically highly complex programs, which require considerable expertise, and much time and effort, to design and disseminate successfully.

What is unusual about most viruses is that they are not typically intended for any financial or political purpose: the anonymous authors gain nothing material for their work, whether a virus is restricted to a small number of PCs or spreads around the world disabling hundreds of thousands. The apparent motivation for most virus writers is simply a demonstration of their code writing skills. The most effective viruses can result in many millions of dollars in damages and lost productivity.

In response, the antivirus software business has become one of the most lucrative markets in the software industry. According to Gartner, several billion dollars in antivirus packages and update subscriptions are sold each year. There is a very disturbing symbiotic relationship between the hidden, vigilante hackers who create viruses and the responsible, concerned antivirus companies who try to stop them. In fact, the more effective and widespread a virus is, the more valuable it is to the anti-virus industry: every time there's a global alert about a new killer virus scare, the sales of antivirus software and upgrades skyrocket. Not many major businesses are entirely dependent for their existence and prosperity upon the independent, voluntary, and uncompensated actions of anonymous outsiders. Antivirus firms even employ ex-virus writers as some of their most valuable counter-programmers.

In most countries, laws and prosecution relating to computer viruses are covered under more general cyber security and data protection statutes. When a virus causes damage or disruption to personal, corporate, or government computer systems, the creators can be liable for both criminal and civil prosecution.

But legal precedents are not widely established, and juries and judges can face challenges in determining exactly the nature of the crime committed, or the magnitude of damages. In 2002, the creator of the notorious "Melissa" virus, which had infected untold thousands of computers in 1999, pleaded guilty in U.S. federal court to charges relating to the scope of damages caused, and was sentenced to twenty months in prison.[41] However, the author of a copycat virus which was built on the same code as Melissa, known as the "ILOVEYOU" virus, received no prosecution or punishment, although his identity was known almost immediately. This was because this virus was created by a programmer in the Philippines, and upon discovery of the source of the virus, Filipino law enforcement determined that there was no existing law that applied to such an action, if it did not specifically involve fraud or theft.[42]

It is evident that global cooperation and harmonization of laws, investigation, prevention, and enforcement regarding malicious computer viruses must be a high priority. Since viruses are increasingly used as part of cyber crime and other potential cyber threats, electronic epidemics (such as worms and spyware) require concerted action by both governments and businesses in the public interest.

Cost and Impact of Spam

Unlike pure viruses, unsolicited bulk commercial messages, or "spam", are decidedly aimed at profiteering above all. This scourge, which exemplifies some of the worst impulses of unrestrained commercialism, affects every last user of e-mail, which means virtually every Internet user in the world. Infinite sales pitches for Swiss watches, university diplomas, prescription drugs (such as Viagra), fake lottery winnings, sex sites, and innumerable invites to share the hidden wealth of some late African official pass through cyberspace every minute of every day. Estimates of the magnitude of spam messages can only be approximate, but by any measure they comprise more bits, by far, than all other e-mail traffic combined.

This does not mean, of course, that the number of "spammers" (people who deliberately create and circulate commercial con messages) are also in the millions or billions. On the contrary, in general, most spam originates from a relatively small number of sources. A single amateur self-promoting marketer can send thousands, even millions, of messages to unlimited recipients, with access to a simple program and readily available e-mail address lists. While many ISPs will block transmission of bulk messages to more than a certain number of addresses, there are many programs and packages that can get around such limitations. No one knows how many spammers there are, where they are, or how many messages they send, but the impact is astronomically disproportionate to their numbers and their efforts.

The impact of spam on the global Internet is also difficult to measure, but is undeniably large. To maintain adequate service quality, ISPs and mail hosts must invest in huge levels of extra transmission and storage capacity. The costs to block and delete spam are equally burdensome. And the costs borne by users, in lost time and inconvenience, not to mention the losses of those who fall victim to e-mail scams, only compound the injustices caused by those who infest the world with spam at almost no cost to themselves. Spam is also directly linked to "phishing", whereby entities attempt to acquire sensitive information from users such as passwords and credit card details by masquerading as trustworthy entities. This can lead to even more harmful crimes like identity fraud and theft.

