Digital Confidence

Securing the Next Wave of Digital Growth

LIBERTYGLOBAL
POLICY SERIES

booz&co.

Digital Confidence

Securing the Next Wave of Digital Growth

übersetzt aus dem Englischen

DIGITAL CONFIDENCE – KEY TAKEAWAYS

• The digital economy in Europe is expected to grow by 18 percent per annum until 2012 to a volume of €436 billion from €236 billion in 2008.

• Until recently, growth in the digital economy was largely driven by infrastructure rollout and technology development, such as digital TV (DTV) migration and next-generation broadband technologies.

• Going forward, there will be a very significant shift in value from access—though still profitable and growing, albeit at single-digit rates—to electronic commerce, online and digital content offers, and online advertising.

• Increased usage and spend per user will fuel strong growth in the next 5 years: Specifically, content and advertising businesses will show double-digit growth. e-Commerce will remain the biggest market in absolute terms.

• However, these growth drivers will have to prevail over major disruptive forces in the European Information Society such as Web 2.0 services converging across platforms (i.e., online, DTV, mobile) and a new "born digital" consumer generation that is hyperconnected and participative but also highly assertive, feeding into press and political action.

• With the growth and success of digital life have come many concerns for consumers and enterprises relating to the security and integrity of the digital environment.

• Therefore, enhancing Digital Confidence, as a measure of how much consumers and suppliers trust in digital and online services, is becoming a key growth enabler—or inhibitor—for the digital economy. €124 billion in market volume (2012) could be at risk, approximately 1 percent of GDP for the EU-27, with market value related to content and advertising being most exposed. The economic upside of being successful in increasing confidence and trust amounts to an extra 11-percent growth (or €46 billion) on top of the €436 billion base case. However, the downside of a failure to enhance Digital Confidence is greater: 18 percent (or €78 billion) could be lost or significantly delayed.

• All players in the industry agree on the importance of building up Digital Confidence credentials and have launched a wide array of activities accordingly—yet, to date, there is a clear lack of coherence and common focus, as most actions are ad hoc, having been triggered by high-profile incidents of trust or security breaches and political pressure.

• Legislation alone cannot keep up with the speed and scope of challenges in this market. Hence, successful companies do more than just comply with legislation; they stay ahead of the curve by adopting proactive policies and practices to drive Digital Confidence.

• Digital Confidence is built on four pillars, which, taken together, address the most vital areas of consumer and industry concern:

1. Network Integrity and Quality of Service (QoS). Focuses on providing secure and resilient enabling technology platforms for digital life and providing an optimal customer experience
2. Privacy and Data Protection. Addresses the security concerns of individuals with respect to their digital data
3. Minors' Protection. Seeks to defend the well-being of minors in the online world
4. Piracy and Theft Avoidance. Seeks to provide a secure digital business environment for all stakeholders.

• As owners of the client relationship, network operators are challenged to put in place policies and practices that find general user acceptance, which goes beyond compliance with legal requirements or serving the interests of particular stakeholders.

• Therefore, policies and practices should not be driven by single issues (e.g., piracy) but should reflect a holistic view of all Digital Confidence areas. The policy implications of these different areas converge in practice and have shown to produce contradictory reactions from stakeholders.

• Key lessons drawn from case studies around the world show that a "can-do" vision is realistic: With regard to enhancing Digital Confidence, network operators can go beyond their traditional roles of "mere conduit" and educator/teacher whilst observing guidelines for acceptable consumer practices and safeguarding legal safe harbours.

• Based on the cases analysed, best practices from a consumer acceptance point of view take shape:

  • Consumers accept practices that are transparent and unobtrusive—network operators and content and platform players, jointly with the regulator, are required to drive such communication forward.

  • Consumers are concerned about how network operators manage and safeguard consumers' digital data—clear statements and a consistent, reliable regulatory framework are key priorities.

  • Consumers require control over the risks to which they're exposed—they seek access to the appropriate tools, opt-in/opt-out mechanisms, and education.

  • Consumers accept measures that guarantee quality of service—if this requires active traffic management, they are open to it, provided there are clearly communicated terms of service.

• To ensure proportional levels of intervention, and to find general user acceptance, when adopting more pro-active policies and practices, network operators should use a graded approach following the E3 paradigm: Educate first; Empower second; Enforce selectively where required.

• Digital Confidence policies and practices need to be embedded within the respective organisations by establishing internal protocols and governance structures to guide product and service roadmaps; choice and deployment of network-based technologies and security solutions; and communication to customers and other stakeholders (e.g., industry peers, content owners, regulators).

I. EXECUTIVE SUMMARY

THE NEXT GROWTH WAVE IN DIGITAL LIFE: USAGE, NOT THE NUMBER OF USERS, DRIVES GROWTH

Europe's digital economy has a strong prospect of growth spurred by Web 2.0–type services that have become mainstream using the functionality, ubiquity, and increased capacity of broadband networks. The migration to next-generation access networks, proliferation of highly sophisticated network technologies, and rise of a new generation of increasingly assertive "born digital" consumers are potentially disruptive forces for the digital economy ecosystem. This new paradigm is a significant challenge for the industry at large as well as for policymakers and regulators.

The stakes are very high: We expect the European market for digital services to grow to €436 billion by 2012, with a compound annual growth rate of 18 percent (2007–2012).

To date, growth in Internet usage has been driven largely by the rollout of new technologies (e.g., broadband access and DTV). The technology enablers now in place have nearly saturated many Internet access markets. The next wave of digital growth will therefore be driven mainly by increasing revenues through growing spend per user rather than increasing the number of users. This growth is expected to be achieved through more innovative products and services complemented by new business models generating incremental revenue streams. The main economic growth areas identified are, in order of their respective growth rates: Advertising, content, e-Commerce, and access.

With the growth and success of digital life have come many concerns for consumers and enterprises relating to the security and integrity of the digital environment. The level of trust that consumers place in service and platform providers in terms of business conduct and the provision of secure service and network environments, as well as their confidence in the ability of governments and regulatory authorities to enforce consumer protection standards, is now a major factor affecting digital economy growth.

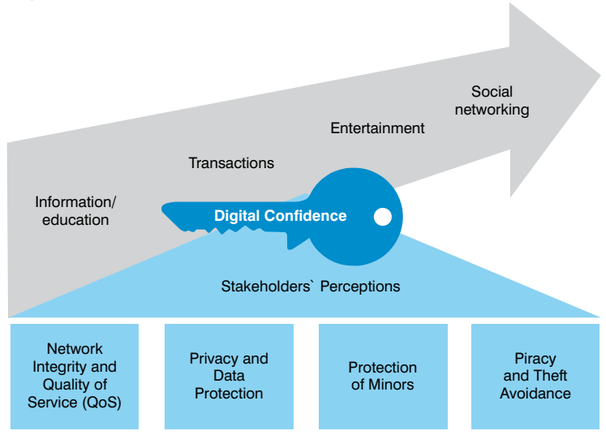
There is an urgent need to develop a common view about priorities in the areas of enhancing trust and security, defining the roles and responsibilities for each player, and understanding appropriate tools and measures that can and should be applied. The objective of this report is to provide a fact base for the debate and introduce frameworks, common language, and ideas to facilitate a joint view and joint—or coordinated—policies and action where appropriate.

DIGITAL CONFIDENCE: SECURING THE FUTURE GROWTH OF DIGITAL LIFE

Against this backdrop, promoting and enhancing trust and security becomes a key driver for the future growth of digital life. This driver is particularly important because consumers "born digital" are increasingly assertive and quick to react by reducing usage or feeding into press and political action—often leveraging Web 2.0 technologies. Based on interviews with 50 experts from across Europe and the United States and on a systematic review of market data and industry best practices and perspectives, we believe that four interrelated pillars address the most vital areas of consumer and industry concern associated with digital life today, and going forward:

- The **assurance of network integrity and quality of service** for consumers and businesses related to protecting technology platforms against criminal security attacks, ensuring optimal Internet connectivity despite peaks in traffic load or external criminal attacks, and securing

Digital Confidence framework



the computing environment for consumers and businesses against disruption through viruses and other malware.

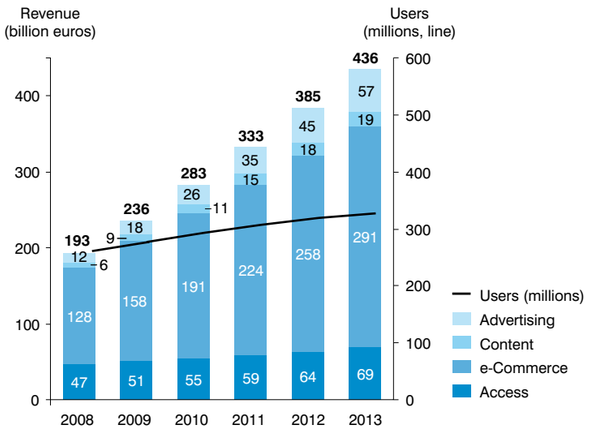
- The **protection of privacy and personal data,** that is, preventing consumers' private electronic data (e.g., identities, passwords, usage, and consumption profiles) from being accessed, published, or commercially exploited without consent, and preventing identity theft and fraud.

- The **protection of minors,** that is, protecting children from exposure to undesired content, preventing bullying and other hostile behaviour, preventing grooming or other forms of children's solicitation by adults, and fighting child sexual abuse content.

- The **avoidance of piracy and theft,** that is, countering the theft of copyrighted content and protecting e-Commerce transactions for all parties.

Industry needs to act proactively based on a holistic view of these issues. Such an approach has been captured in the concept of "Digital Confidence." Digital Confidence transcends legal compliance—it is fast becoming a commercial prerequisite and a license to operate. As certain case studies will show, legal compliance alone does not buy consumer acceptance. Operators' policies and business practices need to address all legal, economic, and public policy stakes associated with these areas, together and coherently, to enable the next phase of growth of digital life.

Digital life—revenue summary Europe



Note: Europe including EU-27, Norway and Switzerland
Source: Forrester e-Commerce Forecast, Company Report Apple, Company Report Google, EU TV and Broadband Forecast Model, Booz & Company Analysis

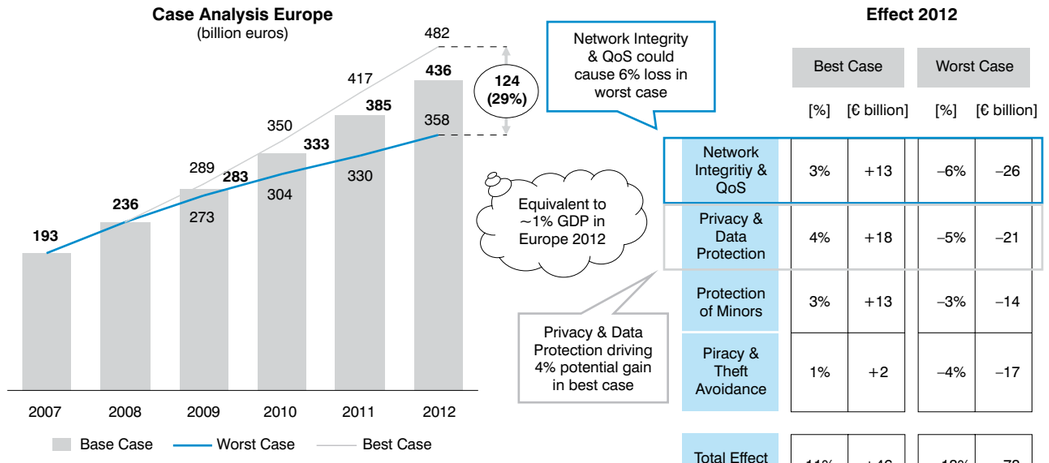
RISK/BENEFIT ANALYSIS: DIGITAL CONFIDENCE PAYS OFF

According to Booz & Company research and analysis, a €436 billion digital access, commerce, content, and advertising market with 18 percent compound annual growth is at stake in Europe by 2012. The difference between "getting Digital Confidence right" in a best-case scenario and "getting it wrong" in a worst-case scenario adds up to €124 billion, or almost 30 percent of the total market at stake—approximately 1 percent of total EU-27+2 GDP in 2012! The combined downside of failing to establish Digital Confidence is, at €78 billion, far greater than the upside at €46 billion—primarily driven by the effects of Privacy and Data Protection as well as Network Integrity and Quality of Service, which impact all the revenue areas of the digital economy and the level of use and number of users across the major revenue categories.

Privacy and Data Protection is financially important, especially but not only because its implications for innovative (targeted) advertising business models. Consumers may become less willing to undertake e-Commerce, digital content purchases, or subscriptions to innovative digital services if they don't trust how their personal data are being handled and secured. Network Integrity and Quality of Service will be required to support the continued growth of content and video services. Managed well, networks will be able to deliver high bandwidth at a quality of service that supports digital life for all users. In addition, the area of Piracy and Theft Avoidance is relevant for content owners as well as for e-Commerce. Apart from the obvious revenue implications for the content industry in protecting existing value of their rights portfolios as well as in introducing innovative digital and online content business models, there is a sizeable risk related to the negative impact on e-Commerce transactions due to people shifting consumption to offline channels, which is not possible for many new business models (e.g., online auctions).

The revenue categories most sensitive to Digital Confidence concerns are content and advertising markets. Both markets are in a nascent stage and their development is highly dependent on Digital Confidence: Advertising could be severely held back by adverse reactions of consumers if not implemented in ways that find general user acceptance, or by too restrictive legislation. For example, protecting consumer privacy very restrictively may impact new business models based on targeted and personalised advertising—a major contributor to the

Digital Confidence impact



Note: GDP Europe 2012 estimated at roughly 12.5–13.5 tn EUR (Europe: EU-27 + Norway + Switzerland)
Source: European Union, Booz & Company Analysis

projected €57 billion online advertising market in Europe in 2012. Moreover, advertising will play a central role in monetising all emerging and fast-growing Web 2.0 services such as social networking sites and innovative content offers. Content providers fear that excessive piracy could fundamentally challenge their digital business models. e-Commerce is relatively less exposed but shows the highest absolute impact due to its large business volume, contributing €52 billion to the potential downside, and half of that to the potential upside, of Digital Confidence.

The risk/benefit analysis shows that, in purely economic terms and disregarding for a moment the wider societal aspects, the digital industry has a significant economic incentive to coherently address all areas of Digital Confidence to at least avoid worst-case revenue scenarios and ideally to strive for best-case revenue potential.

All players in the industry agree on the importance of building up Digital Confidence credentials and have launched a wide array of activities accordingly—yet, to date, there is a clear lack of coherence and common focus, as most actions are ad hoc, having been triggered by high-profile incidents of trust or security breaches and political pressure.

The key distinction between the best- and worst-case scenarios is the level of alignment between the industry players in the approach to Digital Confidence. Alignment does not necessarily mean that players do all things in an identical way; rather, it is the level of agreement across the industry to follow the same direction. It refers to the extent to which there is a common understanding of such a direction and the overall priorities as well as of the resulting responsibilities of each stakeholder.

Network providers need to continue to play an important role because their core business is a key enabler for the identified economic growth drivers. The level of network integrity has a major economic impact even if a provider's own core access business seems least exposed to the benefits or risks of getting Digital Confidence right or wrong.

FRAMEWORK FOR ACTION

All four pillars of Digital Confidence need to be addressed as a matter of urgency. They are highly interdependent, with all areas contributing to users' overall awareness of the digital world being safe or unsafe.

Due to the complexity of the issues involved and the interdependence of many players across the value chain, it becomes obvious that everyone in the digital economy has a role to play. While network operators are instrumental in many areas to deliver a solution, it is clear that they can contribute only their part to the overall puzzle.

To map out the various roles that network operators can play in the identified areas of concern, a Digital Confidence Positioning Framework has

been developed. This framework depicts how measures are taken (e.g., passively in a "hands-off" manner or actively in a "full-control" approach) and differentiates the underlying principles. The resulting roles can be clearly linked to generic societal roles. For example:

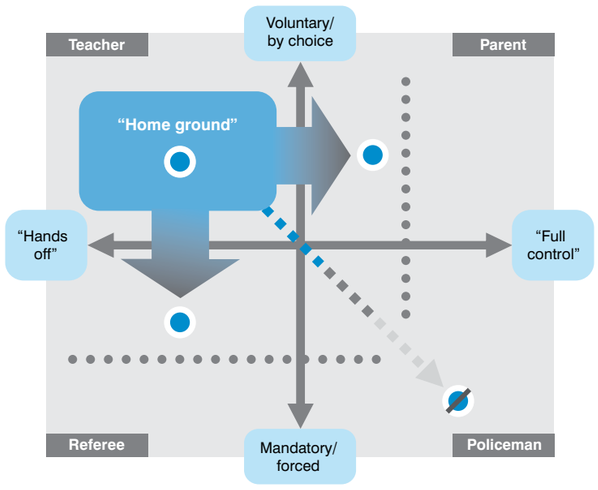
- The teacher educates users about opportunities and threats as much as possible, but will normally not take active corrective measures (e.g., "Web Wise Kids" producing educational material for children on the Internet).

- The parent educates users about threats and measures, similarly to a teacher, but will take measures proactively if deemed necessary to protect users (e.g., YouTube filtering copyright protected content).

- The referee relies on self-imposed enforcement of rules on a case-by-case basis and on guidelines rather than on education, but rules are based on mutual agreement (e.g., UPC NL proactively restricting access to child sexual abuse content domains).

- The policeman is naturally inclined towards strong enforcement based on legal mandating, takes all measures necessary to do so, and does so based on strict rules such as to block all illegal activities (e.g., the implementation of a "three strikes and you're out" rule in case of copyright infringement).

"Home Ground" positioning for Network operators



In defining their positions in this field, network operators need to be very careful, however, when assuming roles outside of their primary business activity and responsibility. Any move that may undermine their safe harbour of "mere conduit" and expose them to uncontrollable liabilities will ultimately not enhance Digital Confidence—whilst raising expectations among the public to the contrary.

Based on our analysis of successes and failures in the area of Digital Confidence, there seems to be a traditional home ground along these dimensions for network operators: The position referred to as the "teacher"—which focuses on educating users about opportunities and threats as much as possible, but will normally not take proactive corrective measures. But our analysis clearly shows that leaving this home ground only to comply with legal regulations will not be enough going forward.

Legislation often cannot keep up with the speed and scope of the changes related to Digital Confidence. As owners of the client relationship, network operators are challenged to put in place policies and practices that find general user acceptance, which goes beyond compliance with legal requirements or serving the interests of particular stakeholders.

Hence, successful companies do more than just comply; they stay ahead of the curve by adopting some key principles to drive Digital Confidence:

- They work on confidence-building procedures and protocols.

- They are as open and transparent as possible in their communication with consumers.

- They make an extra effort to educate and enable consumers to protect their interests in the digital world.

To ensure proportional levels of intervention, and to find general user acceptance when adopting more proactive policies and practices, network operators should also use a graded approach following the E3 paradigm: Educate first; Empower second; Enforce selectively where required.

Based on the cases analysed, best practices from a consumer acceptance point of view take shape:

- Consumers accept practices that are transparent and unobtrusive—network operators, service providers, and content and platform players, jointly with the regulator, are required to drive such communication forward.

- Consumers are concerned about how network operators and ISPs manage and police consumers' digital data—clear statements and a consistent, reliable regulatory framework are key priorities.

- Consumers require control over the risks to which they're exposed—they seek access to the appropriate tools, opt-in/opt-out mechanisms, and education.

- Consumers accept measures that guarantee quality of service—if this requires active traffic management, they are open to it, provided there are clearly communicated, fair, and transparent terms of service.

These principles apply to all stakeholders.

As a next step, Digital Confidence policies and practices need to be embedded within the respective organisations. Exploring the implications for network operators, it is essential to align activities to achieve the next level of Digital Confidence. Providers need to act at five levels:

1. POLICIES AND PROCEDURES

Network operators and ISPs must have a Digital Confidence positioning statement defining their strategy and position for each confidence pillar. This needs to be the basis for all Digital Confidence-related policies. The positioning statement needs to be precise enough to provide tangible guidance on the underlying questions related to these issues, for example, "How does a company balance the trade-off between inappropriate content and freedom of expression?"

As a next step, these policies need to be embedded in the core processes of the company. In most cases this will have direct impact on the way network operators think about product development, for example, by making sure that all product and service releases meet the own standards.

In addition, network operators must keep Digital Confidence policies and procedures up to date by conducting regular legal, public policy, and technical reviews of existing policies and procedures.

Last but not least, as the cases analysed in this report show, confidence requires trust, and trust can best be built on open communication; transparency pays off. As a consequence, companies should be open about the policies they apply and the rationales behind them—including business rationales. Consumer acceptance is generally high if rules and underlying rationale are openly communicated. This also opens a dialogue with the consumer, which can be very helpful to improve solutions.

2. GOVERNANCE

Digital Confidence is complex, very sensitive, and cross-functional in nature. Very often, it is required to define fundamental positions for the company—for example, "How do we deal with sexual abuse content?" Getting it wrong bears high reputational and financial risks. Hence, it is of utmost importance to devote sufficient top management attention to the subject. Digital Confidence should be clearly embedded in the organisational structure, through, for example, a Digital Confidence Board with senior oversight including the authority to oversee and implement all related activities.

3. TECHNOLOGY

Enabling technologies are largely in place for Digital Confidence, and the focus of attention turns to deciding individual positioning, defining appropriate policies, and establishing the supporting governance structures. Nevertheless, there are certain technology-related investments that will need to be made by the majority of network operators to prepare for the future. They relate to ensuring that the quality of service can be maintained despite the increasing levels of multimedia traffic. Network operators will need to make investment decisions by managing the trade-off between adding further transport capacity and active traffic management, that is, via tiered pricing or technical measures. Network operators and ISPs will need to work with content providers to optimise their networks for multimedia content delivery through technologies such as peer-to-peer caches (e.g., approaches developed by the P4P initiative) or content delivery networks. Regulators will need to know that they have addressed the issue appropriately.

Another major technology area of risk currently relates to end-user equipment. Such equipment is generally not sufficiently protected from threats such as viruses, botnets, and other forms of malware. Software solutions already exist; however, network providers should be even more active in encouraging customers to use them. Service providers must also deploy tools and solutions that empower consumers to control and manage their own exposure (e.g., via an opt-in/opt-out facility). This will require a step change

in the level of activities: Offering solutions for download on the website is not good enough; network operators and ISPs should launch programmes to drive and track the number of installed solutions.

4. CONSUMER EDUCATION

Network operators and ISPs should engage in industry programmes jointly with NGOs and undertake their own appropriate education initiatives (e.g., information campaigns on their own websites).

These programmes need to cover threats related to data publication, targeted advertising, piracy, and online behaviour overall (including what constitutes bullying, solicitation, and unacceptable content).

Education messages should be targeted to specific user groups, including parents and children. The parents' programme should focus on how to monitor children's activities, build awareness of the threats of the environment— and showcase the tools available to parents to manage their children's online environment. Children's education should focus on recognising and dealing with threats.

5. REGULATION

Network operators and ISPs need to encourage regulators to focus on specific actions to support industry's endeavours in proactively building confidence in areas that clearly fall outside service providers' activity (e.g., blacklisting of illegal content, law enforcement). Regulators should be careful not to proactively create regulatory obligations in these areas unless the proportionality of those measures can be ensured.

In response, industry needs to demonstrate that it is serious about Digital Confidence by taking the initiative to develop coherent solutions. Such solutions must have the commitment of all players and need to proportionately allocate the cost of implementation and the resulting financial rewards. Regulators must allow industry to develop such solutions and foster stakeholder cooperation and financial support programmes whilst allowing competitive pressures to work in favour of consumer interests being upheld, rather than applying regulation that, although well-intentioned, may be counterproductive from a consumer point of view and cause economic damage. For example, our analysis shows that a strict quality of service regulation banning most forms of traffic management could increase the capex requirements of network operators across Europe by up to €6 billion. In executing measures across these five initiative areas, network operators and ISPs are overall well advised to cooperate with NGOs as broadly as possible. Many aspects can be addressed much more effectively if one provider takes the initiative jointly with an NGO because the latter can ensure neutrality and industry-wide applicability, leveraging the good reputation NGOs have. Recent surveys show that NGOs rate highly in consumer trust.

PRIORITIES FOR REGULATORS

Regulators and government agencies are challenged to define their position in this field, which oscillates between censorship and consumer education, heavy regulation and free market, self-regulation philosophies. The cross-border nature of Digital Confidence threats places particular emphasis on international (judicial) cooperation to increase awareness of the urgency to act and, for governments and enforcement authorities, to allocate appropriate resources to establish effective mitigation structures and partnerships with industry. To date, the lack of a coherent approach comes ultimately to the detriment of the consumer, who lacks transparency and guidance around the risks and benefits of digital life, whilst businesses are challenged to create sustainable, new digital business models.

There appears to be a trend in politics and regulatory policies to put greater emphasis on stakeholder cooperation and co-regulation instead of greater legislative activity. At the same time, there will be a need for continued review of the proportionality of any regulatory activity, particularly with highly interventionist approaches (such as "three strikes" or moves towards imposing mandatory network filtering) that may infringe on basic Internet freedoms and basic consumer rights (e.g., to privacy) and undermine vested legal certainties for industry players.

Undoubtedly, regulators have an important role in securing Digital Confidence. Given the complexity of Digital Confidence issues, for example, regulators can help foster increased stakeholder cooperation. The following areas deserve continuous attention of regulators:

- Encourage network operators and ISPs to establish Digital Confidence policies and procedures as well as codes of conduct based self-regulation on industry level—particularly in areas where more intrusive regulatory intervention could lead to negative economic results (e.g., on traffic management) or infringe basic consumer rights (e.g., "three strikes" rule).

- Consider measures to limit the legal and in some instances reputational risk for network operators and ISPs introducing Digital Confidence policies and procedures, for example, lead the development and foster the industry-wide deployment of a register of sites banned in the interest of minors' protection—and, in Europe, harmonise the current, scattered approaches across countries, including establishing structures for internationally coordinated proceedings for minors' protection.

- Create incentives for industry players to take a more active role in consumer education—provide funding and establish umbrella initiatives to leverage scale, for example, building on experiences gathered from the Safer Internet program.

- Increase the effort for international cooperation to develop global solutions or frameworks for solutions to essentially global problems, for example, in the area of copyright protection.

- Put a special focus on the interdependencies of the different areas of Digital Confidence for the different stakeholders, and balance decisions accordingly. For example, enforcing very strict quality of service requirements could unintentionally create significant network upgrade costs that may ultimately increase costs for the consumer.

In summary, Digital Confidence does not necessarily cost a lot—in terms of required investments—to get right. On the other hand, the cost of getting it wrong would be substantial. However, getting a Digital Confidence programme right is neither easy nor free. Most CEOs believe that their organisations are engaged in many of the activities suggested above—and rightly so. But in most cases, this will not be enough. Digital Confidence transcends making educational material available on the corporate Web site. It is about engaging with the leading institutions in this field—private and public—at a senior level and launching serious campaigns that make a difference. This will require funding and potentially new skills in the organisation. Digital Confidence is not just about having a data privacy policy on file; it is also about changing the way a company thinks and communicates about these topics internally, with its customers and the community at large. In short, Digital Confidence requires leadership from the top in order to prevail.

II. THE NEXT GROWTH WAVE IN DIGITAL LIFE: USAGE, NOT THE NUMBER OF USERS, DRIVES GROWTH

1. DIGITAL LIFE: INTRODUCTION

Digital technologies have revolutionised everyday life—from the office to the home—at breathtaking speed. Decreasing development cycles and, as a result, ever-more-powerful devices, when combined with drastically shortening replacement cycles of technologies in the home, have led to a mass market penetration of digital technology. Whether it is connecting and communicating with friends, watching movies, listening to music, or taking pictures—life today is digital. Digital technologies have long stepped out of their niche as a toy for technology-savvy "geeks" to be at front and centre of modern life. Most consumers today find it more upsetting to lose their Internet connection at home than to lose their telephone service.

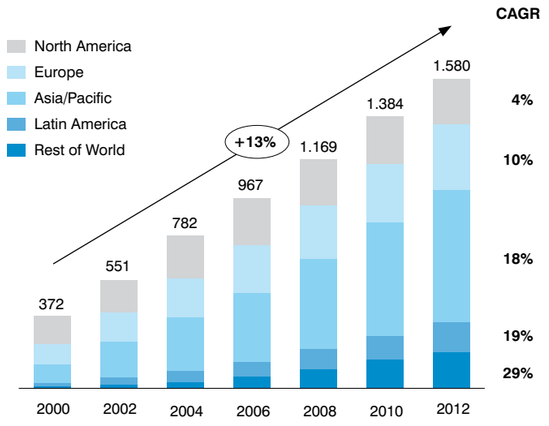
The latest development of digital services, ranging from digital TV to so-called Web 2.0 applications, has made this fact strikingly clear: The full potential of digital technology and services is unleashed only if technologies and applications are networked, physically and logically. What is the true revolution in digital photography: The fact that celluloid film rolls disappeared from the shelf, or the fact that pictures today can be shared with friends in minutes? In particular, Web 2.0 applications like Facebook and YouTube that focus very much on community aspects of digital technology underline this point. When communication, community, content, and commerce are combined, the value added for the consumer is tremendous—and in many instances profoundly innovative. The exploding growth rates of these services in all Western economies and beyond are an impressive testimony. Interestingly enough, all of these services take immediate advantage of the community aspect for their own purposes: Viral marketing, that is, word-of-mouth or PC-to-PC communication, is the main growth driver. All of this is possible only in a networked environment.

In this context, it is important to note that the majority of European households are or soon will be equipped with three digital network connections: Internet, digital TV, and mobile. All are capable to different degrees of delivering broadband services, and all—again to different degrees—are interactive.

Internet and broadband penetration levels are now reaching saturation as penetration has reached 70 percent across most central European markets.

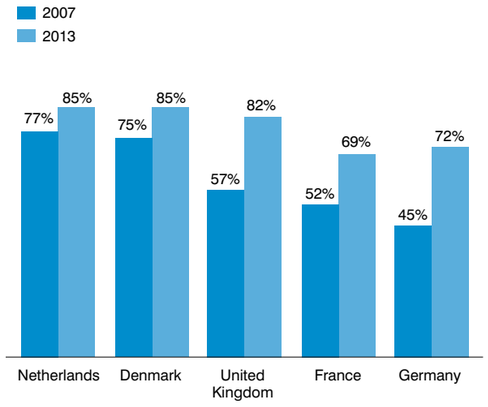
The current migration of broadband networks to next-generation access networks will further accelerate the development of digital life. Next-generation networks of cable providers (based on EuroDOCSIS 3.0 technology), telecommunications incumbents (xDSL), mobile operators,

Exhibit 1: *Internet users global (million users)*



Source: Economist Intelligence Unit

Exhibit 2: *Broadband penetration (percentage of households)*



and local FTTH network providers, in combination with wireless clusters like digital terrestrial networks and satellite, will address demands for increased broadband speeds, ubiquitous connectivity, and individualised media consumption across platforms.

The availability and level of acceptance of the Internet are such that the penetration of broadband is in excess of 70 percent in many European countries and has achieved mass market status similar to other media formats such as television and radio. This fact is also driving the next wave of change in consumer behaviour: More and more consumers expect to access the service they choose at the time and place they decide using the device available.

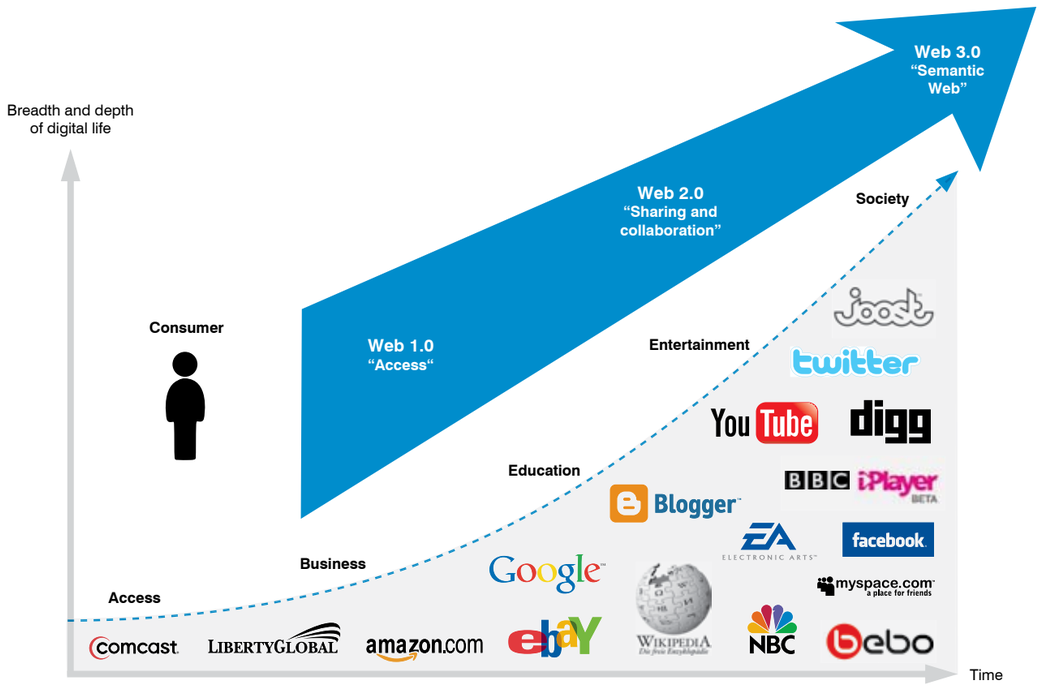
Consumers are shifting behaviour patterns, not only by spending more time online but also by interacting more online—through social networks that provide the opportunity to exchange content and ideas. On the supply side, comparing more traditional media companies with the new digital giants shows very clearly where the growth was in recent years (Exhibit 4). And even within the category of more traditional media companies, those companies with more online involvement grew faster than the others: News Corp., with its strong digital initiatives such as MySpace, is a good example.

2. DIGITAL LIFE: A DEFINING FORCE IN TODAY'S ECONOMY, POLITICS, SOCIETY, AND EDUCATION

To date, growth in Internet usage has been driven largely by the rollout of new technologies. End-user equipment, such as PCs and mobile devices, provides cost-effective access and storage platforms. Broadband networks are migrating towards ultra-high-speed next-generation networks. All relevant infrastructures provide high capacity (with standard broadband providing around 5 Mbps, and in more developed countries up to 25 or even 100 Mbps) combined with interactive capabilities and always-on functionality. Indeed, mobile network operators (MNOs) have finally introduced the mobile Internet with the widespread availability of 3G across Europe.

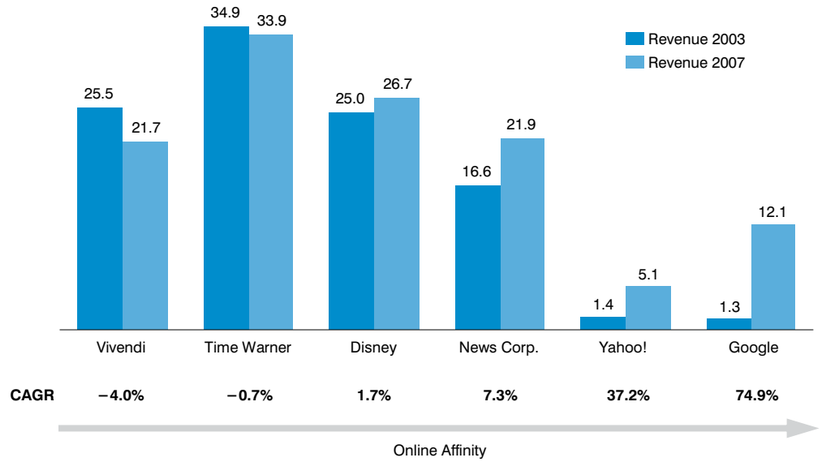
The technology enablers now in place have driven the penetration levels of Internet access to near-saturation in many markets. Thus, the next wave of digital growth will be driven by exploiting the enabling technologies to a far greater

Exhibit 3: *Digital life evolution*



Source: Booz & Company

Exhibit 4: *Revenue, online companies vs. media companies (revenue in billion euros)*



Source: OneSource, Company Reports

extent rather than penetrating them further. This implies changing usage or user behaviour much more than increasing the number of users. And we are seeing this already today in many markets. Consumer behaviour is changing dramatically: The main source of information influencing the buying decision for a car is the Internet; every third book sold in the United States today is sold online through Amazon; and U.S.-based cable operator Comcast registers roughly 40 million on-demand movie downloads per month.

In response to the changing media consumption patterns, businesses are embracing the power of the Internet for advertising and marketing purposes—in the UK, for example, more than 15 percent of advertising spend is allocated to online media.

The Internet and the digital environment in general have developed into a very attractive platform for diverse advertising and marketing activities: First, consumers spend an increasing amount of time with digital media; and second, digital media has both huge efficiency and effectiveness advantages over other advertising formats—a crucial point. Many sophisticated advertising approaches, especially those that aim to increase their relevance to the individual consumer, can be deployed only if the digital media exploits a wealth of user and usage information.

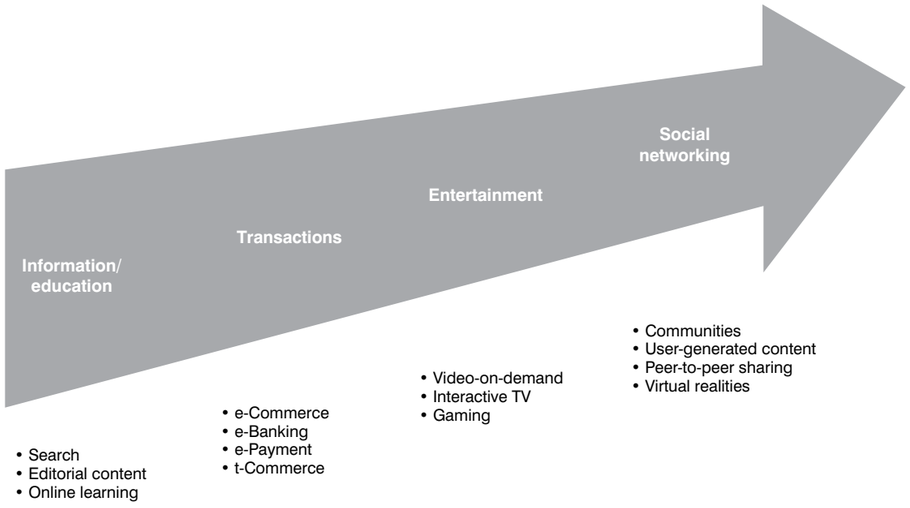
The Internet has changed industries Internet: Amazon sells more than $4.5 billion worth of books in the United States, accounting for every third book sold, comparable to Barnes & Noble in traditional sales.

For example, users of Google's e-mail offering, Gmail, are shown advertising tailored to the content of their e-mails. In the same way, browsing history, actively administered profiles, and other data can be used to tailor advertising to individual consumers. Also, in digital TV, user data and usage data can be tracked via the set-top box and used to present targeted advertising to specific segments or individual users. And with interactive DTV, advertising offers the same interactive response features as online.