The front line in the battle against spam is primarily manned by private sector companies. ISPs, major software companies such as Mozilla and Microsoft, and e-mail hosting services such as MSN, Yahoo! and Google have all invested heavily in developing spam filtering technologies. These filters reside on e-mail servers and seek to identify and quarantine spam messages, while passing through authentic e-mails. It's an inexact science, but there are few practical alternatives. These companies recognize their self-interest in fighting spam. Only the extensive investment in spam filters, which reduces the number of unsolicited messages actually received by most typical users to a small fraction of those actually sent toward their inboxes, prevents this epidemic from overwhelming consumers. Without effective filtering, the impact of having to sift through dozens or even hundreds of spam e-mails per day to locate the handful of legitimate messages might degrade the online experience to such an extent that demand may even decline.

Meanwhile, governments and law enforcement have taken on the task of seeking out the worst offenders, trying to reduce spam at the source. The challenge of legislating against unsolicited commercial e-mail is difficult. In principle, the goal is to prohibit massive bulk transmission of unsolicited commercial messages, but defining those terms in legally defensible language, and distinguishing spam from legitimate commercial advertising, requires drawing many fine lines. Nevertheless, dozens of governments have reacted to the spam plague by adopting a range of measures to criminalize this particular form of mass solicitation. ITU conducted a comprehensive survey of anti-spam legislation worldwide in 2007-2008, identifying more than two dozen countries where laws have been adopted, but with widely varying terms and conditions.[43]

The evolution of anti-spam law in Russia is a representative example.[44] Prior to 2006, intervention and enforcement against spammers required patching together a series of disjointed existing laws and codes of conduct. While the Russian Federation Constitution guarantees all citizens the right to communicate in any way they choose, federal law stipulated that citizens also had the right to "refuse reception" of messages. The national ISP association, meanwhile, established its own code of conduct, which stated that "bulk distribution of messages by means of e-mail and other means of personal information interchange" which are transmitted against the "obvious and unambiguously expressed initiative of addressees" is prohibited, and companies that violate this rule can be disconnected. A separate federal law against false advertising also applied to spam that could be shown to be fraudulent. In 2006, new federal legislation was proposed, to prohibit sending of any commercial messages without the recipient's consent, an approach which was problematically broad. Instead, more succinct, if difficult to interpret language was suggested:

> Creation and transmission of electronic or postal messages for an unidentified list of users of communication services is inadmissible.

While anti-spam laws target spammers, an alternative approach is the establishment of enforceable codes of conduct for ISPs, enforced by regulators. Such a system of 'managed self-regulation' would require ISPs to prohibit their customers from using that ISP as a source for spamming and related bad acts, such as spoofing and phishing, and not to enter into peering arrangements with ISPs that do not uphold similar codes of conduct. Rather than continue to rely upon chasing individual spammers, regulators in the most resource-constrained countries in particular would be more likely to succeed by working with and through the ISPs that are closer to the source of the problem, to their customers, and to the technology in question. The regulator's job would be to ensure that ISPs within their jurisdiction adopt adequate codes of conduct and then to enforce adherence to those codes.

While some ISPs can be expected to resist even such light-handed regulation, the advantage is that it places all ISPs on a level playing field. Under current practices, responsible ISPs find themselves bearing the brunt of the costs of spam. This explains why some ISPs have begun suing spammers for damages, an option that may not be available in all jurisdictions. The goal of managed self-regulation is to reduce spam in a way that protects responsible ISPs. ISPs that implement responsible, effective anti-spam measures should be rewarded for their good behavior. One means of rewarding those responsible ISPs is for regulators to hold their irresponsible competitors accountable. Regulators can also make consumers aware of the good works of the best ISPs, for example, by certifying ISPs that enforce their codes of conduct and allowing such ISPs to use the regulator certification in their advertising.