Advertisers are now allocating more of their spend to the Internet—online advertising represents 15 percent of the overall advertising in the UK.

Achieving a high level of privacy protection is a very important concern from a consumer point of view that needs to be addressed with great care even when users' Internet traffic data are used for commercial purposes on aggregated, anonymous levels. But as intrusive as this may sound at first, experience shows that tailored advertising can increase consumer acceptance, if done well, because the advertising is relevant to the consumer. In addition, there are many ways to design such advertising so that unwanted participation is avoided: Via opt-in or opt-out procedures. For example, users can be given the choice not to have their data used for targeted advertising—but may then increasingly be asked

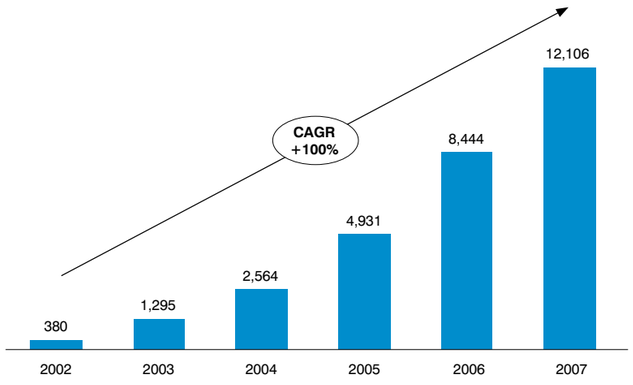
Exhibit 5: Digital life—growth levers



to pay for services in order to contribute to the revenue lost on the advertising side. Moreover, advertising will remain one of the major means for financing many services and offerings in the digital environment, just as advertising has been financing traditional media for decades.

Against this backdrop and with the digital economy ex-periences of the last 15 years, it is very likely that advertising in a broad sense will be one of the major revenue categories to support the future growth of the digital economy. Managing the actual and perceived intrusion on digital life is a prerequisite for capturing that growth. Particularly against a background of increasing pressure to monetise new Web 2.0 services, this will be one of the biggest challenges for all industry players concerned.

Exhibit 6: *Growth of Google (revenue in million euros)*



Source: Google

From an application perspective, we see four major growth levers for digital life:

- **Information and Education.** The traditional Web 1.0 applications combined with some Web 2.0 tweaks like user-generated content, for example, in e-Learning.

- **Transactional Services.** Mainly e-Commerce and online banking.

- **Entertainment.** Digital TV, video services (streaming video and video on demand offers like YouTube), and gaming as well as download services such as iTunes.

- **Social Networking.** All services built around the interaction of people, for example, in communities, exchanging content mainly generated by themselves or meeting in virtual realities.

INFORMATION AND EDUCATION

Information—in particular, search—has been one of the main drivers of growth in Internet usage from the beginning. Search engines have achieved notable success in translating the plethora of data available on the Web today into information meaningful to end users.

The Internet is also facilitating collaboration and providing consumers with education through user-generated content and ideas, for example, Wikipedia—which has amassed more than 10 million user-generated articles in 250 languages. Started only in 2001, Wikipedia is developing into the most accessed source for (encyclopaedic) information, not among Internet offerings alone—but overall. It is thus becoming one of the most important education and research tools in existence—even leading to discussions about students losing the ability to do "real" desk-based research in libraries. The open and community nature of Wikipedia, both in terms of its user-generated content as well as its user control, makes it a prime example of a true Web 2.0 application entering into the information space. According to some, its dynamic nature may provide more accuracy than many other, more static, information sources.

Over 45 percent of companies use Internet-based training regularly.

Digital TV is another major driver of the information age. The TV channels broadcast in Europe have reached the staggering number of 1,703 (in 2005) starting from 93 just 18 years ago. A large number of the channels available to consumers today offer news, documentary, or foreign language programming that was non-existent or not accessible in the analogue world.

Universities and other higher education institutions increasingly leverage the possibilities provided by the Internet to distribute information very effectively and to allow convenient and rich interaction, supported by solutions such as WebEx (a Web conferencing and collaboration solution). Particularly, distance learning, which involved many physical tasks 15 years ago (e.g., people travelling, exercises being sent in), is fully embracing these possibilities. Several universities and colleges (Open University in the UK, for example) started to engage in Second Life to leverage it as a virtual classroom environment. Businesses as well deploy the Internet and associated digital media to deliver training to their employees, deploying formats such as Webcasts or Web-based training (WBT), an extension of the traditional computer-based training (CBT).

Information and education will continue to be important growth levers for digital life. In particular, search supported by online advertising will continue to grow strongly. Google, the role model for translating search into advertising revenue, has enjoyed a compound annual growth in revenue of more than 100 percent over the past 5 years as it pushed out its business models aggressively and kept innovating its offerings very dynamically in order to reach an audience of more than twice the size of the largest European TV broadcaster.

TRANSACTIONS

The Internet has proved to be a medium ideal for transactional activities.

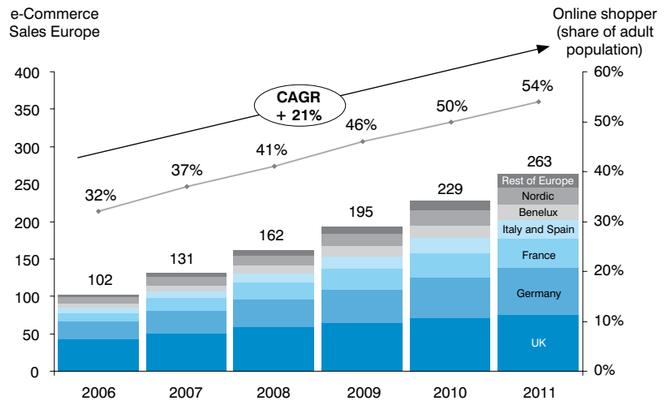
When shopping online, consumers enjoy competitive pricing aided by comparison sites, among many other advantages. Today, with more than 40 percent of consumers shopping online, annual e-Commerce spending is in excess of €150 billion in Europe, having grown by 50 percent over the past 2 years. This e-Commerce spending today accounts for more than 4 percent of total European retail sales, predicted to grow to 11 percent in 2011. For certain products like event tickets, travel, and media (e.g., books, music, video, and software), the share in 2011 is predicted to be between 25 percent and 35 percent.

More than 40 percent of consumers are shopping online, and e-Commerce now accounts for more than 4 percent of total European retail sales.

In addition, the Internet has revolutionised the way consumers operate their finances by allowing digital transactions. While the Internet succeeded in establishing a significant level of confidence in its—generally solid—security, e-banking has developed into a mass phenomenon. And alongside the growth of e-Commerce, a broad array of e-payment solutions such as PayPal have been established to support the increasing drive towards purchasing goods and services online. With the especially high sensitivity around financial transactions, however, these fields obviously are exposed to security concerns.

New businesses have been established based on Internet-only models that take advantage of the opportunity to operate a virtual business

Exhibit 7: *e-Commerce retail sales Europe (billion euros)*



Source: Forrester

model at a fraction of the cost of a bricks-and-mortar business; they leverage the power of the Internet as a low-cost sales channel and as an enabler for efficient supply chain management. Also, bricks-and-mortar businesses benefit from an additional low-cost platform for customer service and billing activities—often charging a premium for users unwilling to use the Internet service. Mobile operators, for example, introduced Internet-only offerings a few years ago.

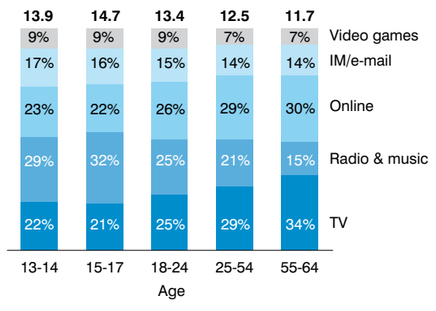
ENTERTAINMENT

Probably the most profound change the digital life is bringing to most consumers is in the area of entertainment. The average consumer in Europe spends between 160 and 240 minutes watching television per day, and up to another 140 minutes using the Internet—increasingly for entertainment purposes as well. With these activities taken together, using or consuming interactive media is by far the number-one leisure activity in Europe in terms of time spent. And this experience is changing dramatically. The Internet is already becoming the leading media format in many developed economies with people spending more time online and with e-mail than watching TV (Exhibit 8).

As consumers have increasingly busy schedules, they are looking to on-demand entertainment services that allow them to watch what they want, when they want, and how they want. The higher capacity of broadband networks allows services such as video on demand to be delivered cost-effectively.

Digital TV is about to revolutionise consumers' TV experience. Recent years have brought explosive growth in the number and diversity of TV channels, with many regionally or thematically specialised channels being added.

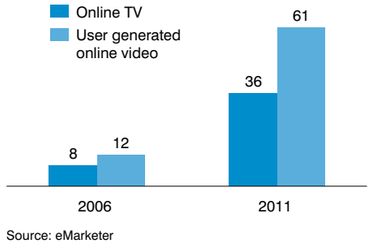
Exhibit 8: *Time spent with media per day, United States 2007 (hours per day)*



Source: eMarketer

In addition, digital TV enables significantly better image quality with HDTV offerings. Digital TV also introduced a number of genuinely new functionalities such as video on demand and time-shifted TV, and it supports special features such as interactivity and electronic programme guides.

Exhibit 9: *U.S. online video streams (billions)*



Source: eMarketer

In addition, commercial platforms are emerging that take advantage of the higher capacity of broadband networks to deliver multimedia services over the Internet—for example, the BBC iPlayer provides TV shows and radio over the Internet in the UK.

More than half of U.S. Internet users (57 percent) have used the Internet to watch videos online, and almost 20 percent of consumers do this every day. And these percentages are even higher for users with broadband connections (74 percent of them watch videos online). Last year, some agile startups have begun to turn the Internet into a real TV: Joost, Babelgum, and others are deploying high-quality TV offerings enriched by Web 2.0 elements in a so-called over-the-top (OTT) approach, that is, "on top" of a cable or telecom operator network without any liaison with the network provider.

These trends are not only making the Internet a more important medium for advertising; they are also establishing it as a more important shaper of public opinion. Advocates for freedom of opinion and a well-informed public (i.e., regarding politics, social sciences, and cultural institutions) will exhibit increasing interest in such media consumption changes.

SOCIAL NETWORKING

Society is experiencing greater levels of interaction through social networking sites such as Facebook and Bebo, which, on the one hand, have brought functionalities impossible without the Internet and allow individuals to live their friendships online with physical distance not

mattering at all, but which, on the other hand, also raise some fears around what happens to traditional societal behaviour such as face-to-face interaction and friendship.

Social networking is a relatively recent phenomenon that is supporting the general Web 2.0 trend towards online social communities. Users—particularly those from the "born digital" generation—are part of social interest groups operating in an online context that are generating, posting, and sharing content online. Social networking is used by an increasing portion of the Internet users, with most accessing multiple sites on a regular basis.

The Internet has for quite some time influenced the social behaviour of consumers. In a 2004 Social Ties survey in the United States, the average Internet user had a larger group of people he interacted with regularly (37 ties for Internet users compared to 30 for non-Internet users). More than 30 percent of Internet users furthermore stated that the Internet increased their number of ties and casual acquaintances.

Social behaviour is changing—people connect faster and with larger social groups when using the Internet

CHANGES IN SOCIETY

As laid out above and discussed in more detail throughout the report, digital technology is already a major economic force—and will be even more so in the future. But it should not be restricted to a purely economic factor. The Internet in particular and digital services more broadly will be major change drivers with far-reaching impact beyond the sales of books or airline tickets. Digital technologies enable everyone to make his or her voice heard and connect to large audiences in any context relevant to the individual.

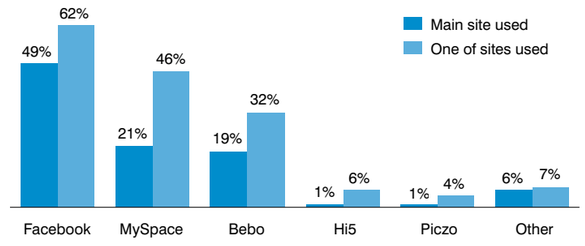
The Internet is an increasingly important opinion shaper—Google is frequently cited as one of the most reliable global news sources, right after CNN and the BBC.

Politicians use the Internet for presenting themselves and their ideas, for interacting with their supporters, and for organising their campaigns. For example, Presidential candidate Barack Obama in the United States is extensively using social networking applications in his presidential campaign. On Twitter, more than 30,000 users are his "followers," regularly getting short updates from him. Nearly a quarter of Americans today use the Internet regularly as a source for political/campaign information; in the 18-to-29 age group, the share is more than 40 percent. Obama has taken the use of the Internet as a political tool to new levels: He is using it also to collect funds for his campaign. More than 1 million individuals contributed an average of $105—an unknown possibility 10 years ago, but now one of the major sources for funding.

Society has been reshaped by the Internet—for exam-ple, 60 percent of U.S. consumers could give up their phone, but only 55 percent Internet

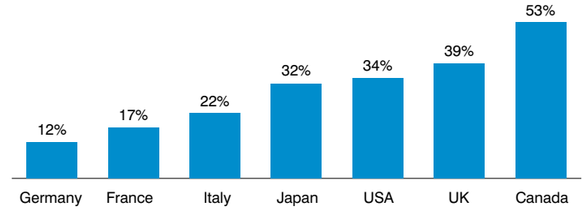
Blogs, podcasts, chat sites, user forums, newsgroups, and other advanced communication and online publishing tools have not only changed completely the communication needed in organisations to fulfil business purposes and other communication requirements; by having made communication so much easier, it also has significantly increased the speed and volume of sharing rumours and news. One of the consequences is that organisations have been confronted with a dramatically increased need to design and deploy information and communication policies, especially with respect to confidential business information. Opinion portals like ciao, which operates in several European countries and registers visits from more than 38 million consumers each month, and blogs have created

Exhibit 10: *Social networks used by adults (UK, 2007)*



Source: Ofcom

Exhibit 11: *Social networks used by adults (2007; percentage of Internet users per country)*



Source: Ofcom, Nielsen n=391

Generation "Born Digital"—Bringing Digital Confidence to the Fore

Children and youths in industrialized countries are the first generation that was born into a digital world. They are the early adopters of new technology and IT specialists compared to most parents. And up to now, only parts of the older generation are being "reborn" into this digital life.

Wired magazine writes on "born digital":

- A self-characterization: "We learned to crawl alongside the PC. We came of age with the Internet. Early-adopting, hyperconnected, always on."

- On technology: "From IM to MP3 to P2P, we lab-test tomorrow's culture. While others marvel at the digital future, we take it for granted. Think of it as the difference between a second language and a first."

The generation "born digital" does not distinguish between on- and offline as much as many adults tend to do—both "worlds" are a lot more interconnected for them; they live in real as well as virtual communities with often significant overlap in their age groups; and they have their own "online" culture, language, and netiquette.

But the generation "born digital" also poses some challenges, for itself as well as for the rest of society:

- Quite a paradox—They broadly expose information about themselves on social networking sites, thereby giving in on privacy, but they react strongly if they dislike the way their data is used—as in the Facebook Beacon case, in which more than 50,000 users signed a petition in December 2007 complaining about a programme intended to integrate Facebook with external partner websites for cross-referencing and targeted advertising purposes.

- Parents and schools (the "natural educators") are overburdened by the breadth of new phenomena and the speed of innovation.

- Traditional legal standards and values are more difficult to apply to "ambiguous" digital activities and find less acceptance, for example, around sharing of copyrighted content.

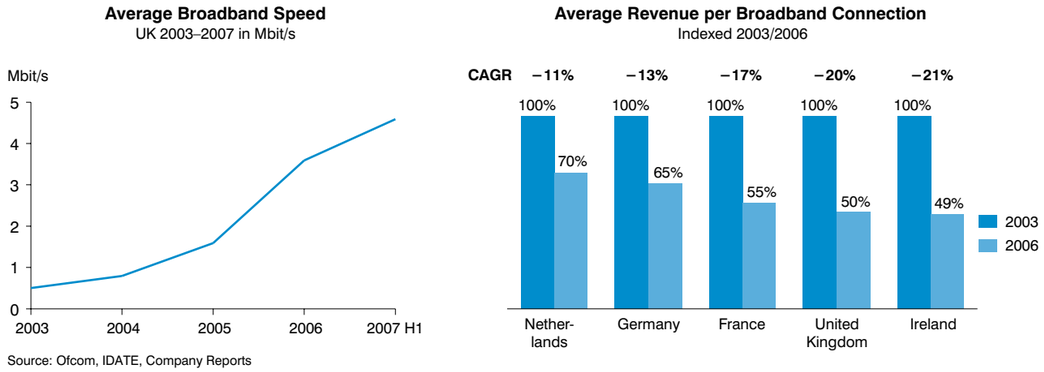
Overall, "born digitals" are not given enough guidance on appropriate behaviour in digital environments—which has put pressure on business models for many years already, in the case of sharing copyrighted content, and will continue to do so as the industry seeks to implement new advertising business models.

a genuinely new source of pre-purchase information that can both go clearly in favour or strongly against individual marketers, services providers, retailers, etc. The power of blogs and online "syndication" reaches far beyond pure e-Commerce and the digital world itself: Kate Hanni, an individual airline passenger severely dissatisfied by American Airlines' practices, founded The Coalition for an Airline Passengers' Bill of Rights with some companions in misfortune after having been "stranded on several American Airlines planes for up to 9 hours at Austin International Airport" in December 2006, without "food, water or access to working bathroom facilities." The coalition now has more than 20,000 members, utilises a website and a blog to exchange "horror stories" and to make its voice heard— and has visited members of the U.S. Congress repeatedly, with legislation and regulation changes now under discussion to avoid the horror stories its members have experienced.

The power of Web 2.0 offerings such as opinion portals and features such as user reviews on Amazon finds confirmation in Edelman's Trust Barometer: The 2008 edition shows that in many countries, including the United States, the Netherlands, and Germany, "a person like me" is considered the most credible source of information about a company, rating much higher than any official source of information including the CEO. Across all countries, four out of five respondents said that they "are much more likely to believe what you see, read, or hear about a company if someone you know has already mentioned it to you." On the institutional side, NGOs are rated as most trustworthy, compared to business, media, and government—in the UK, Germany, and France, NGOs lead the rankings by substantial margins.

The pace with which change is taking place in the digital world is breathtaking for many of us. At the same time, there is a new generation "born digital" for whom the possibilities of the digital world are as common and un-spectacular as those of radio were to most people 50 years ago: They are the early adopters of new technology and IT specialists compared to most parents; they do not distinguish between on- and offline as much as many adults tend to do, but rather live in real as well as virtual communities with often significant overlap in their age groups; and they have their own online culture, language, and netiquette. However, the generation "born digital" also poses significant challenges because it lacks guidance around what constitutes appropriate behaviour—with

Exhibit 12: *Broadband connectivity dilemma*



Source: Ofcom, IDATE, Company Reports

respect to sharing personal data or to sharing of copyrighted content. This not only is a burden for itself and therefore an educational task for society—it is also a tangible problem for digital business models, for example, in the fields of digital content or innovative advertising. Industry is well advised to come to a collaborative view on how to deal with the "born digital" generation and identify new ways of working together.

CONCLUSION

The identified growth drivers for digital life are stimulating fundamental change across all elements of business and society. What is certain is that digital life will continue to drive economic growth and prosperity and become a more central part of everyday life. The digital infrastructure is creating new ways of interacting, communicating, and doing business that are still in the early stages of being exploited.

3. REVENUE AND GROWTH DRIVERS: CONTENT AND ADVERTISING, NOT ACCESS

The growth areas identified drive increased revenue for the digital economy across four revenue categories:

The next wave of growth in the digital economy will be fuelled by increasing usage rather than by the number of users.