As with many other telecommunication-related policy issue that are salient across national borders, the importance of consistency, shared strategic approaches and international cooperation is paramount. International cooperation is needed because perpetrators can be located in almost any remote corner of the world, while the victims are spread out across the planet. ITU has again taken a leading role, coordinating policy initiatives and providing a range of information resources for government agencies and corporate members. The OECD created a Task Force on Spam and produced an "Anti-Spam Toolkit" of recommended policies and measures.[45] In 2004, a group of 27 countries and government agencies established the London Action Plan, a cooperative agenda for sharing information and coordinating policies against spam.[46] Still more cooperation is needed, especially among less developed countries where the illusory allure of instant riches will continue to grow in

appeal as the ICT phenomenon continues to transform their societies.

7.8. Green ICT

As ICTs have emerged as the dominant means of human communication and a central source of globalization, their impact and role in the environment is starting to take center stage. Regulatory authorities can cooperate to help minimize negative impacts and promote the positive benefits that ICTs can contribute.

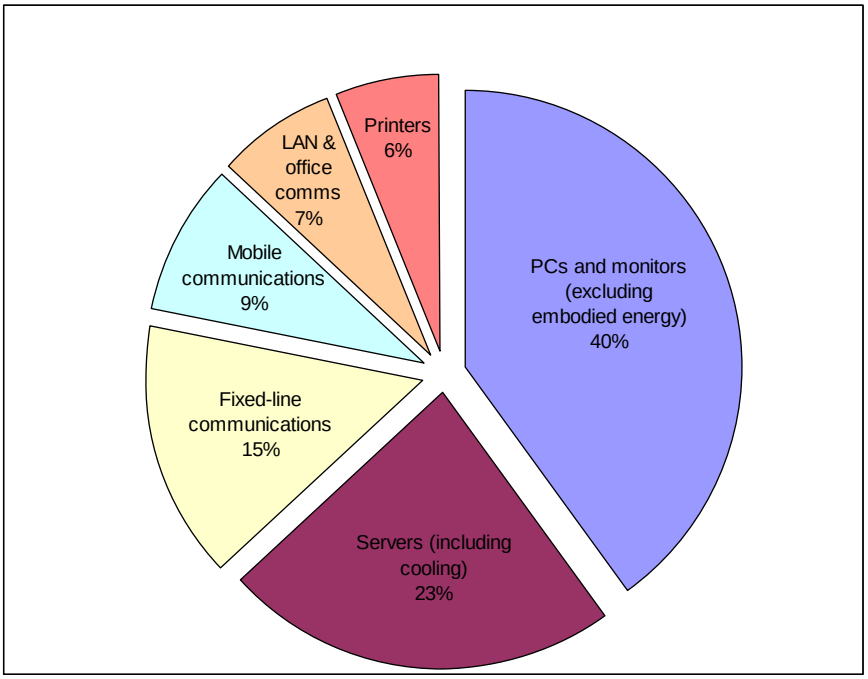
7.8.1. The Nexus Between Communication and Conservation

Environmental concerns, including climate change, represent some of the most serious global challenges of the 21st century. Advanced information and communications technologies can contribute significantly both to the problems and to the solutions. As a growing, energy-intensive, ubiquitous industry, ICTs have a strong impact on the environment in virtually every country. At the same time, as a field driven by innovation and competition, these technologies present a variety of opportunities to engineer Green alternatives to traditional modes of operation. And ICTs can play a vital role in helping to facilitate research, analysis, awareness raising, and cooperation to address critical environmental issues.

The Environmental Footprint of ICT

ICTs utilize a tremendous amount of energy in the aggregate. From the factories that manufacture equipment, to the permanently running transmission networks, to the servers, computers, phones, video displays, and more that all depend upon electricity (or rechargeable batteries), the Information Age is also a highly energy dependent age. As of 2010, ITU estimated that as much as 2.0 to 2.5% of global greenhouse gas emissions were attributable to ICTs. According to an earlier 2007 study, the largest contribution to the ICT footprint was PCs and monitors (40%), with servers next (23%). While mobile telephony accounted for only 9% of the total, this level has undoubtedly been growing in both absolute and relative terms (see Figure 7.8).

Figure 7.8 Estimated Distribution of Global CO2 Emissions from ICTs



Source: Adapted from Gartner, 2007.

To some extent, the energy utilized to power communications may be offset by energy savings in other respects. In particular, there are many instances where extensive use of ICT resources can have a direct impact in reducing energy use and

emissions from transportation: by facilitating long distance contacts through e-mail, telephone, and even video conferencing. The Global eSustainability Initiative (GeSI), a lobbyist group on behalf of the industry, estimates that the savings in emissions of greenhouse gases (i.e. mitigation effect) that can be achieved through the application of ICTs exceeds their direct negative impact five-fold. The precise degree of the impact is open to question.

Nevertheless, as ICT demand and utilization continues to expand, the net adverse impact of this sector on climate change and the environment in general is likely to increase steadily, unless strong measures are taken to alter the ICT energy equation. Some companies have taken leading steps, in cooperation with governments and environmental groups, to set examples of Green operating philosophies. One example is the web portal company Yahoo!, which announced in 2007 that it would implement "carbon neutral" practices in its operations. In 2010, Yahoo! announced plans for its new data center in New York, which was granted $9.9 million by the U.S. Department of Energy to implement energy-efficient plans, including use of wind and hydropower and specialized building design to increase natural cooling of the company's servers.

Mitigating Environmental Effects

There are many ways in which ICTs can directly or indirectly serve a positive role in promoting environmental objectives. Some of these may be within the authority of regulators and other policy entities to influence, whether through negotiations, laws, or economic incentives. Green awareness and energy efficiency initiatives such as Yahoo's program can create favorable publicity among customers and activists, whereas companies that may exhibit less responsible practices should be prepared for criticism and possible market consequences. As more is learned about the options for reducing energy consumption, pollution, radiation, and other hazards, public authorities may consider incorporating green ICT mandates in new or revised licenses and regulations.

As ICT networks extend farther into remote rural areas, there are new challenges concerning access to electric power, but also new opportunities to introduce renewable, efficient alternatives. In many such locations, operators utilize solar energy panels for cell sites and satellite receivers, for example. While these may be the only available option in many cases, they also tend to be far more expensive than attaching to an available electrical grid. Regulators and public subsidy programs should take account of the environmental benefits of solar and other low emission power sources, and should be prepared to endorse or compensate such initiatives wherever possible.

Further environmentally responsible policies can be adopted at every level of the manufacturing and delivery of ICT products and services. In the process of obtaining the raw materials needed for most electronic equipment, appropriate mining practices should be adopted, in line with sustainability and certification principles that have been adopted by many such operations. In factories and assembly plants, energy efficient and low emissions machinery should be employed. Land use policies, cell tower construction, data processing centers, and even retail sales outlets, the benefits of Green conscious approaches to doing business can have a strong influence on the overall impact of the sector. For instance, NGNs are expected to reduce energy consumption by 40 per cent compared with today's PSTN.

From another perspective, ICTs can serve the cause of environmental sustainability and mitigating impacts of climate change by serving the very purpose for which they are deployed. Advanced ICT systems, for example, have become critical to the measurement and monitoring of global temperatures and natural disasters, helping scientists to evaluate and anticipate impacts of shifting climate conditions. And of course, ICTs can be an extremely effective and influential partner in the movement to spread awareness of environmental concerns and to mobilize responses.

Finally, addressing these planet-wide challenges depends most of all upon collaboration among many stakeholders and experts, across multiple industries. As the ICT and environmental fields have both been following critical paths of development in recent years, there have been increasing opportunities for collaboration on research, policy, and technological initiatives. Especially in the realm of climate change, organizations on the ICT side have taken a significant lead in pursuing such cooperative endeavors. These include, among numerous others:

- *ITU and Climate Change:* A major initiative by the ITU to address the global impacts of ICTs on

climate change, and forge international cooperation on research and innovative solutions;

- *info*Dev *and DFID Climate Technology Program:* A joint initiative to provide seed money for innovative pilot projects utilizing advanced technologies to evaluate creative solutions to environmental challenges, by creating a series of climate technology centers as incubators for small businesses;
- *The Global e-Sustainability Initiative (GeSI),* a non-profit ICT industry cooperative organization which conducts research, publishes studies, and brings together multiple stakeholders to explore sustainable and environmentally appropriate industry practices.