1. Advertising. All forms of online advertising, including click-through revenue[1], IPTV advertisements, and sponsorships (e.g., an online TV show with a sponsor that announces "This show is brought to you by xyz").

2. Content. Digital content delivered online, including video on demand, gaming, TV (paid Web TV and streaming video), and music downloads.

3. e-Commerce. Products and services ordered over the Internet and delivered via traditional means (e.g., ordering books from Amazon or an airline ticket from an airline's website).

4. Access. Transportation of traffic to the Internet and access to digital TV offers, specifically the revenue received by network operators (Cable and DSL) for providing Internet access.

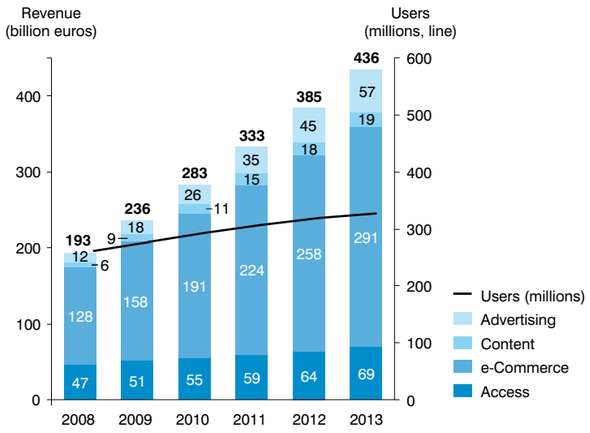
e-Commerce is the most established and largest revenue category. Online advertising and content are relatively new revenue categories, growing at 32 percent and 22 percent, respectively, although from a low base (Exhibit 13).

To date, the digital economy has been driven to a large extent by technological advancement; the migration from narrowband to broadband networks created an explosion in Internet penetration and usage. Broadband access has now become a mass market phenomenon in many European, Asian, and North American countries and is nearing saturation levels in certain countries, especially in Western Europe, with some countries in Southern and Eastern Europe lagging behind. Therefore, access revenues in these countries are expected to remain stable over time, with single-digit growth. At the same time, transport infrastructure is becoming increasingly commoditised, which is the result of a highly competitive

The total market for digital life will grow by 18 percent per year, reaching a volume of €436 billion by 2012.

(1)Click-through revenue refers to volume-based payment to a search engine for a sponsored link to directed traffic to a website

Exhibit 13: *Digital life—revenue summary Europe*

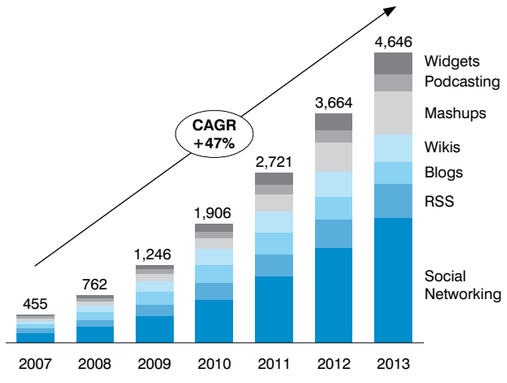


Note: Europe including EU-27, Norway and Switzerland
Source: Forrester e-Commerce Forecast, Company Report Apple, Company Report Google, EU TV and Broadband Forecast Model, Booz & Company Analysis

market with established technical solutions and limited opportunity for differentiation. Slowing growth in subscriber numbers and modest growth in access revenue combined with the increasing traffic demands of more bandwidth-hungry applications (e.g., video on demand, P2P) are placing pressure on access margins. The overall value share associated with access will drop from 24 percent today to less than 16 percent by 2012.

There will be a significant shift in value pools away from infrastructure: The share of access business for digital life will drop significantly in the next 5 years—from 24 percent today to less than 16 percent in 2012.

Exhibit 14: Worldwide annual sales Enterprise 2.0 (millions U.S. dollars)



Source: Forrester

As revenues are predicted to grow more rapidly than Internet users (18-percent compound annual growth for revenues compared to 4-percent for users) over the coming years, there is evidence of a fundamental shift in value distribution across the value chain. Future growth will come from increasing revenues through stimulating spend per user, rather than increasing the number of users. This growth is expected to be achieved through more innovative products and services complemented by new business models generating incremental revenue streams.

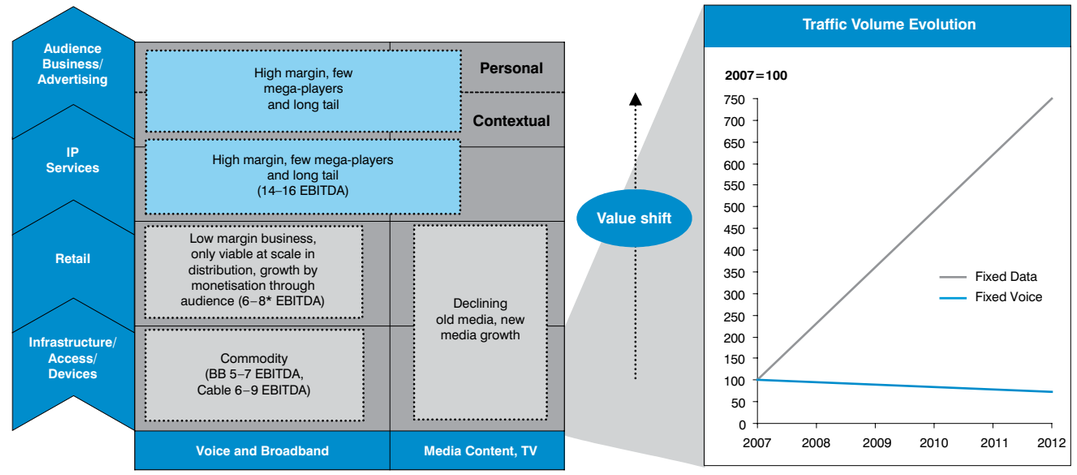
Network operators, as the enabler of digital life, need to support greater levels of traffic at diminishing return.

These new services will apply to both consumers and business environments. For example, Forrester estimates that Web 2.0-related B2B sales will grow by 47 percent per year, resulting in almost $5 billion in growth worldwide by 2013.

As a result, the next wave of growth in the digital economy will be driven by services and applications that can be realised only in step with broadband penetration per country. Consequently, in those countries with a significant digital divide, rollout of broadband infrastructure continues to be the key basis for growing the digital economy. In countries where broadband is more advanced on its maturity curve, network operators will need to continue to push next generation network (NGN) conversion in order to prepare for the traffic flows expected from further increasing usage generally and broad introduction of high-quality TV and video specifically.

Network operators need to adopt new business models, generating value through services and applications rather than infrastructure rollout—they also need to invest in NGNs in order to capture growth and be able to offer value-added services.

Exhibit 15: *Transport perspective: Fixed-line telecoms landscape*



Note: Europe 27+2 (CH, NO), i.e. including lesser developed broadband markets; conservative estimate for developed markets
Source: Ovum, Booz & Company Analysis

III. DIGITAL CONFIDENCE: SECURING THE FUTURE GROWTH OF DIGITAL LIFE

1. THREATS TO DIGITAL LIFE

The growth of digital life can be sustained through the continued growth in online usage and spending. To achieve this, consumers and enterprises need to have confidence in the environment in which they operate. Consumers will need to be educated as to what the potential threats of the Internet are and how to deal with them—and will need to feel safe and indeed be safe. One of the main challenges for industry will be to provide a secure network environment and optimal customer experience.

With the success of digital life have come concerns for consumers and enterprises relating to the security and integrity of the digital environment.

The proliferation of user-friendly technologies and ubiquitous connectivity have contributed to the Internet's position as the main platform of digital life. Cross-platform strategies and "webification" of other platforms will also bring other platforms, like digital television and mobile platforms increasingly into the frame.

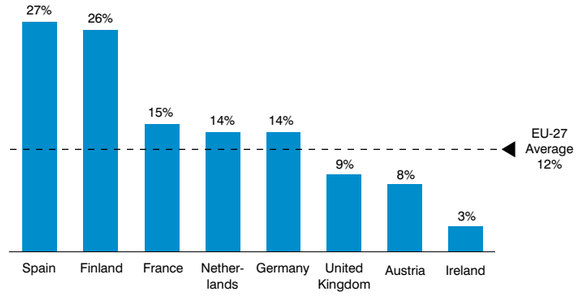
With the growth of Web 2.0 economy there is also cause for concern, related, first, to the behavioural patterns of consumers themselves, for example the increased flow of personal information over the Internet through profiling activities over social networking sites. The general pressure on service and platform providers to monetise Web 2.0 applications (particularly in the case of social networking sites) and next-generation network investments increases commercial pressure on consumers, for example, by new advertising-driven business models and other forms of targeted marketing making use of users' online profiles. But also in the professional space, users' online profiles, blogs, and photo albums can have consequences when future employers scan their candidates.

Other concerns relate to malicious network security breaches threatening the protection of personal data online or threatening business continuity and undermining growth in services relying on secure network environments (Exhibit 17). These concerns are in many cases justified; for example, an analysis of the top 10 Internet scams in the United States during 2007 shows that the majority of cases were related to e-Commerce activities and resulted in real and tangible financial losses of up to $4,000 per person (as shown in Exhibit 18 for the top Internet scams). Twelve percent of Europeans avoid e-shopping specifically because of concerns over Internet security (Exhibit 16). In addition to fraudulent activities, businesses face the growing threat of attack from malicious users. Data suggests that in 2005 such attacks were costing the industry in excess of $1,000 billion per year worldwide in lost revenue and the cost incurred in idle time, cost to repair damage to systems, and any associated loss of reputation. These costs were growing extremely fast between 2000 and 2005 due to the rapid growth of digital life (Exhibit 19). Even today, industry experts are not able to assess the full damage.

One in eight consumers avoids e-shopping due to concerns over Internet security.

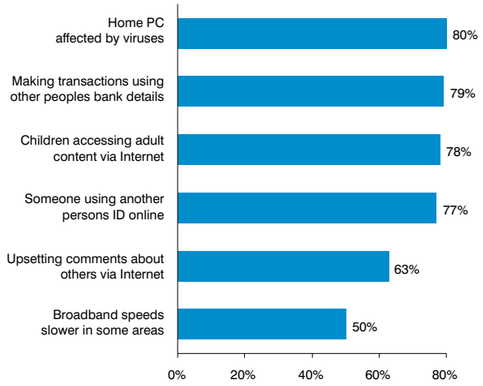
Web 2.0 is also a major disruptive force for the audiovis-ual content industry due to online piracy and a wide-spread perception among the "born digital" generation that all content should be free. The media industry is grappling with traditional legal standards finding less acceptance in the context of "ambiguous" digital activity, for example, sharing of copyrighted content, which puts pressure on media industries to find

Exhibit 16: *Percentage of consumers avoiding e-shopping due to security concerns (Europe, 2007)*



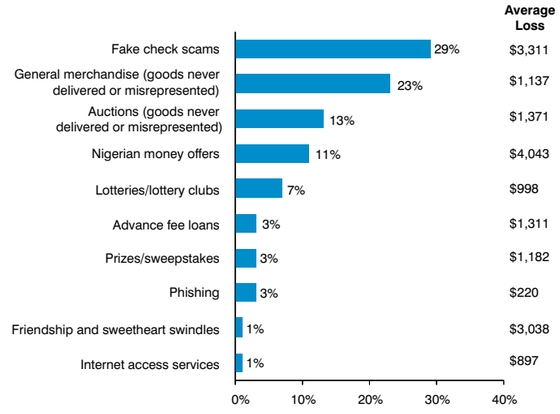
Source: Eurostat

Exhibit 17: *Prompted awareness of various Internet issues (UK survey, 2007)*



Source: Ofcom

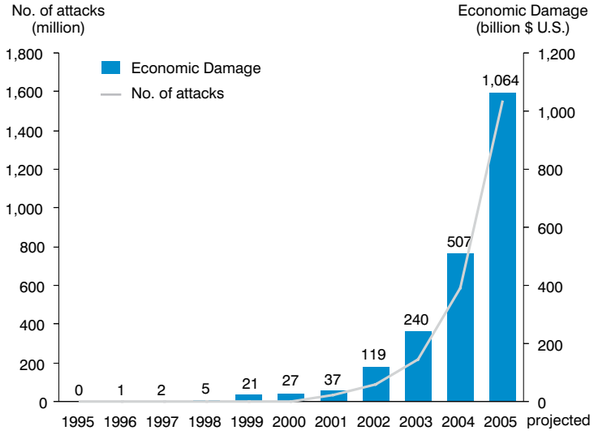
Exhibit 18: *Top 10 Internet scams (U.S., 2007)*



Source: NCL's Fraud Center

Note for Auctions: "In the fall of 2003, online giant eBay removed the link from its Web site to fraud.org. As a result, the number of auction complaints reported to NCL's fraud center has dropped to a fraction of its previous levels."

Exhibit 19: *The explosion in overt digital attacks (worldwide)*



Source: NCL's Fraud Center, Congressional Research Service, mi2g, Craig Fosnock, Eurobarometer e-Communications Household Survey 2007, Symantec, McAfee, Booz & Company Analysis

Overt attacks are those that become public knowledge including:
- Data attacks where confidentiality, authenticity or integrity of data is violated, or
- Control attacks where network control or admin systems are compromised

ways to effectively enforce legal protection in the online environment and to educate the "born digital" generation. Being "born digital" is not an excuse for illegal behaviour, but it can explain it, as such users have become accustomed to the "for-free" Internet model and expect to be able to download digital content without the need for subscriptions or payments.

The Internet has spawned an entire underground economy that provides a marketplace for illegal digital activities. For example, it is possible to purchase digital "products" such as e-mail passwords and addresses as well as services such as spam mail and "bots" with custom functions capable of wreaking havoc on targeted companies. Businesses recognise and are starting to respond to such threats. Microsoft employs about 65 investigators and lawyers working full-time on tracking cybercrime (January 2008).

To sustain the growth of digital life, consumers need to be educated about the threats and provided knowledge and the tools to deal with them.

Altogether, the risk now visible in the digital world is causing concern for consumers and business alike, which is threatening the continued growth of the Internet and the digital life that has been described.

2. DIGITAL CONFIDENCE: CONCEPT AND OVERVIEW

The level of confidence that both traditional and "born digital" consumers place in industry in terms of providing secure services and network environments and good business conduct, as well as in the ability of governments and regulatory authorities to protect consumers, is rapidly becoming a major factor affecting the potential growth of the new digital economy.

Digital Confidence is therefore becoming a key growth enabler—or an inhibitor—for the digital economy, as a measure of how much consumers and suppliers of digital services have confidence in digital applications in the broadest sense, that is, feel comfortable in engaging digitally.

Industry has become increasingly aware of how important it is to be proactive on Digital Confidence and have, to some extent, started to do so. However, it is a complex topic, involving many players often with diverging positions and interests, and with activities being undertaken in a fragmented, piecemeal manner triggered by well-reported confidence breaches.

Digital Confidence is a key growth enabler—or an inhibitor—for the digital economy and a measure of how much consumers and suppliers trust digital life.

For industry going forward, it is important to focus on the key factors on the basis of which consumers will judge businesses' performance in providing new digital and online services and platforms. These key factors are derived from an analysis of the focal points in current Web 2.0 policy and lawmaking processes, parliamentary debates, international (trade) agreements, blogging activity, and media attention. These factors relate to four areas:

- Network Integrity and Quality of Service.
- Privacy and Data Protection.
- Minors' Protection.
- Piracy and Theft Avoidance.

Industry needs to take steps proactively on the basis of a holistic view of all these issues, which, in this report, has been captured in the concept of Digital Confidence. Fostering Digital Confidence transcends corporate responsibility and compliance—it is fast becoming a commercial prerequisite and a license to operate. As certain case studies will show, compliance alone does not buy consumer acceptance.

The four pillars that support the concept of Digital Confidence (Exhibit 21) cover the major threats, issues, and attacks relevant today and experienced as such by consumers. The framework structures and identifies risks that need to be addressed and the objectives for Digital Confidence for each pillar:

- **Network Integrity and Quality of Service.** How to maintain network integrity when faced with malicious IT attacks? How to put in place network management practices that optimise the customer experience? Ensure a fair distribution

Exhibit 20: *The four pillars of Digital Confidence*

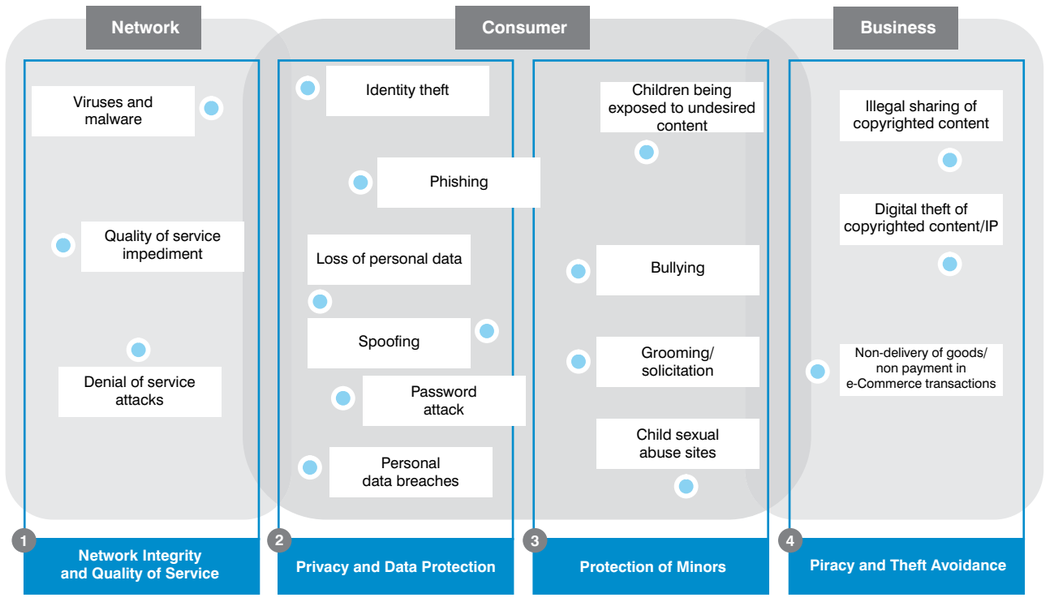
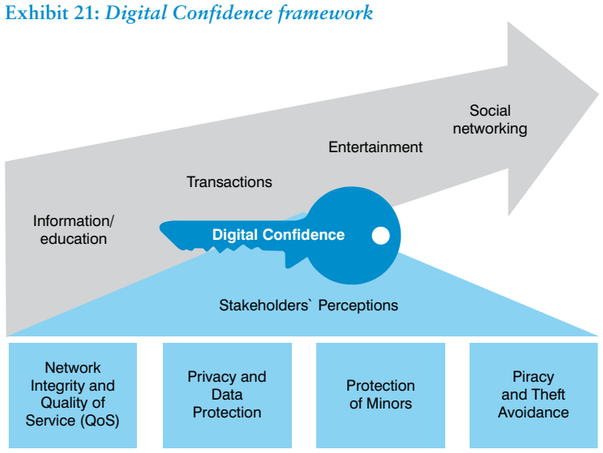


Exhibit 21: *Digital Confidence framework*



of network bandwidth in peak times, dealing with traffic growth, and protect against malware.

- **Privacy and Data Protection.** How to handle and protect consumer data and privacy online? Prevent identity theft, incidental loss of private data, and commercial data exploitation.