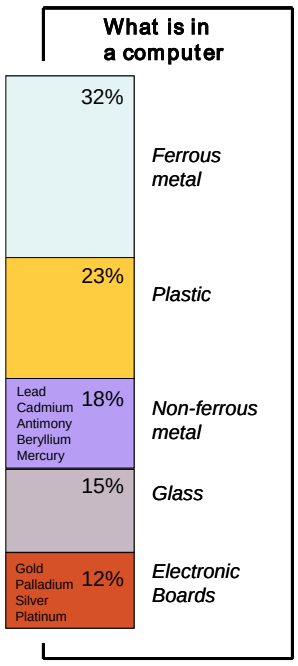
7.8.2. Cyber Waste, Digital Trash

While energy use and conservation are a central issue during the life-cycle of all ICT products and services, and equally important problem, which is growing rapidly, is what happens to these products once their useful lives are over. In recent years, the explosive growth in this sector, together with the inherent trends of frequent equipment upgrades and obsolescence, have led to dramatically increasing levels of cyber waste (or "e-waste"): discarded phones, computers, printers, and other digital trash, which not only cannot biodegrade but is generally hazardous to the environment.

Hazardous E-Waste

Hundreds of millions of used (and recently purchased) mobile phones are discarded every year around the world. Millions of cathode ray tube (CRT) monitors, printers and print cartridges, as well as PCs, LCD televisions and laptops, and an unimaginable number of batteries of all kinds are thrown away, to be replaced by newly manufactured substitutes. Nearly all of these products contain one or more hazardous materials in significant quantities: copper, silver, gold, palladium, platinum, lead, nickel cadmium, lithium, and mercury (see Figure 7.9). If these materials enter the soil and groundwater by being buried in landfills, they can create real and lasting health risks for local populations. For environmentalists and policy makers already struggling with excess industrial waste and pollution, this new source of cumbersome and poisonous refuse is a crisis in the making.

Figure 7.9 What is in a Computer?



Source: United Nations Environment Program.

Addressing this problem requires coordinated efforts on the part of government, industry, and consumers. Multinational ICT corporations bear a large portion of responsibility to create more sustainable products, utilizing a minimum of hazardous materials and allowing for longer useful lives rather than planned obsolescence. Consumers need to educate themselves about proper maintenance, recycling, and disposal methods, as well as the environmental impacts of the upgrade and throw-away mindset. And governments from the national to local levels, as well as international organizations, need to provide guidance and resources to both require and encourage proper recycling and safe disposal of ICT waste.

Recycling in particular is a critical component of the measures needed to combat e-waste. Many used items such as mobile phones and computers cannot always be easily recycled directly for reuse or refurbishing, and with dropping prices the markets for second-hand equipment are small. But many of the internal materials, including rare and hazardous metals, can be recycled and utilized in the manufacture of new ICT products. However, extracting these resources from discarded cyber trash can be a costly and complex process, not necessarily more cost-effective than using newly

mined materials. Government and industry cooperation can help reduce these costs and ensure sector-wide compliance with recycling mandates.

A number of government agencies, including several in less developed economies in Africa, for example, have taken initiatives to define e-waste disposal and recycling requirements and procedures. Africa has become a dumping ground in some areas for international e-waste, and so these issues are becoming even more acute in this region. In Kenya, the Kenya ICT Action Network (KICTANeT) organized a study supported by Hewlett Packard (HP), the Digital Solidarity Fund (DSF) and the Swiss Institute for Materials Science and Technology (EMPA), to examine the extent of e-waste and methods of treating it in Kenya, and develop a roadmap of policy responses.[47]

In 2010, the Nigerian government proposed issuing strong regulations governing the treatment of e-waste in the country, which has become one of Africa's largest cyber dumping grounds. The regulations would empower the government to investigate and prevent illegal waste dumping, including inspecting imported equipment to determine if it may be actually for sale and use, or is merely intended to be disposed illegally within Nigeria.

In Brazil, *info*Dev is working with the Department of Science and Technology to study best practice in the field of handling e-waste and to develop a national policy.

7.9. Regulation in a Global Era

Although regulators typically still function under national governments and legislation, the boundaries within which communications services are provided are increasingly artificial. Regional and global cooperation on most issues will become a growing challenge as the industry continues to expand and consolidate.

7.9.1. Cross Border Governance

One of the common themes throughout nearly all the new and changing regulatory trends arising due to the convergence and expansion of digital communications technologies is globalization. ICTs are perhaps the most central force driving the globalization of markets and integration of economies worldwide, and consequently the policy issues they raise are increasingly global in nature. Vast amounts of traffic and information passing across borders every day, through links and landing points which in principle connect one national network to another, but which are effectively invisible to users. Mobile services in particular are impossible to contain within artificial boundaries, and users often roam onto networks of neighboring countries. Many of the corporations that own and invest in telecommunications networks often own multiple licenses within a region, and some are looking to integrate services among markets. Technology has moved beyond national boundaries, and regulation must follow.

Regional and Global Cooperation

International cooperation has been a critical feature of the telecommunications industry since the earliest days of the telegraph. The ITU was founded in 1865 to facilitate and oversee international agreements on the development and use of the telegraph. As first telephony and especially wireless communication became prominent, the need for multilateral coordination grew even more essential, as radio signals don't stop at national boundaries, and intricate agreements were needed to minimize interference and assure compatibility among equipment and networks. Because most services were provided through state PTTs, these agreements involved government-to-government treaties. But as the telecommunications sector has moved to a privatized, competitive, globalized model, cooperation among governments has focused more on harmonizing regulatory practices.

In this context, ITU has continued to play the leading role, with 192 Member States and over 700 additional Sector Members and Associates. While continuing to coordinate worldwide utilization of radio spectrum and communications satellites and establishment of common technical standards for industry evolution, ITU has also established itself as a focal point for supporting governments and regulators in the developing world in particular. The ITU Telecommunications Development Bureau (ITU-D or BDT) is one of the three Sectors within ITU, along with Radiocommunication (ITU-R) and Telecommunication Standardization (ITU-T). As detailed throughout this chapter, ITU has established working groups, programs, and studies on nearly every major issue confronting telecommunications regulators and policymakers in the digital era. ITU also organizes worldwide and regional exhibitions, forums, and publications, including the ITU Telecom events, as well as the

annual Global Symposium for Regulators (GSR), which brings together regulatory officials and experts from scores of countries to address the prevailing issues confronting the sector in detailed and in-depth collective discussions.

Many other international organizations are also actively involved in promoting global cooperation on telecommunications regulatory policies. The World Bank has been among the most prominent in financing and advocating the transformation of ICT policy regimes while supporting establishment and capacity building for regulators around the world.

The Information for Development Program (*info*Dev) is a multi-agency partnership based within the World Bank, with a primary focus on helping to increase access to information infrastructure, applications and services, and supporting private sector ICT innovators and entrepreneurs. Among other activities, *info*Dev provides technical and financial support to improve regulatory and policy frameworks, increase capacity for design, implementation and monitoring/evaluation of ICT programs and projects, and to scale up successful pilot projects to increase their impact and sustainability. This work has included providing some of the most extensive information to regulatory authorities, in both printed and online formats. In 2000, *info*Dev published the first edition of the *Telecommunications Regulation Handbook* (ed. H. Intven) in order to provide a one-stop reference manual for the growing number of telecommunication regulatory agencies being formed around the world. More recently, jointly with the World Bank and ITU, it developed and sponsored the online *ICT Regulation Toolkit* on which the present *Handbook* is based.

During 2010, *info*Dev launched a project with partners entitled the Broadband Strategies Toolkit, which is likely to evolve into a similar body of knowledge for the promotion, regulation and universalization of broadband networks.