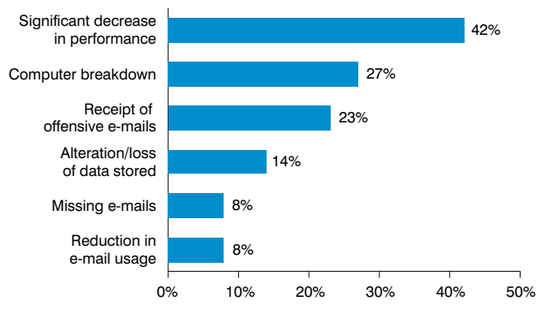
- **Minors' Protection.** How to ensure child safety online? Protect them from undesired content, bullying, and grooming and fight child sexual abuse content.

- **Piracy and Theft Avoidance.** How to manage copyright infringements? Counter theft of copyrighted content and protect e-Commerce transactions.

**Source: Pew Internet & American Life Project*

(2) In a Denial-of-Service (DoS) Attack, many machines send traffic to a single target machine, essentially overloading the target with data and using up all resources. As a conse-quence, the target system crashes or at least becomes un-usable

Exhibit 22: *Resulting problems from spam and viruses (UK, 2007)*



Source: Euro barometer e-Communications Household Survey 2007

Across these four pillars, a diverse set of stakeholders either influence or are affected by the level of Digital Confidence.

This report aims to highlight certain case studies on Digital Confidence best practices and distil what is required to accelerate proactive, industry-led initiatives being deployed. It aims to contribute to the thinking on appropriate and proportionate "levels of intervention" and forms of cooperation by industry and governments; fostering Digital Confidence in alignment with fundamental Internet freedoms as well as business requirements.

*Social networks facilitate cyberbullying—a 70-percent increase of bullying of minors occurred using social networks.**

3. NETWORK INTEGRITY AND QUALITY OF SERVICE

Network Integrity and Quality of Service focuses on protecting the enabling technology platforms for digital life. It has two main objectives:

1. Ensure the network platform and computing environment for consumers and businesses is secure and protected from external attack—counteract the disruption to consumers and businesses from malicious digital attacks, for example, viruses, malware such as spyware, and trojans that gather or destroy information, and flooding or spamming of websites causing denial of service.(2)

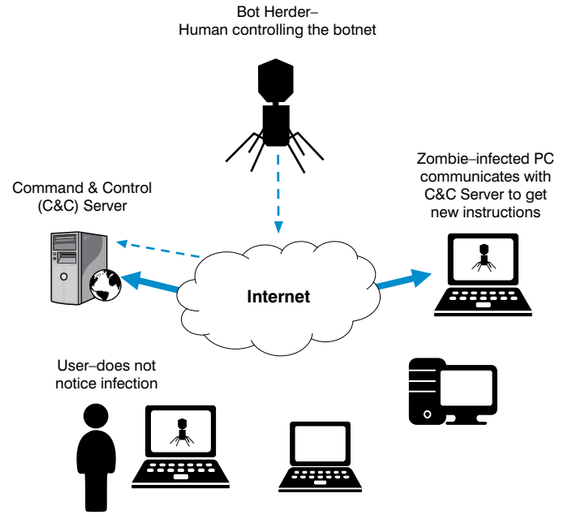
Spam makes consumers less trusting in e-mail, and 18 percent see it as big problem.

2. Ensure end users are delivered a consistent quality of service—ensure that the network is able to manage the increasing traffic volumes in a manner that ensures end-user service quality despite peaks in traffic load that strain network resources.

VIRUSES AND MALWARE

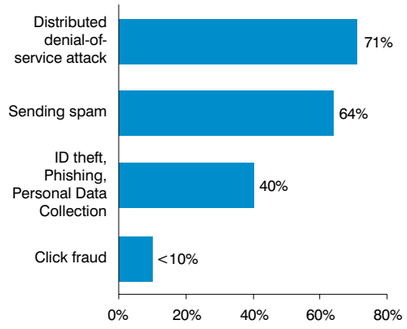
Viruses and malware are malicious attacks on end-user devices and local area networks resulting in various problems (Exhibit 22). The level of awareness regarding problems with spam and viruses varies significantly with the level of Internet usage. Those countries with high levels of Internet usage have a greater appreciation and understanding of the risks of such attacks as well as levels of security employed. For instance, the Nordics and Benelux have a high awareness of malicious digital attack: Over 35 percent believe

Exhibit 23: *Botnets—Bot Herder and his zombies*



Source: WatchGuard

Exhibit 24: *Use of botnets for attacks*



Source: Arbor

they have experienced problems with spam and viruses. Conversely, there is relatively low awareness of such risks in Southern Europe—less than 15 percent believe they have experienced problems. In the United States, 55 percent of Internet users say spam has made them less trusting in e-mail, and 18 percent see spam as a "big problem."

So-called "botnets" are responsible for 80 percent of worldwide spam.

The most common consequence of spam, viruses, and spyware is usually damage to hardware. The Consumers Union found that over a 6-month period spyware infections prompted nearly 1 million U.S. households to replace their computers.

As the level of consumer awareness with respect to this particular risk increases, it is apparent that consumers are more willing to take some responsibility for the prevention of viruses and spam affecting their hardware. Indeed, the global software security business is now worth $9.1 billion annually and growing at around 12 percent each year.

BOTS, ZOMBIES, AND BOTNETS

A bot is software used to automate specific tasks in a semi-intelligent way.(3) Bots can be used in a harmful way by an attacker (bot herder) to remotely control other computers known as zombie computers, as shown in Exhibit 23. The attacker can then perform almost any task he wants on the zombie computer.

Botnets are used for several purposes from spamming and denial-of-service (DoS) attacks to phishing and click fraud (click fraud is an attack against advertisement providers; the bot pretends to click on the ads several thousand times per hour) and identity theft (see Exhibit 24).

The combined bandwidth of several thousand PCs, most with broadband connections, can cause very significant DoS attacks and are responsible for an estimated 80 percent of worldwide spam.

A botnet describes all zombies under control by a single bot herder. Famous botnets include:

- **Kraken.** Almost 500,000 zombies, including infected PCs in 50 Fortune 500 companies, almost undetectable by anti-virus software.

- **Srizbi.** More than 300,000 zombies.

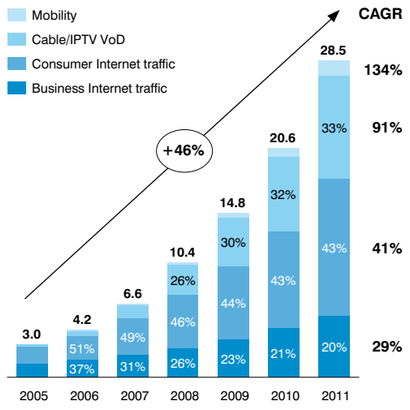
- **Storm.** Around 150,000 to 200,000 zombies.

- **Bobax.** Potentially a predecessor of Kraken or a separate botnet.

Not just consumers and business can be victims of bot-nets. Even countries may become targets, as the DoS attack through botnets against Estonia in 2007 shows. Targets of the DoS attacks

(3) Bots are a piece of software running on a local system and receiving tasks from a remote control server. The bot exe-cutes the task as autonomously as possible and then waits for new commands.

Exhibit 25: *IP traffic growth global (2005–2011 in ExaBytes per month)*



Source: Cisco

included the Estonian presidency parliament, almost all of the country's government ministries, political parties, three of the country's six big news organisations, two of the biggest banks, and firms specialising in communications.

Minors Education and Network Integrity

France, May 2008: Authorities arrest 22 people suspected of being hackers in an international hacker ring. Disturbing fact after the arrests: Sixteen out of the 22 suspects are under 18 years old.

Security experts from Sophos applaud the authorities for the success, but they ask: "What is going wrong with our education of young people to make them think that computer hacking might be an acceptable way to behave? "More has to be done to teach children in school how to use their computer skills responsibly."

QUALITY OF SERVICE

To the extent that quality of service issues reside in the network (quality of service depends on the end-to-end path across the Internet, not just the access network), they result from two main drivers: The growing volume of Internet traffic generally and the peaks in traffic due to heavy users using bandwidth hungry applications simultaneously.

The volume of Internet traffic has been growing particularly fast in recent years—and this growth is also expected to continue in the future (Exhibit 25). Therefore, measures are required to address the anticipated increase in traffic resulting from applications such as video on demand, HDTV, file sharing, user-generated video, rich content, P2P, and online gaming, which are expected to drive the next wave of growth in digital life. QoS in this report only relates to IP service—cable operators ensure QoS in video services based on DVB-C by using a dedicated spectrum, which does not impact Internet broadband speeds. This is different in an IP environment where (multiple) IPTV streams put a strain on broadband capacity.

Heavy users place a strain on quality of service for all users.

The second point of concern is related to the "heavy user." Broadband networks—in common with all networks—are engineered to meet the expected peak-load requirements experienced during the busiest period of network use. Heavy users cause peak traffic volume to exceed the engineered maximum load. Without active network management, end users would experience degradation in the quality of the service they receive although the level of degradation may vary depending on the application (e.g., Web banking versus mp3 downloads). In broadband networks, where capacity is a shared resource, this effect would reduce connection speed or, in extreme cases, interrupt service.

To counteract the effects of traffic levels exceeding the capacity of the network, operators may add additional capacity (building new infrastructure and upgrading existing one) incurring capital expenditure and fixed cost, or applying active traffic management techniques to save bandwidth for particular types of traffic for all users.

From a pure capacity standpoint, adding the additional capacity seems a straightforward option, but this also has a significant economic impact. Due to the fast growth in traffic, network providers would have to add more and more capacity, meaning the upgrade costs of networks are also increasing. Based on the network provider business model, these costs have to be borne by the consumers using the network—leading to increases in end user prices. Furthermore, increasing capacity alone will not solve the challenge of network congestion or service degradation at peak usage times. Depending on the type of Internet application, network dimensioning, or speed of the source equipment, peak traffic may always use the maximum bandwidth available, independently of all capacity upgrades a network provider can perform.

To mitigate congestion incurred by heavy use of bandwidth-hungry applications, network operators deploy active traffic management techniques. Apart from technical traffic management solutions, usage-based pricing models are considered. Pricing-based models encourage users to avoid busy hours for their Internet use.

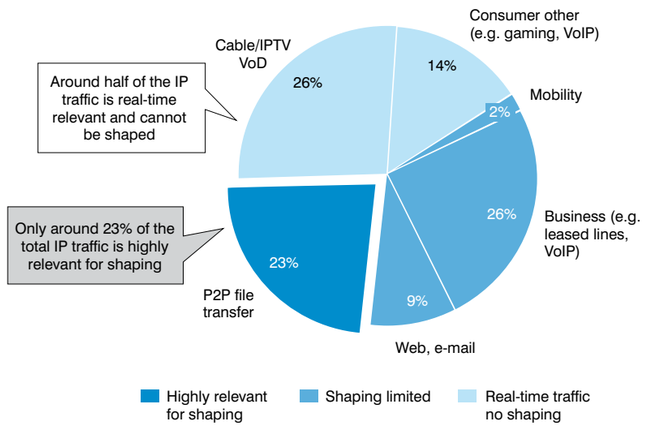
Technical active traffic management is often referred to as bandwidth management or traffic shaping. These technical measures detect lower-priority, non-real-time traffic and give it a lower priority on the network. As a result of bandwidth management, non–real-time data downloads, for example, downloading music from iTunes, would take a little longer—however, time-sensitive applications, for example, streaming music or VoIP telephony, would not be affected.

Traffic management can nevertheless be only part of the solution for ensuring optimal traffic flow over broadband networks. Shaping-based traffic management without significant end-user impact can be applied only to non–real-time traffic, which constitutes around only one quarter to one half of actual IP traffic, as seen in Exhibit 26.

Industry has for some time recognised that a small proportion of the users account for a disproportionate share of traffic carried over the network. For many network providers, approximately 80 percent of bandwidth is consumed by less than 10 percent of users. Not only does this represent a disparity in fair usage, it further exacerbates the bandwidth issue during busy periods. This heavy usage is often associated with peer-to-peer and video applications, and network operators are therefore most concerned by the congestion due to these two very popular applications. An example of a sudden increase of bandwidth due to streaming video was the introduction of the BBC iPlayer.

The situation in the UK with respect to the BBC iPlayer platform is typical of the dilemma the industry faces. The iPlayer is used to distribute and view radio and video content over the Internet. More than 42 million programmes were streamed or downloaded within the first 3 months of service following the official launch in December 2007. It has been causing hot debate in the UK among the platform operator, the BBC, several Internet access providers, and regulators as a result of the unprecedented level of use and traffic generated by the platform. Many ISPs concerned with bandwidth requirements have requested the BBC to partially fund required network upgrades. The BBC has rejected such claims as "inflammatory," warning ISPs that if content providers found certain operators "squeezing, shaping, or capping" their content, they would indicate on their sites which ISPs their content works best on—and which to avoid.

Exhibit 26: *Traffic-shaping applicability—distribution of global IP traffic 2008*



Source: Cisco

Ofcom estimated that supporting the additional 3GB/month of traffic generated per user by the iPlayer would cost UK network providers up to £831m over 5 years to upgrade the capacity of their networks. For the ISPs, the question is who will ultimately have to pay for the extra capacity needed—the platform provider or the consumer? Responding to these concerns, Ofcom has, in April 2008, stated its position, saying that "investment burden [is] to be shouldered by network operators and consumers, with prices likely to rise for faster connections" (Ofcom chief executive Ed Richards). Ofcom argues for "content-led tariff models" where ISPs and content providers jointly establish services guaranteed to run smoothly over the network, albeit at appropriate consumer price levels.

Less than 10 percent of users account for over 80 percent of network traffic.

Managing network traffic and capacity clearly has benefits for the majority of end users, ensuring that they continue to receive the quality of service they expect. However, as traffic continues to increase, driven by bandwidth-hungry applications such as video on demand, additional investments will need to be suppor-

Managing peak-load traffic is an effective way to secure the quality of service for the vast majority of the users.

BBC iPlayer Case Study

According to data provided by UK ISP Plusnet in February 2008, traffic spiked significantly since the launch of iPlayer:

- The per-user streaming of video went from 180MB in December to 292MB in January, a 62-percent increase.
- Streams outnumber downloads eight to one.
- The cost of streaming traffic tripled in the same time frame.

The above may point to a trend whereby users, when faced with the choice between a high-quality streaming option or downloading, will prefer to stream content rather than waiting for a full download. There would probably be a difference in the way music and video is used, as consumers may prefer to own the music via a download, whilst they are happy to consume video in a streaming fashion.

Should this indeed be a trend, then traffic management will be ever-less-effective because it cannot be applied to time-sensitive streams. The onus will therefore once more be on capacity build.

ted through higher prices, more tiered access products, or clearly differentiated approaches to managing traffic in busy periods. In essence, traffic management techniques attempt to balance the trade-offs between quality of service and capital expenditure due to network build out against rising end user prices to cover the cost.

Migration of current broadband networks to Next-Generation Networks with significantly higher capacities will partly address increased bandwidth demands associated with time-sensitive dependent services and applications. However, traffic management for non–real-time services will remain significant.

ACTIVE TRAFFIC MANAGEMENT OVERVIEW

Various technical mechanisms exist for network operators to actively manage traffic on their network and optimise the available bandwidth. All essentially involve saving the bandwidth consumed by specific traffic flows during peak traffic periods and by heavy usage. The methods are based on two components: (i) identifying the traffic to be shaped and (ii) reducing priority for this traffic and hence reducing the bandwidth used by the selected traffics.

TRAFFIC IDENTIFICATION AND SELECTION

Identifying traffic suitable for shaping can be achieved in many different ways, as seen in Exhibit 28. A simple way is based only on the source or target IP addresses and ports (e.g., to enforce fair use bandwidth limits). Identifying traffic on the basis of IP addresses and ports is not well targeted since it selects very large chunks of traffic that can affect multiple applications (i.e., if a port is used by several systems).

Alternatively, a more sophisticated approach to identifying traffic for shaping is deep packet inspection (DPI). Every IP packet is profiled, so that the underlying protocol can be read and a signature produced. This signature can be compared with a list of known signatures in order to classify the packet, for example, as a video on demand. Based on this identification, specific protocols or even services can be selected or deselected (in the case of real-time applications) for shaping. A crucial aspect of DPI is the need to maintain and frequently update the signature databases in response to the rapidly evolving Internet architecture.

The biggest disadvantage of DPI is cost: Because every single packet needs to be inspected, a lot of equipment is required. Systems usually use a hybrid approach, where traffic is prefiltered based on IP address and port, and DPI is applied only to selected packets.

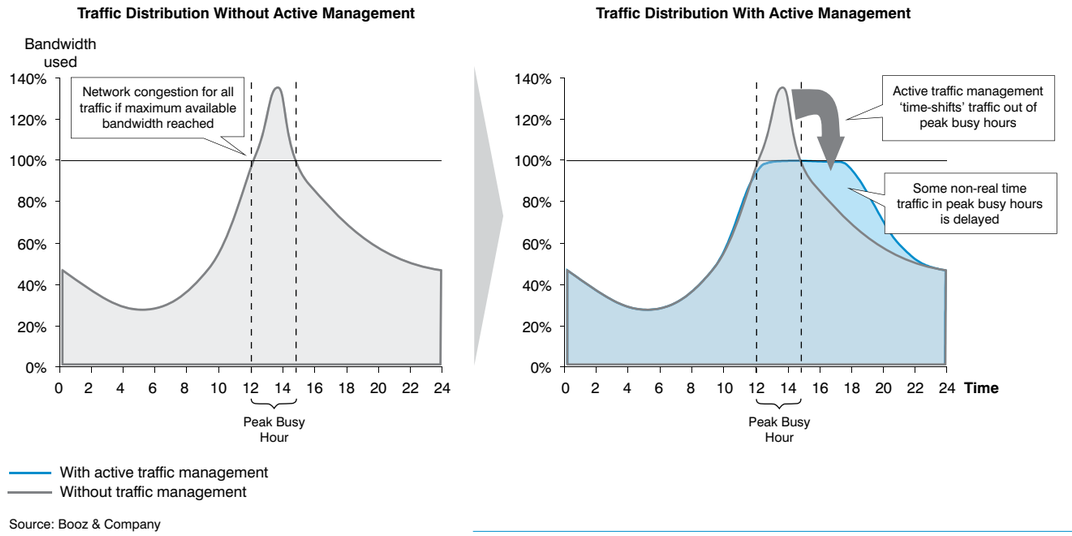
In summary, the selection of traffic can be user-specific (based on IP addresses), protocol-specific (based on port selection or DPI, for example, mail protocol), and/or service-specific (where a service is a certain server or application, for example, YouTube or BitTorrent).

TRAFFIC PRIORITISATION

Several methods exist to increase or reduce the priority and hence bandwidth absorbed by specific traffic flows. Some of these methods can be used in every IP network whereas others are specifically designed for certain networks. For example, packet cable multimedia (PCMM) is a QoS solution specifically created for cable networks.

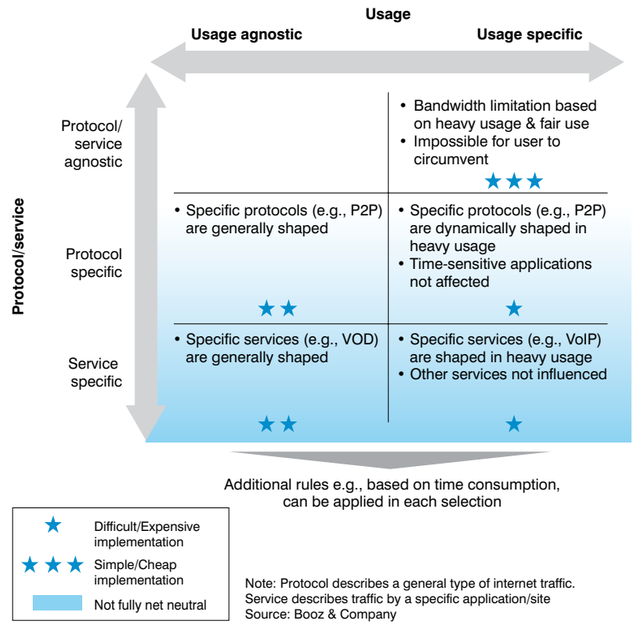
All techniques rely on slowing down the selected traffic and therefore reduce the data flow on the network. From an end-user point of view, applying traffic management on non–real-time traffic will only slow down long-running downloads without impacting e-mail or browsing.