Several other United Nations agencies contribute expertise, research, funding, and program initiatives to global ICT policy deliberations: the UN Development Program (UNDP), Educational, Scientific, and Cultural Organization (UNESCO), Conference on Trade and Development (UNCTAD), and Commission on Science and Technology for Development (CSTD), among others. Many other development finance institutions and agencies also contribute significantly to policy reforms and regulatory strengthening in ICTs. They include the major regional development banks – the European Bank for Reconstruction and Development (EBRD), Asian Development Bank (ADB), InterAmerican Development Bank (IDB), and African Development Bank (ADB) – as well as national development agencies, such as the U.S. Agency for International Development (USAID), Canadian International Development Research Centre (IDRC), Japan International Cooperation Agency (JICA), and many more.

Also gaining in importance are regional regulatory associations and other multilateral institutions, which bring together officials from multiple countries to share information, coordinate policies, and advocate for the mutual interest of their members. These include Regulatel, the Latin American regulators association; the Communications Regulators' Association of Southern Africa (CRASA), the Economic Community of West African States (ECOWAS), the Arab Regulators Network (AREGNET), and the Eastern Caribbean Telecommunications Authority (ECTEL). Of course the European Commission and European Parliament take the lead in setting policy for the countries of the European Union. The Organisation for Economic Cooperation and Development (OECD) has established a Committee for Information, Computer and Communications Policy (ICCP), which undertakes a variety of studies and maintains international databases of ICT trends and policies. The Asia-Pacific Telecommunity (APT) is a focal point for ICT development initiatives for its 34 member countries. The Commonwealth Telecommunications Organisation (CTO) provides a variety of services in support of its members' telecommunications development policy needs. The Association for Progressive Communications (APC) is a global network of civil society organizations focused on enabling opportunity for developing countries through ICTs, with emphasis on policy, women's networking, and capacity building.

Representatives of all these groups, along with most of the world's governments and ICT companies came together in 2003 and 2005 to convene the World Summit on the Information Society (WSIS), a United Nations sponsored and ITU hosted worldwide event. Recognizing the increasing importance of ICTs and the need for high-level focus on shared policy perspectives and development objectives, the Summit participants

prepared first the Geneva Declaration of Principles and Plan of Action (2003), followed by the Tunis Agenda for the Information Society (2005), which identified a range of critical issues for the world community to address, particularly with respect to Financial Mechanisms to support ICT development, as well as Internet Governance (see below). Subsequent to the World Summit, the participants agreed that there should be ongoing follow-up and implementation activities, which have continued under the auspices of the UNCTAD, UNESCO, UNDP, and ITU.

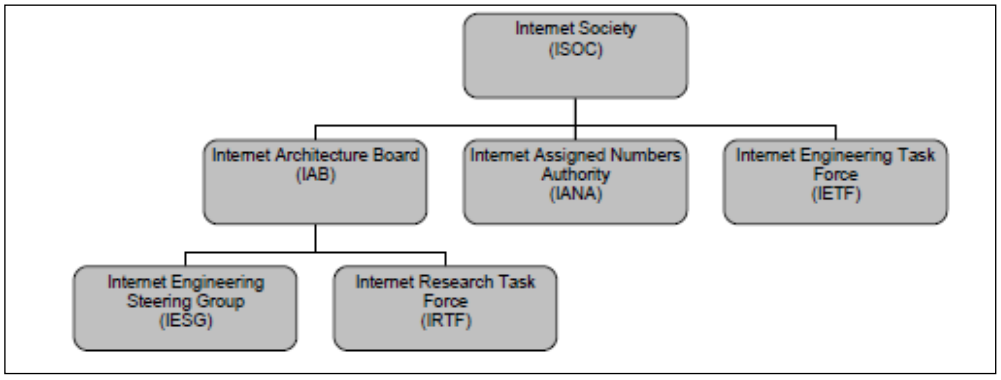
Internet Governance

One of the most vital new areas of international cooperation, and a key theme of the WSIS, is Internet governance: the policies and institutions that manage the day-to-day functioning of the global Internet, and its ongoing evolution. The globalization of ICTs and the central place of the Internet in nearly every society has given rise to increasing calls for changes to the historically United States-centric mechanisms which continue to dominate much of the Internet's oversight.