Exhibit 27: *Traffic management overview*



Source: Booz & Company

Exhibit 28: *Traffic shaping toolbox—traffic selection*



Note: Protocol describes a general type of internet traffic. Service describes traffic by a specific application/site
Source: Booz & Company

4. PRIVACY AND DATA PROTECTION

Privacy and Data Protection addresses the security concerns of individuals with respect to their digital data. It has four main objectives:

1. Protect consumers' private data from being published—inadvertently or deliberately by themselves (e.g., on social networking websites) or by operators' databases being hacked or via careless and unsafe data transfers.

2. Prevent consumers' private data from being used commercially, such as in support of new advertising-driven business models, without the individuals being made aware, for example, enterprises using information relating to marital status and family situation in support of targeted, personal online advertising.

*The average person has 36GB of data stored by institutions—equivalent to 80 hours of video or 1 million pages of text.**

3. Protect consumers' private data from being accessed illegally—by means such as spoofing and phishing, for example.

4. Prevent identity theft and fraud—where criminals obtain money or other benefits by replicating and using someone else's private digital data.

Privacy and Data Protection is essentially centred on two methods: First, inadvertent or deliberate publication and, second, data obtained illegally through methods such as phishing.

Second Life—The Danger of Ending Up in the Wrong Place

In 2008, a mother in Germany reported that her 13-year-old daughter started to engage in Second Life—a virtual platform that allows users to take a "virtual identity" and "life" in a virtual world.

The daughter asked her mother for money to buy Linden dollars, the currency used in Second Life. The mother refused to finance these activities.

Months later, she found out that her daughter acted first as a virtual stripper, then as a virtual prostitute in a sexually explicit "club" in Second Life in order to earn Linden dollars.

*Source: IDC

DATA PUBLICATION

There is a proliferation of social networking websites on the Internet, from those for general-interest groups (e.g., Facebook) to those focusing more on professional networks (e.g., LinkedIn). These websites request, store, and publish increasing amounts of information about users, including residence, age, interests, and photographs. Most websites offer the facility to limit the users that can view detailed profile information—however, almost half of the users make profiles available to everyone. Also, many other websites require users to register to use them (e.g., Web mail providers) or to access all features and content (e.g., many forum systems)—these sites also collect user and behaviour data.

Missouri, United States, May 2008: Cyber Bullying May Become Illegal After Suicide

After the suicide of a 13-year-old girl being cyber-bullied by neighbours, legislation is being proposed to make cyber bullying illegal. Harassment and intimidation would be punished by up to 2 years in prison.

Reactions focus on the difficulty in deciding what constitutes "harassment" as compared with "normal" interaction or joking between friends. Furthermore, the methods of enforcing the law are seen as critical.

Making such information publicly available has implications for personal safety, security, and personal reputation—for example, the threat of identity theft or when businesses are using personal information on social websites for checking the validity of information in job applications as well identifying suitable job candidates based on searches of professional communities. Furthermore, information once spread into the digital world on the Internet cannot be retracted, since it is so easy to copy, distribute, and save data.

Internet users are becoming more aware of their digital footprint—47 percent search for information about themselves online. But 60 percent are not worried about how much information can be found online.

Beyond consumers themselves, businesses are also a source of data privacy risk. Information stored digitally is by its very nature more convenient to manage, handle, and share for organisations. At the same time, it is more at risk of being inadvertently made publicly available, as a recent case in the UK illustrates. The UK's Revenue and Customs government department had to apologise to customers of investment bank UBS Laing and Cruickshank after losing sensitive account information. The department lost a computer disk, sent by the bank, that contained address and account details of UBS's Personal Equity Plan investors. This event was attributed to the error of an individual—however, it shows how real and significant the risk is.

*The U.S. CIA uses Facebook to recruit new employees.***

Businesses are also leveraging the detailed customer information they have in support of legitimate business transactions, for example, so-called "super servers" such as Meredith, a U.S. media company, that sells excerpts from its databases holding information on 85 million U.S. citizens, including details on 6 of 10 women and 8 of 10 households. Meredith has incorporated digital advertising agencies into its operation to monetise the value of the information it holds through targeted advertising.

PHISHING

Phishing is the most common method for illicitly obtaining individuals' private data. It involves masquerading as a trustworthy entity to obtain sensitive information such as use names, passwords, and credit card details. The targets of phishing attacks are end users, with the majority (over 65 percent) of phishing attacks assuming the appearance of e-Commerce sites such as eBay and Paypal.

Phishing attacks are the most common method for obtaining private data—and 65 percent of them are targeted at major e-Commerce sites.

Phishing has become a major source of concern for the industry, with each successful attack resulting in a $220 loss per individual consumer on average. The problem is becoming more widespread—with 30,000 new phishing sites being identified each month during 2007.

Tackling privacy and data protection concerns is increasingly difficult because of the diverse range of organisations that hold individuals' information in digital form—from business (retail, banks) to government organisations and social networking sites.

Furthermore, the definition of what constitutes private data is a dynamic issue that needs rethinking in view of technological progress (for example, the question whether an IP address should be considered personal data or not is vividly disputed). Another key point is determining how consent should be granted to allow data to be shared. Two alternative models are often discussed—"opt-in" versus "opt-out"—the former requiring consumers to actively consent to their data being shared. The alternative "opt-out" model is less popular with consumers as they are allowing data to be shared by default unless they remove this consent, and it is not always clear that they need to or indeed how they can choose to opt out. Increased transparency about the intended use of personal data will alleviate many concerns relating to the opt-in versus opt-out discussion.

With illegal forms of data-gathering, such as phishing, it is more clear-cut in determining that a crime has been committed. However, the international nature of this crime makes it difficult

**Source: Wired, 2007

Phishing—Explanation and Main Techniques Used

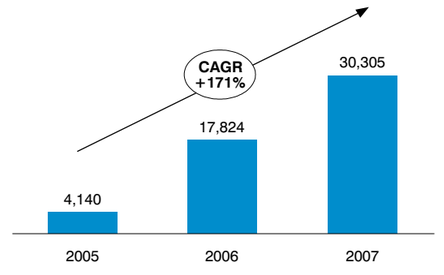
Phishing is mainly initiated via faked e-mails. Prevention with spam filters in mail clients is often quite effective but not always perfect.

Former phishing e-mails were poorly implemented, with unconvincing design and wording (spelling mistakes), but have now improved dramatically—even experienced users have difficulties seeing the difference.

Phishing is based on two main techniques:

- **Link Manipulation.** For example, "g00gle.com."
- **Website Forgery.** Phishing sites look like the original site, sometimes including the address (using some flaws in browser security).

Exhibit 29: *Average number of new phishing sites (worldwide, per month)*



Source: Phishtank, APWG, NLC Fraud Center

Privacy and Piracy

United States, May 2008: Walter Reed Army Hospital has exposed the personal information of more than 1,000 patients in a security breach. The data was contained in a single file, which was unintentionally shared on a peer-to-peer (P2P) system.

Several other data breaches have already happened due to file sharing on P2P systems, for example, at ABN Amro and Pfizer. Although policies in most companies and organisations forbid the use of P2P systems, some users are not aware of the danger of doing so.

to police and prosecute. Most phishing attacks are launched from criminals not located in the same country as the victims, and the equipment being used for the attack is often located in a third country without sophisticated cyber-laws. This makes it nearly impossible for police to enforce local laws.

5. MINORS' PROTECTION

Minors' protection seeks to defend the well-being of minors in the online world. It has four main objectives:

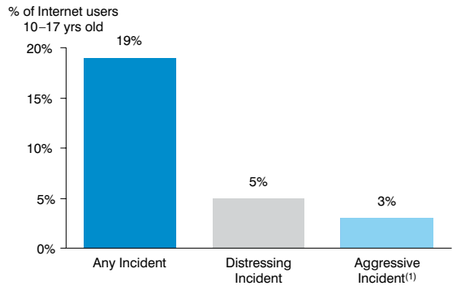
1. Protect children from being exposed to undesired content—this ranges from sexually explicit to violent to seductive content that parents and society may want to protect children from accessing and viewing (e.g., pornography).

2. Prevent bullying—defined as deliberately hostile behaviour targeted towards a minor by peers or groups of peers in the digital environment (e.g., happy slapping, posting of demeaning personal photographs).

3. Prevent grooming and solicitation—where adults use digital environments (e.g., chat rooms, social networking sites) to seek out children and build up trusted virtual relationships to then seek personal contact with malicious intent.

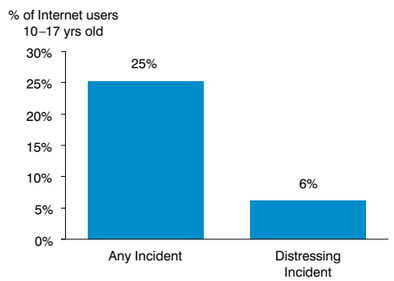
4. Counter child sexual abuse content—which involves the sexual abuse of children in the production of pornographic material (i.e., pictures, videos). Three main action areas are involved: (1) prosecute child sexual abuse content users, (2) prosecute child sexual abuse content suppliers and remove material, (3) prevent Internet users from being exposed to child sexual abuse content accidentally.

Exhibit 30: *Online solicitation (U.S., 2006)*



(1) Note: Aggressive used to describe solicitations including an attempt to contact the child in addition to online–by telephone/post
Source: Crimes Against Children Research Centre

Exhibit 31: *Unwanted exposure to adult material (U.S., 2006)*



Source: Crimes Against Children Research Centre

Addressing Digital Confidence with respect to minors' protection is crucial as it is arguably the most emotive area of Digital Confidence. It is also a very real threat with almost 20 percent of youths being subject to online solicitation and 25 percent having been exposed to indecent material (Exhibits 31 and 32). With respect to child sexual abuse content, The Sydney Morning Herald in June 2008 reported devastating numbers in conjunction with a major wave of arrests of child sexual abuse content users: 99 pictures that a hacker had inserted in "a respectable European website" received "an incredible 12 million hits in just 76 hours after word got around online paedophile networks that the images were available and the website's address was circulated."

Minors' Protection is a real issue, with 20 percent of youths in the UK having been subject to online solicitation and 25 percent having been exposed to indecent material.

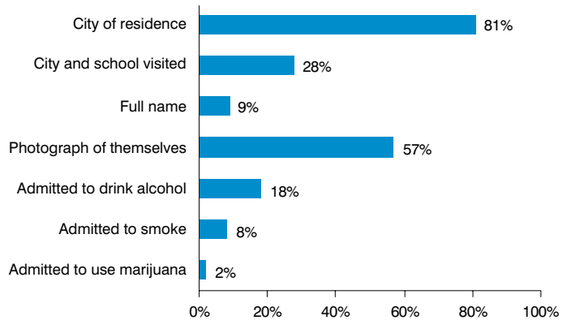
However, there is a range of challenges that the industry faces. Many parents are distant from digital life and lack awareness of the breadth of undesired content and the level of sophistication of other online malpractices like grooming and bullying. As a result, they are not taking the necessary steps to monitor and protect their children in their online activities. This is particularly relevant in the context of social networking sites used by predatory adults.

Herein lies a further issue in tackling this threat: Many of the risks are closely coupled with the rich functionalities of social networking sites, the anonymity of digital environments, and the ability to create a false identity. In essence, many of the enablers that are enriching digital life also create the opportunity for undesirable activities and by nature threaten the sustainability of digital life.

*Thirty-two percent of U.S. teenagers experience private data being forwarded without their consent.**

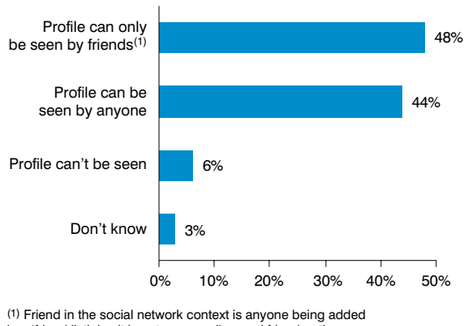
In addressing this area of concern, it needs to be first defined and identified. Everyone would agree that child sexual abuse content is unacceptable and is an activity that all stakeholders should try to prevent. Beyond this area however, there will still be much debate and divergent opinions around what constitutes acceptable content for minors and what forms of content can be criminalised set against concerns over freedom of expression and civil liberties.

Exhibit 32: *Content of profiles for young users of social networks (UK, 2007)*



Source: Ofcom

Exhibit 33: *Visibility of profiles in social networks (UK, 2007)*



(1) Friend in the social network context is anyone being added in a 'friend list', i.e. it is not necessarily a real friend or the person supposed to be
Source: Ofcom

6. PIRACY AND THEFT AVOIDANCE

Piracy and Theft Avoidance seeks to provide a secure digital business environment for digital life. It has two main objectives:

1. Counter illegal sharing of copyrighted content—that is, sharing copyrighted content illegally through applications such as peer-to-peer networks.

2. Protect e-Commerce transactions—that is, ensure individuals adhere to the usual standards of service when undertaking online transactions, for example, failure to pay or failure to provide agreed goods or services.

For business and content providers, having access to safe distribution environments is a precondition for stimulating production and availability of digital and online content, which will also accelerate the transition to successful new, online, paid-for business models. Transactional e-Commerce services also need protection against consumer failure to pay or failure to provide agreed goods or services. Transactional e-Commerce providers needs certainty that customers and businesses adhere to the usual standards of the offline world when undertaking transactions online. For users, their main concern is that they are not exposed to risks of being criminalised for using legitimate protocols and applications available over their broadband Internet connection, for example, when using a P2P-based content distribution system.

File sharing is a real concern to content copyright owners—in Germany, peer-to-peer traffic accounts for 50 percent of overall network traffic.

PIRACY: PEER-TO-PEER FILE SHARING

With the increase in bandwidth available to consumers and the digitalisation of content, sharing this content has become incredibly easy. Starting with Napster, today dozens of file sharing systems are available, most of them using P2P technology to distribute the content. P2P traffic today is between 30 percent and more than 60 percent of total traffic (depending on region). When file sharing began, it was

*Source: Pew Internet & American Life Project

Piracy and Network Integrity

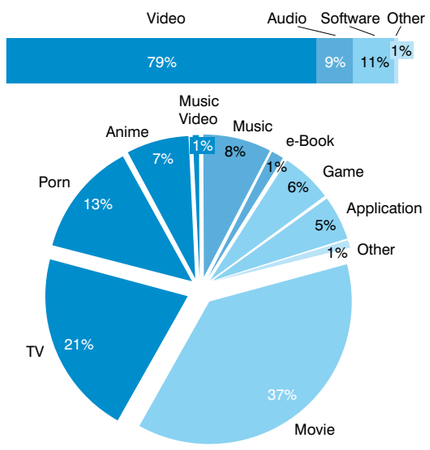
In early 2007, a remarkable and damaging virus was being distributed on the Winny network in Japan, the most popular P2P application in that country. The Trojan, which taunted file-sharers and threatened to report them to the police and even kill them, deleted a wide variety of file types and replaced them with popular comic book character images warning them not to use P2P.

It isn't illegal to write viruses in Japan, so the author of the Trojan horse, a Japanese student, was arrested for breaching copyright because in his malware he used cartoon graphics without permission.

generally music files being shared; but as broadband networks evolved, sharing videos became more viable, and today almost 80 percent of shared content is video (Exhibit 30). Because commercial offers of P2P content distribution were slower to emerge than anticipated, it is widely assumed that most shared content at present is in fact copyright-protected and is therefore being shared illicitly.

Due to the exponential growth of IP traffic, mainly driven by P2P solutions, piracy is the most prominent issue determining the success of new business models and the level of development of online and digital legal content offers going forward. With emerging broadband products with up to 100 Mbit/s, P2P traffic (legal and illicit) is expected to stay one of the most important drivers of Internet traffic.

Exhibit 34: ***P2P Germany, 2007 content distribution***



Source: ipoque

A variety of mitigation measures have been implemented to allow digital rights to be protected effectively by content owners, with varying degrees of success and controversy. For example, DRM usage has drawn criticism from politicians and consumer associations on grounds of non-transparent user rights. This has led to pressure on network providers and ISPs to engage more proactively in mitigating copyright infringement. Network providers and ISPs are not held liable to monitor the nature of their customers' Internet use or the traffic over their networks due to the long-held legal principle of their business being classified as "mere conduit." Still, we observe that network providers and ISPs are increasingly active in deploying self-regulatory codes and awareness campaigns to raise awareness and create a value perception of the concept of intellectual property among the "born digital" generation who predominantly believe that all online content should be free. Awareness campaigns and codes are also among the mitigation measures discussed in the context of national (co-)regulatory initiatives.

Potential measures contemplated in such cases include: Monitoring through inspecting traffic (DPI) and/or filtering content; notice and takedown upon notification by competent authorities (applicable to network providers that host content); restriction or blocking of access to certain sites or certain protocols; obligatory disclosure of user personal data like IP addresses for prosecution purposes; dispatching of letters to Internet account holders when their accounts have been identified as having been used to unlawfully share copyrighted material; direction of consumers to other sources of legally available material; and even temporary bans of persistent illegal downloaders from accessing the Internet—the so-called "three strikes" rule or "graduated response."

All of these measures entail important questions as to how to arrive at best practices, balancing anti-piracy objectives with existing legal liability regimes established for "mere conduit" providers; with fundamental user rights in relation to personal data and online behaviour; and with the general notions of a free Internet, freedom of information, and digital inclusion. The political tide in Europe appears to favour protecting the user, provided that he/she does not intend to make profits from his/her action. Disconnecting downloaders from the Internet is seen as a disproportionate measure set against objectives of reaching an all-inclusive Information Society. Copyright enforcement focuses more on criminalising uploading of

BitTorrent—P2P

BitTorrent is a widely used, real P2P protocol for content distribution. BitTorrent works without a central server for files; only a tracker server is needed as a central coordination point—essentially it has two tasks: (i) distribute torrent files (index server, that is, just a normal file/Web server; the torrent file describes the complete torrent download) and (ii) maintain a list of peers for each torrent file (i.e., if a new node connects, the tracker gives him a seed list of P2P nodes to connect to).*

Although BitTorrent is also used to distribute illicit content, the number of commercial uses is constantly rising—even more so the non-commercial legal use. Some examples for the use of BitTorrent (from Wikipedia and news reports):

- Sub Pop Records distributes music; Vuze distributes movies.
- Podcasting services recently picked up BitTorrent for distribution, mainly supported by the player software "Miro."
- Amazon S3 (a storage solution) uses BitTorrent for file transfer.
- World of Warcraft uses BitTorrent to distribute updates to the game (several 100MB files).
- Patches are distributed, for example, INHOLLAND university distributed 22TB of patches to 6,500 PCs in only 4 hours—almost impossible in a client/server environment (took 4 days without BitTorrent)—and reduced download servers by 20 (previously 22; now 2).

Due to this increasing use, the protocol can not be "banned" from the Internet, as is sometimes proposed (to minimize file sharing and to help universities avoid liability issues with the media industry).

* Note: BitTorrent can also be implemented without a central tracker server, for example, using distributed hashtables (many implementations already support this). This allows for a real, serverless P2P system.

Direct Download Links (DDL)—An Alternative to P2P File Sharing

- Direct download links work like normal Web servers, that is, they do not transfer files between peers.
- Users can create account and upload files (up to several 100MB). These files are accessible via a direct link, which is known only to the user (that is, there is generally no way to search for content on the DDL server).
- The uploader now distributes the link (normally via third-party forums) and anyone can then download the files.
- Users without a paid account on the DDL server have limited bandwidth and a maximum volume to download. Furthermore, users have to wait before every download (around 1 to 2 minutes for the first download, with the time increasing for subsequent downloads based on volume used) and fill out a captcha for every download.
- Popular DDL solutions are, for example, Rapidshare and MegaUpload; the services are currently not very popular in Europe but are heavily used in the Middle East (9 percent of traffic in the Middle East is DDL traffic).

copyrighted material than on downloading, which is not even illegal in all jurisdictions. Furthermore, measures such as filtering and DPI require heavy investment from operators, and the question remains who should be responsible for incurring the cost of such actions, weighed against the extent to which value preservation in the content industry can be quantified and directly attributed to such measures. For example, a 2007 report of the Value Recognition Strategy working group in the UK suggested that format changes (i.e., "unbundling" of CDs into "a la carte" selections of songs by the likes of Apple iTunes) and price pressure from discounted CDs on sale in supermarkets are more responsible for the value loss of the British recording industry than are P2P file sharers.

7. SUMMARY

Addressing all of the four pillars of Digital Confidence will enable the next phase of growth of digital life. The actions already being taken by various stakeholders point to a broad recognition of the issues and the need for action.

But stakeholders are facing a multi-dimensional problem. For example, there are important differences in legislation on key issues in many countries, whilst, for example, digital attacks

like phishing are cross-border and require international cooperation with regard to prosecution. It is often difficult or even impossible to track down offenders and prosecute them—the measures and tools defined for the "analogue" world simply are not effective in the digital environment. Furthermore, there exist huge gray areas due to the rapid evolution of technology and behaviour and the new possibilities in the digital world, ranging from easy duplication of digital goods to the worldwide accessibility of the Internet.

The industry broadly recognizes Digital Confidence as a top agenda item but is still wrestling how to address it effectively.

Regulators and government agencies are being challenged to define their position and can be seen to be oscillating between heavy-handed legislation and consumer education or are pursuing market self-regulation philosophies. A crucial role in tackling Digital Confidence issues is also played by international cooperation and ratification of international treaties to approximate national legislation allowing for common criminalisation of activities that sometimes may appear clearly illegal but are lacking a legal basis to tackle. For example, in the UK only recently, in May 2008, new legislative proposals were announced to close a legal loophole that left drawings and computer-generated images of child sex abuse unpunished.

Industry is faced with a choice of different levels of intervention. It must weigh requirements of new business models and capital expenditure against the broader public policy concerns and the need to innovate and develop new services and network topologies that satisfy the needs and values of the "born digital" generation. Industry is generally concerned about exposing itself to uncontrollable legal liabilities and relies on backup by government agencies or regulators. Depending on the issue at hand and on the country, there can be no "one-size-fits-all" approach to fostering Digital Confidence, but important lessons can be drawn from best practices. The lack of a coherent approach comes ultimately at the detriment of the consumer, who lacks transparency and guidance around the risks and benefits of digital life, whilst businesses are challenged to create sustainable, new digital business models.

The most difficult aspects of Digital Confidence centre not around what needs to be tackled, but around how and by whom. The most appropriate measures need to be defined and responsibilities assigned—that is, on what level is action required: Consumer, company, regulator? And crucially: Who should pay for such actions?

Based on the interviews we conducted, the difficulties reside less in the technological solutions but more in the fundamental, underlying policy issues: Should a company get involved in, for example, blocking illegal and undesired content, which may mean facing the risk of legal liabilities? If so, who determines what illegal and "undesired" means? How should the line be drawn? For example, if child sexual abuse content is blocked, what about racism?

Defining the four pillars of Digital Confidence allows companies to analyse the problem, set priorities, and tackle it.

Ultimately, the issues faced involve a broad range of interests, with no simple answers. The four pillars of Digital Confidence as defined order and structure the most important aspects of the problem, which allows for a comprehensive debate and action.

CONTENT FILTERING

Content filtering is used to restrict access to specific sites or parts of sites on the Internet. Traffic/content filtering can be used for many different purposes, for example, to:

- Filter spam e-mails.
- Restrict or block access to illegal content, like child sex abuse content or copyright-infringing content.
- Deny minors access to inappropriate content.

According to the underlying motive, the approach to filtering is different. Generally, a distinction can be made between end-user equipment-based filtering (often used for minors' protection solutions as parents can easily disable it for themselves) and network-based filtering (e.g., to restrict or block access to illegal content) or in a combination (e.g., for spam filtering; e-mail servers filter spam based on blacklists and e-mail clients filter the rest of the spam based on content).

For network-based filtering, a variety of approaches exist, as shown in Exhibit 36. The most common implementation is DNS-based URL filtering*. In this case, certain access to the IP address underlying a specific domain is blocked based on the domain name (e.g., "www.google.com" would be restricted, but not "www.google.uk" because these are different domain names). This filter can be implemented quite easily by each individual network provider and is effective for all customers using the provider's DNS server. On the downside, this filter can be easily evaded by connecting to an alternative DNS server without filters installed, and it can be used only for blacklisted content. DNS filtering has nevertheless proven to be effective in preventing unintentional or accidental access to illegal content.

More sophisticated filters examine the actual content of the traffic, to determine if it should be filtered. A simple example is the detection of spam e-mails. In this case, the mail server analyses the content of the e-mail. Another example is simple "adult content filters," which scan the text of a website for keywords like "porn" and then block the access to them. The most complex version of this is Dynamic Content Fingerprinting Filters, which can analyse the content of audio and video traffic, for example, to determine if copyright-protected files are transferred. DPI is another example. The technology needed to enable these more sophisticated filtering techniques is, however, controversial. DPI enables monitoring of individual traffic on a "keystroke-by-keystroke" basis, which could also include e-mail correspondence. DPI has raised privacy concerns as it allows for collection of personal data (websites visited, searches) and raised concerns regarding unlawful intercept.

Blackholing is a very simple but yet extremely effective filter—but not without significant shortcomings. Blackholing blocks complete access to a single IP address (packets destined for this address are not forwarded) and is difficult to circumvent, even for experienced Web users. But since several systems and websites can be located at the same IP address, blocking one IP might block hundreds of websites or users as "collateral damage" (called "overblocking"). Therefore, this is a measure used only if the integrity of large networks is endangered or users are at high risk if blackholing is not deployed.

Filtering measures in general can be effective only when listings of illegal content are governed, maintained, regularly updated, and well enforced. However, there are broader public policy implications at stake should lists be extended beyond their original purpose and in instances where illegal content is not taken down within an adequate time frame.

Exhibit 35: *Website traffic filtering toolbox*

	Proxy based URL filter	DNS based URL filter	Dynamic Content fingerprint filter	Content keyword filter	IP blocking/ blackholing
Description	URL of request is analysed and verified with black/ white list	DNS entries for specific domains are blacklisted and rerouted	Content of packets is inspected (DPI) and fingerprinted (i.e. identification of content)	Content of packets is inspected (DPI) and keywords are detected–normally for http/smtp only	Selected single IP addresses are blocked in routers (border and internal possible)
Impact of intervention	Precise/Targeted → Number of affected sites				
	Single Page	Single Site/Domain	Content fitting the fingerprint	All pages/URLs containing keyword	All sites/devices located at this IP
	★★	★★★	★	★★	★★★
	Proxy server needed	DNS configuration	DPI very complex and content database needed	DPI needed	Router configuration
Pro/con	Less easy to circumvent than DNS-based filtering but higher technical complexity and problems with traffic volume	Filter easy to circumvent with changes in local DNS configuration	Content can be detected, but decision about legal use not possible	Depending on keyword very over-blocking, circumvented by encryption	With NAT/shared hosting extreme over-blocking, circumvented by tunnelling
Example		Blocking of sites based on blacklist (e.g., ThePirateBay block in Denmark)	Detection of copyright protected audio files when file sharing	Simple filters for PCs, blocking all sites containing the word "sex"	Blackholing used to protect networks and devices from Denial-of-Service

Note: Non exhaustive, e.g., Port based blocking can be used in addition to DNS based filtering to make circumvention more difficult

Source: Booz & Company

★ Difficult/Expensive Implementation ★★★ Simple/Cheap Implementation

* DNS is the domain name system that allows a PC to find the server for a given domain.

IV. TODAY'S APPROACHES TO DIGITAL CONFIDENCE: SIGNIFICANT ROOM FOR IMPROVEMENT

To develop a coherent framework for ensuring Digital Confidence, it is essential to review the approaches used by various stakeholders to address the increasingly prevalent challenges around Digital Confidence.

A set of case studies is discussed to understand best (and worst) practices and to derive lessons learnt to build on going forward. The case study view is then complemented by a brief review of the regulators' agenda as it relates to Digital Confidence.

1. CASE STUDIES: HOW TO GET DIGITAL CONFIDENCE RIGHT—OR WRONG

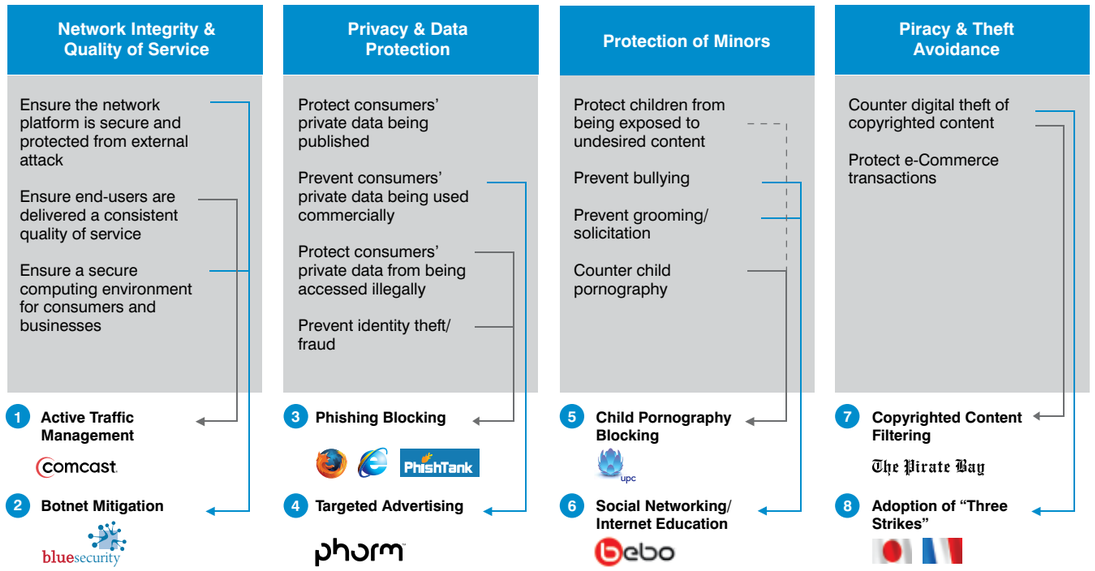
The cases have been identified along the four Digital Confidence pillars—Network Integrity and Quality of Service, Privacy and Data Protection, Piracy and Theft Avoidance, and Minors' Protection. Per pillar, two cases have been selected to illustrate the objectives of each pillar as much as possible and to allow for insightful conclusions (Exhibit 36):

- "Learning potential".
- Timeliness.
- Geographic diversity.

As set out in Chapter III, one of the key issues is the general position a company takes in a specific area of Digital Confidence: How protective or even prescriptive do I want to be or do I need to be? How intrusive can the measures applied be?

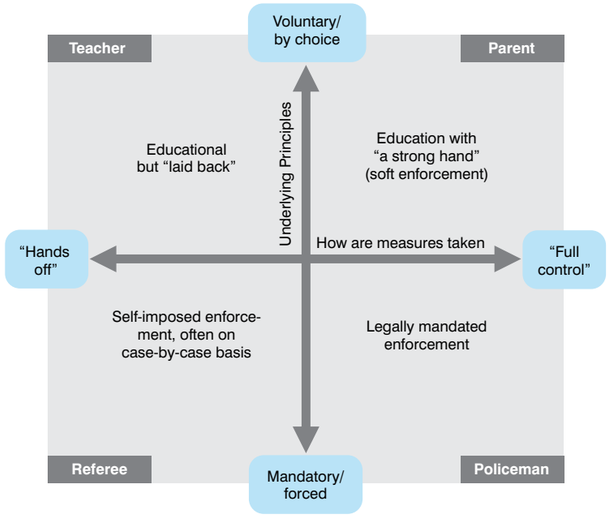
To examine the cases, a generic Digital Confidence Positioning Framework has been developed (Exhibit 36). Within this framework, the horizontal axis depicts how measures are taken (e.g., passively in a "hands-off" manner or actively in a "full-control" approach) whereas the vertical axis differentiates the underlying principles. The resulting four quadrants can be clearly linked to generic societal roles.
For example:

Exhibit 36: *Today's approaches—selected cases*



Note: Colors of arrows only to distinguish cases
Full line = major aspect in case; Dashed line = minor aspect

Exhibit 37: *Digital Confidence positioning framework*



- The teacher educates users about opportunities and threats as much as possible, but will normally not take active corrective measures (e.g., "Web Wise Kids" producing educational material for children on the Internet).

- The parent educates users about threats and measures similar to a teacher, but will take measures proactively if deemed necessary to protect users (e.g., YouTube filtering copyright-protected content).

- The referee relies on self-imposed enforcement of rules on a case-by-case basis and on guidelines rather than on education, but rules are based on mutual agreement (e.g., UPC NL proactively blocking child sexual abuse content domains).

- The policeman is naturally inclined towards strong enforcement based on legal mandating, takes all measures necessary to do so, and does so based on strict rules, for example, to block all illegal activities (e.g., the implementation of a "three strikes and you're out" rule in case of copyright infringement).

CASE 1: ACTIVE TRAFFIC MANAGEMENT

*Problem: **Network providers face increasing bandwidth usage and need to manage network traffic to avoid network congestion and ensure quality of service.***

*Risk: **Quality of service (QoS) may suffer due to spikes in bandwidth demand—but upgrading network bandwidth alone would be prohibitively expensive whilst not providing a long-term solution.***

Heavy users consume high amounts of bandwidth at the expense of regular users. Applications such as file sharing and video streaming are significantly more bandwidth-hungry than standard Web browsing or e-mail. This varying intensity translates into strong peaks in utilisation of the overall capacity of any given network. Network providers are addressing this by investing in next-generation access networks to continuously expand the capacity available to end users. But to ensure that all customers experience optimal QoS, more than just expanding capacity is needed. There is a group of heavy users, increasing in size, that uses an increasing amount of bandwidth, which means that capacity increases alone can only be a short-term solution to dealing with bandwidth crunches. Therefore, traffic also needs to be managed to ensure a "fair" distribution of bandwidth consumption and QoS for all users (Exhibit 38). In a flat fee tariff environment, users with high consumption (steep part of curve) are "subsidised" by users with low consumption. As an illustration: If 10 percent of heavy downloaders would be traffic-shaped or migrated to higher-usage tiers, fairness in distribution of available bandwidth to all users would increase by almost 50 percent.

Tiered pricing and traffic management measures are the two major remedies. Tiered pricing could incentivise heavy users to decrease network usage by charging premiums for downloading at peak time, especially for bandwidth-hungry applications such as file sharing. These premiums have two effects: First, they will shift demand anyway from peak times, and, second, they will translate into additional revenue that can contribute to covering infrastructure expansion cost. Canadian cable operator Rogers introduced tiered pricing, AT&T in the United States is evaluating a special pricing model for BitTorrent traffic to mitigate the impact of P2P traffic on the network (the company predicts total bandwidth use on its network will increase fourfold over the next 3 years), and Time Warner is testing a metering pricing system that charges users by the amount of bandwidth they consume.

Traffic management measures encompass a broad array of network-driven measures aimed at facilitating traffic flow and ensuring quality of service—complementing general network dimensioning, which is particularly aimed at dealing with peak usage times. Measures range from enforcement of fair use limits to various forms of shaping and implementation of different approaches in traffic selection to ensure the best QoS (see also Chapter III).

Approaches that players have taken to traffic management can be discussed with reference to an adapted version of the generic Digital Confidence Positioning Framework (Exhibit 39). The vertical axis differentiates the general position a network operator or ISP can take towards traffic management. In this, the upper pole is a position that sets incentives but does not interfere with actual user activity whereas the lower pole is a forced position that actively reacts to and manages traffic based on the overall user activity at a given point in time. The horizontal axis differentiates the degree to which actual traffic data determines the actions being taken, that is, how specific the employed technical measures are. Service-specific shaping differentiates between various types of traffic at a more granular level than protocol-specific shaping, for example.

Certain positions in the matrix are more natural than others: For example, a "pricing-only" approach as in the Teacher quadrant is unlikely to exist, given the current imbalance between bandwidth availability and demand –network operators cannot ensure a well-operated network without any technical measures of traffic management.

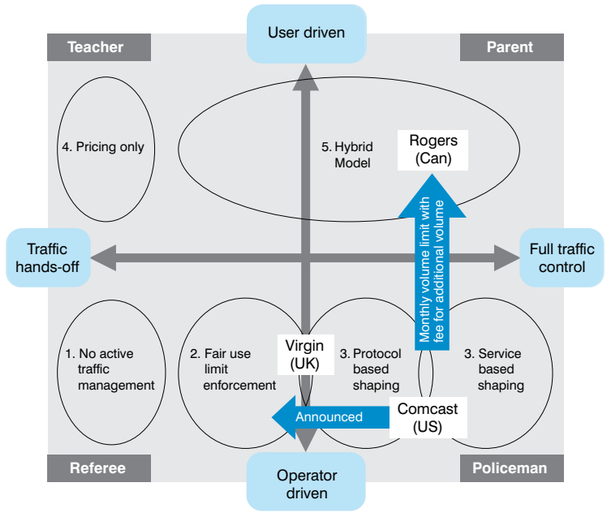
Against the matrix, a number of recent practices stood out. Comcast, one of the largest cable operators in the United States, faced significant traffic increase due to the increased use of P2P systems. Under this pressure, Comcast tightened its traffic management and faced strong opposition from the public. Rogers, in Canada, introduced usage allowances, charging extra for traffic above certain limits (a limit of two up to 100GB per month). This is an example of an hybrid approach, combining traffic management with tiered pricing. In addition, Virgin Media in the UK is an example of a cable operator being very open about its traffic management activities.

*"Unmanaged networks result in serious degradation of service availability and quality for all users. It will also mean that customers will be paying more for less, as providers are forced to continually build out their networks to stay ahead of the massive bandwidth consumption growth."**

Comcast implemented network management measures impacting on P2P traffic from BitTorrent that produced too restrictive outcomes: BitTorrent download was possible, but users reported that uploads were delayed and that the implementation also affected other, more time-sensitive applications like Lotus Notes. Individual user complaints eventually led to broad public attention including investigation by the FCC. Comcast was also accused of providing a misleading service promise and computer fraud. In response, Comcast took on the problem in a very dedicated manner, worked together with

**Kurt Dobbins, Arbor Networks*

Exhibit 38: *Digital Confidence positioning–active traffic management*



1. Few network operators do not actively manage their traffic
   – Pro: As long as enough spare capacity, no real need for guaranteed user experience–potential networkcongestion
2. Network operators have "Fair Use" policies in place, based on network dimensioning aimed at managing peak usage times
   – Users exceeding Fair Use limits may be migrated to alternative (higher bandwidth) broadband subscriptions
3. Active traffic management is deployed to guarantee QoS for all users
   – From a net neutrality standpoint, a protocol-agnostic approach is preferable to a service-specific approach
4. A business-driven alternative to bandwidth management is usage based, differentiated pricing
   – Pro: Market-backed incentive to manage congestion by creating disincentives for excessive use
   – Con: Undermine usage convenience, potentially, competitive disadvantage
5. Hybrid models ("additional use policy") use differentiated pricing when usage exceeds certain upper limits/caps
   – Average user still benefits from "flat fee" convenience–only heavy users will pay usage premium

BitTorrent, and found a mutually acceptable solution, that is, Comcast will use a platform-agnostic technique that may ultimately slow down P2P traffic only from its heaviest users.