Because the Internet emerged from an unplanned and disjointed sequence of events, but was initially underwritten and operated by the U.S. Defense Department's ARPANET and later the National Science Foundation's NSFNET, most of the basic protocols and technical standards that still govern the Internet's operations were introduced and long controlled by the United States government. This control extended to the creation and financing, for example, of the Internet Engineering Task Force (IETF) in 1986, the informal Internet Assigned Numbers Authority (IANA) since 1988, and IANA's formal successor, the Internet Corporation for Assigned Names and Numbers (ICANN) beginning in 1998, all initially under U.S. government contracts.

The current institutional structure of Internet governance arose with the establishment of the Internet Society (ISOC) in 1992, which was organized outside of any official government agency, with membership open to any individual, organization, company, or agency with an interest in contributing to the Internet's development (see Figure 7.10). Over time, the ISOC has absorbed other organizations, including the IETF and the IANA (see diagram). However, the IANA's critical function of controlling naming and numbering conventions – the assignment of top-level domains among countries and ultimately the distribution of web addresses and associated URL numbering has remained with ICANN (which continues to administer IANA).

Figure 7.10 Internet Architecture Organizations



Source: ITU, The Future Internet, 2009.

This status quo, among other related issues, was central to the discussions and negotiations of the WSIS. Representatives of a majority of the world's governments as well as many international civil society organizations, took the view that governance of the global Internet should be permanently removed from the influence and control of any one government (the United States), and made the collective responsibility of a neutral international forum. The U.S. government has resisted this change, while proposing that ICANN should operate on an essentially autonomous basis as a non-

profit corporation. Coming out of the World Summit, negotiators did not agree to alter the role of ICANN for the present, but did establish a Working Group on Internet Governance, which went on to create the Internet Governance Forum (IGF) in 2006. The IGF is now responsible for convening multi-stakeholder meetings, discussions, and studies on the issues raised by the WSIS regarding Internet governance (most recently in Lithuania in September 2010, where its initial five year mandate was renewed) and to propose options for a way forward.

Innovative technological advances are having a revolutionary impact on the ICT sector and the economy as whole, requiring that all players (equipment manufacturers, operators, service providers, policy makers, regulators, and even users) reassess their traditional knowledge and decision-making models. In particular, traditional telecommunication regulators must respond to these fast-paced changes in order to enable their economies to thrive while protecting the public interest. For this, global cooperation will remain as vital as local innovation for years to come.

7.9.2. Cooperation across Sectors and Boundaries

The ICT sector is highly dynamic and rapidly changing. Therefore, making predictions of what is to come in the next decade is difficult. The deployment and take-up of ICTs, however, is happening at a faster pace than ever before, particularly with regard to developing countries and the use of mobile services and applications. This all creates further challenges for authorities. Nevertheless, market and regulatory trends over the past few years demonstrate increased competition in ICT markets and evidence a continued and deepening path of convergence both within ICT sector as well as with other sectors of the economy. As such, the following conclusions can be drawn:

- As markets become more competitive, regulators will need to shift to a more targeted approach towards intervention in the sector, withdrawing ex ante regulation where it is no longer warranted, and transitioning towards ex post rules. Development of strong competencies in the economic and legal techniques and methodologies for competitive analysis will be a critical input for regulators going forward. This will be particularly pressing in countries where competition law and authorities have traditionally been lacking or have had a very limited scope of action. Accordingly, ICT regulators should engage in capacity building initiatives to develop the necessary institutional know-how and make efforts to increase cooperation with competition authorities where possible.
- Continued convergence within the ICT sector will present regulators with new challenges associated with vertical and horizontal integration of on-line services and applications. New players are progressively developing novel equipment, devices, services and applications that have the potential of altering the ICT competitive landscape. However, when facing the challenges posed by nascent services and applications, regulators should exercise caution to avoid stifling innovation and investment. A light-hand approach is often-times the right regulatory response under these circumstances and may contribute to create the appropriate enabling environment for innovative services and applications to develop.
- Expansion of ICTs into our everyday activities will demand ICT regulators to increase their cooperation with different cross-sector regulators and policymakers, including in areas such as law enforcement, education, banking, health and the environment. Increase coordination of policies and initiatives in these areas, and likely many other, will be critical within the coming decade to harness the potential efficiencies that ICTs can bring to consumer and the society at large.