*"So the real question for today's broadband networks is not whether they need to be managed, but rather how."**

This agreement seems to be finding approval among net neutrality proponents. Google called Comcast's commitment to a protocol-agnostic approach to network management "a step in the right direction." However, it did not appease the FCC, which decided to move ahead with a ruling that denounced Comcast's earlier practice.

While appreciating the need for "reasonable" network management, the FCC alleged that Comcast arbitrarily blocked Internet access regardless of the level of traffic, and failed to disclose to consumers that it was doing so. In July 2008, the FCC chairman recommended enforcement action requiring Comcast to stop its "practice of blocking" (although "delaying" is probably a better description); provide details to the consumer on the extent to which and the manner in which the practice was used; and to disclose to consumers details on future plans for managing its network going forward. This action follows an FCC policy statement issued in September 2005 that outlined a set of principles meant to ensure that broadband networks are "widely deployed, open, affordable and accessible to all consumers." The principles, however, are "subject to reasonable network management." The FCC ruling on Comcast seems to be more of a statement of principle, also because Comcast is unlikely to be fined, and appears aimed at setting a precedent by further specifying what "reasonable network management" means in practice.

Some players like Virgin Media or Rogers are very transparent on their approach to traffic management—acceptance seems high.

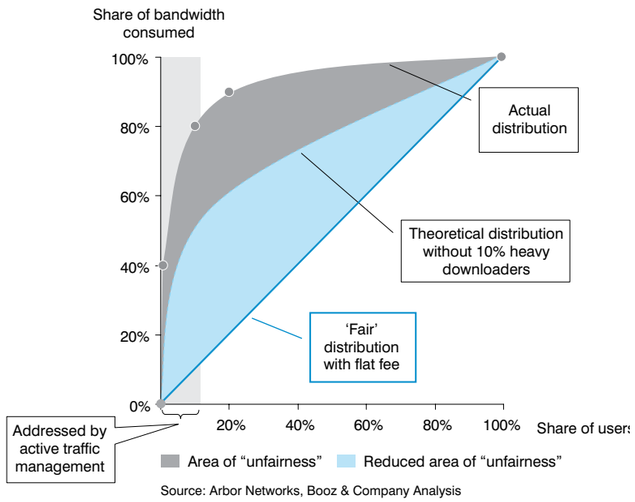
*Vint Cerf, Chief Internet Evangelist, Google

Rogers introduced usage premiums in March 2008. Users have to pay an extra $1.25 to $5 per month depending on their tariff plan, with a maximum of $25 across all plans. An increasing number of network providers have started considering the introduction of usage-based pricing models to manage their increasing bandwidth demand. The difficulty with this tiered approach is that it may undermine the basic promise of "flat fee," which was a key driver for the development of the broadband mass market, that is, carefree broadband use without having to worry about inflated cost due to usage that was difficult to monitor. Rogers is addressing this issue with the $25 cap. Rogers itself is very open and unpretentious about its policy, stating on its website: "The majority of our customers are on plans that meet their needs and should not expect to go over their monthly usage allowance. If you do go over, you can pay for additional usage on a monthly basis, or change your level of service so that it meets your online needs. Measuring usage this way more fairly reflects how our customers are using the service and allows us to maintain competitive monthly rates for all of our customers."

In the UK, Virgin Media is also very open about the need for traffic management and the chosen implementation. Currently, Virgin is using traffic shaping to manage the top three percent of its heavy users—the rules deployed are publicly available on the website. Virgin Media is putting its measures in the context of a fair use policy safeguarding QoS for the vast majority of users. Virgin Media is also thinking about the introduction of pricing-based models in the future.

Traffic management is increasingly attracting more regulatory scrutiny. The expected FCC ruling on the Comcast case underlines that consumer protection is high on its agenda in the context of defining what constitutes "reasonable" traffic management. But the topic is complex also from a regulatory point of view. Exhibits 40 and 41 illustrate what kind of economic impact regulatory decisions could have in that context. Imposing very strict QoS regulations impacting on the extent to which traffic management may be implemented could add significant extra cost to the industry in Europe. As the cost could not be swallowed by the network providers, they would need to recoup this through higher-end consumer prices. Ultimately, the excessive usage of a fairly small customer segment could lead to a general increase in end consumer prices. This is why regulatory action in the area of traffic management needs to be balanced carefully.

Exhibit 39: *Bandwidth consumption across user groups*



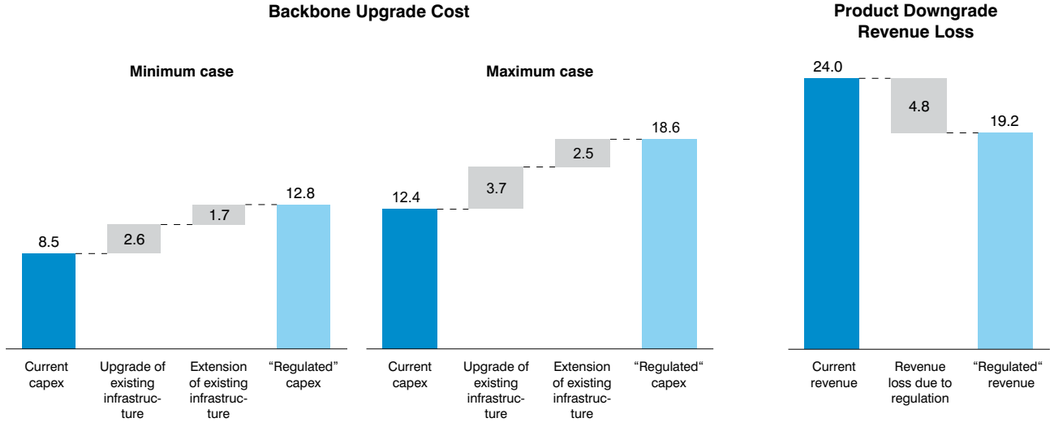
Source: Arbor Networks, Booz & Company Analysis

IMPLICATIONS OF CERTAIN MINIMUM QOS REQUIREMENTS REGULATION ALTERNATIVES

Exhibit 40: *Breadth of possible QoS regulation*

0. No Shaping Allowed	1. Low QoS Requirements	2. Medium QoS Requirements	3. High QoS Requirements
• Net Neutrality can be interpreted as prohibiting traffic shaping in the network • This can potentially be combined with other options but very difficult to achieve	• Can be implemented via configuring existing network management solutions – Shaping based on service/ protocol – More or less aggressive shaping	• E.g., minimum bandwidth or moderate latency requirements • Can be implemented within existing infrastructure and small upgrades – Backbone upgrades for more bandwidth with less shaping – Access upgrades (new CPE)	• High QoS requirement (minimum bandwidth, combined with low latency and jitter) • Existing network not sufficient to fulfil, new technologies need to be implemented
• Network operators, currently applying shaping, have two potential options – Upgrade backbone Network – Downgrade products	• No backbone or access upgrades necessary	• Backbone or access upgrades necessary for parts of network • Differs for DSL and cable operators due to different technical restrictions (e.g., cable with shared access network can easily deliver more bandwidth but more prone to congestion)	• Backbone and access upgrades necessary (essentially rebuild of network)
Product downgrade or upgrade of network	**No upgrades**	**Upgrade of network**	**Network "rebuild"**

Exhibit 41: *Financial impact of "no-shaping" regulation in Europe (billions euros)*



Note: Europe: EU-27 + Norway + Switzerland
Note: This is a hypothetical scenario, assuming shaping is not allowed in Europe and currently 20% of all traffic is shaped and 67% traffic growth p.a. (not assuming any distribution of shaping across players)
Source: U.S. BEA, Merrill Lynch, Ofcom, Company Reports, Booz & Company Analysis

KEY LESSONS

Five key lessons emerge from the discussion:

- Managing network congestion and capacity constraints is an essential part of every network operator's business—tiered pricing and traffic management measures are the two major remedies.

- Usage is expected to grow in step with bandwidth increases in next-generation access networks. This makes the issue even more important as heavy usage of bandwidth-hungry applications is expected to grow. Charging a premium for heavy usage may contribute to more balanced traffic flows and fair distribution of available bandwidth to all users.

- Traffic management measures are always needed to a certain degree and are appropriate to ensure QoS across different traffic types; being transparent in public about these practices is necessary to manage service expectations.

- The implementation of traffic management measures has to consider the net neutrality discussion—implementations that are protocol-specific (like BitTorrent) have been harshly criticised in public. Protocol-agnostic "fair use" enforcement seems therefore fairest when it manages disproportionate usage behaviour and is directly aimed, and limited to, managing the level of traffic only at times of actual congestion. This approach may offer the best overall QoS experience and a level of intervention that is proportional to net neutrality.

- Issues related to traffic management may be effectively governed by reaching mutually acceptable and transparent agreements between network operators and, for example, application providers. The level of broadband competition in a given market should determine the need for regulatory intervention.

(4)Note: Within this document, the term DoS is used, although technically, the attacks from botnets are DDoS attacks (Distributed Denial of Service attacks).

P4P as a Way to Mitigate Some P2P Traffic Whilst Improving Quality of Experience for Users

P4P is the "Proactive Network Provider Participation for P2P," an initiative by the Distributed Computing Industry Association (DCIA). Core working group members include various thought leaders across the industry, including AT&T, BitTorrent, Cisco, Joost, Pando, Telefonica, Verizon, and Vuze.

P4P has two goals of development: (i) decrease backbone traffic, and (ii) reduce network operation costs. The technical idea behind it is to build a P2P system (BitTorrent-based) that uses additional information about the network topology to select the peers to exchange data with. To support this, additional tracker servers are maintained by the ISP, allowing it to sort the available peers based on optimal routes.

Additionally, the idea of caches at the ISP level is introduced—allowing the reduction of data volume in backhaul and access (clients need to upload data only once to the cache; the cache can serve all requests into the network). First tests with Pando (BitTorrent-based) show that delivery speed increases by 200 percent to 800 percent with a 40 percent to 75 percent inter-ISP data transfer decrease.

CASE 2: BOTNET MITIGATION

Problem: ***More and more consumer PCs are infected by bots, malicious software which can be controlled remotely by criminals ("bot herders"): ISPs want to remove bots from the Internet to protect consumers and networks.***

Risk: ***Botnets are the major source of most digital attacks, like phishing, sending spam, click fraud, etc.***

Botnets are likely the most severe form of network integrity infringement for criminal purposes: A botnet is a collection of PC terminals in consumer homes, businesses, universities, etc., that are controlled remotely by an unauthorised, malicious third party without the PC owners being aware. Botnets can consist of several hundred thousand computers.

Botnets can be used for several purposes from spamming and denial-of-service (DoS)[4] attacks to phishing and click fraud. Some recent examples show what drastic consequences botnet-executed DoS attacks can generate. In April 2007, after a Russian statue was removed in Tallinn, the capital of Estonia, a "manual" DoS attack was organised: Bloggers asked their readers to ping specific Estonian services to create a DoS. A ping is a software utility sending a packet to a specific IP address to determine whether the address is available. It is primarily used to troubleshoot Internet connections, but it can be abused in the way described. After being unsuccessful with this attack, a botnet was "rented" and a "real" DoS attack launched. Targets of the attacks included the websites of the Estonian presidency and its parliament, almost all of the country's government ministries, political parties, three of the country's six big news organisations, two of the biggest banks, and firms specialising in communications. The attack literally "took down" the digital side of life in a country where, for example, 90 percent of bank transactions are made online.

In April 2008, Radio Free Europe, a private non-profit organisation funded by the United States, experienced a massive DoS attack. Several Eastern European websites of Radio Free Europe were attacked by DoS, that is, flooded with fake requests (leading to all resources being used by the DoS attack). Both these attacks were essentially politically motivated and were carried out by (often "rented") botnets.

As most of botnets' purposes are illegal, prosecution by law enforcement plays a central role in countering botnets. In the United States, the FBI executed operation "Bot Roast" in Summer 2007, identifying about 1 million computers that had been compromised across the United States and charging numerous individuals with computer/cyber crimes. Beyond prosecution, mitigation strategies against botnets unfortunately are limited—preventing the infection in the first place is most effective but difficult.

*Kraken is one of the largest known Botnets**

Approaches to "non-prosecuting" botnet mitigation can be structured along an adapted version of the generic Digital Confidence Positioning Framework (Exhibit 50). The vertical axis differentiates where mitigation takes place: On the end-user or on the network side. The horizontal axis differentiates the forcefulness of intervention. The left pole stands for no intervention at all, the right pole for a strongly interventionist position.

Education is a clear example for a non-interventionist and user-centric measure: Ensuring that end users understand botnet risks and what to do against them. For example, the European Network and Information Security Agency (ENISA) has published educational materials for consumers about botnets, their threats, and how consumers can protect themselves.

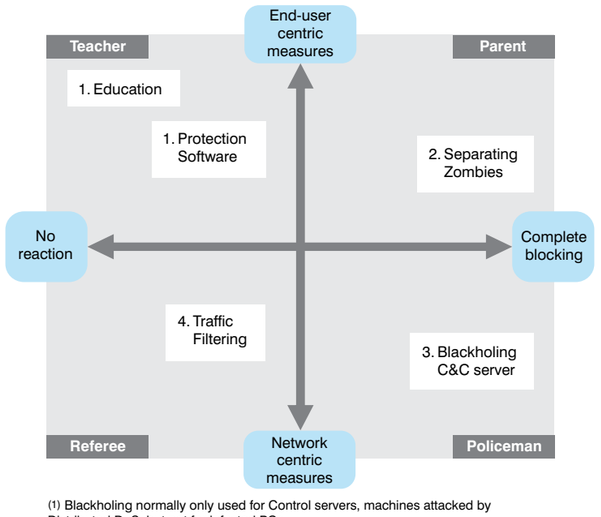
Another measure to be seen in the Teacher quadrant is software that protects computers from being infected with bots. Almost all current commercial anti-virus and firewall products contain features to prevent bot infections. Suppliers of such software are also vulnerable themselves: Blue Security, a small company focused on Internet security software, actually was pushed out of business by a massive DoS attack in May 2006.

Blue Security had developed and brought to market an anti-spammer product that was said to be very effective—and ironically was also botnet-based.[5] Thereafter, Blue Security was blackmailed by spammers to shut down business. After Blue Security refused this, an initial DoS attack was targeted at the Blue Security servers, shutting them down. The administrators redirected the DNS entry to TypePad, one of the largest blog hosters also used by Blue Security. Massive subsequent DoS attacks temporarily

**500,000 infected PCs 50 Fortune 500 companies affected*

(5) If Blue Frog detected a spammer, all machines using Blue Frog sent an e-mail to the spammer, basically being a botnet performing a small DoS attack on the spammer.

Exhibit 42: *Digital Confidence positioning—botnet mitigation*



1. Most ISPs provide users with education and appropriate protection software
   - Pro: Can already prevent bot infection
   - Con: Software protection not 100% safe and users need some technical background
2. Separating infected PCs from the Internet into a "walled garden" is implemented very limited
   - Pro: Walled garden minimises spread of botnets
   - Con: Liability issues with false positives and very customer care intensive
3. Blackholing essentially means disconnecting machines from the Internet[1]
   - Pro: Very effective, especially for older botnets (or to mitigate DoS attacks)
   - Con: Extreme measure since all traffic is blocked to this machine
4. Filtering botnet traffic–although being very effective–is difficult to implement
   - Pro: Minimises threat with little disturbance of other activities
   - Con: Botnet traffic difficult to filter since very similar to normal Internet traffic

(1) Blackholing normally only used for Control servers, machines attacked by Distributed DoS, but not for infected PCs

shut down TypePad and Tucows, Blue Security's DNS provider, both being large and important Websites. Only with a coordinated response of several network operators and service providers, could the attacks, with peak traffic of more than 3GBps, be mitigated to protect these third parties. But Blue Security was offline for several days. Two weeks after the initial attack, Blue Security shut down its anti-spamming business.

*Blue Security CEO Eran Reshef on fighting spam: "This is something that's really got to be left to governments to decide. To fight the spammers you really need to spend $100 million."**

A more end user-centric but interventionist approach would be to separate out zombies, the individual computers in a botnet. This is a powerful yet difficult mitigation measure, suggested by the Message Anti-Abuse Working Group (MAAWG). It means that infected computers are separated from the Internet into a walled garden with security updates and disinfection possibilities. So far, this measure has been implemented to only a very limited extent, for example, in large private networks such as universities, due to the potential liability issues.

The most effective measure always was to blackhole/disconnect the command and control (C&C) server of the botnet. For example, as early as 2004, the Norwegian incumbent ISP Telenor defanged a botnet of 10,000 zombies by shutting down its C&C server. But bot herders have reacted to this, and now increasingly use new types of botnets, without a central C&C server.

Last, a network-driven but less interventionist approach is the deployment of traffic-filtering techniques to mitigate botnets. As for other purposes, filtering here has the aim of recognising the unwanted botnet traffic and then blocking respective IP packets so that they cannot reach their destination. The challenge in this particular case is that botnet traffic is very difficult to filter since it is very similar to regular Internet traffic. Many ISPs and network operators currently use a simplified version of this approach, where they block all traffic that is typical for botnets—running the risk of overblocking legitimate uses as well.

In addition, ISPs also increasingly join forces with law enforcement by monitoring network activity and informing about irregularities. This way a large botnet was taken down in the Netherlands in 2005 when "Internet service provider XS4ALL notified authorities of unusual activity on its network." It had consisted of 1.5 million zombies. Three suspects were charged.

*http://blogs.guardian.co.uk/technology/2006/05/17/spammers_kick_blue_frog_into_submission.html

KEY LESSONS

Seven key lessons emerge from the discussion:

- The nature of IP networks, that is, their openness and neutrality, has made them very powerful, but also makes them easily accessible for "negative intentions" such as botnets.

- Due to their versatility in potential attacks, botnets are a major threat to network integrity and thus for network operators, service providers, businesses, and consumers alike—botnet activity often also has political motivations, as witnessed by the Estonia and Radio Free Europe examples.

- One of the most severe attacks is the denial-of-service (DoS) attack used to cut off unwanted sites or as a threat to blackmail companies—botnets have been responsible for all major DoS attacks in the last years.

- Prosecution by law enforcement plays an important role in countering botnet activities—to be successful, such prosecution typically requires other stakeholders, especially network operators and ISPs, to join in.

- Education is important but with limited effect due to the topic's complexity and the need for explanation and due to the difficulty for consumers in detecting infections.

- Network operators have to react on severe botnet attacks with technical mitigation measures. Since most measures are complex and interfere with user behaviour, network providers have to cooperate with all stakeholders to limit the measures needed.

- Isolating bots in walled gardens and cooperating with software vendors on disinfecting PCs promise to form an efficient solution—but network operators have to find ways to implement this in a user-friendly way (minimising need for customer care and offering opt-out possibilities for false positives).

CASE 3: PHISHING BLOCKING

*Problem: **Phishing mails have the aim of stealing the identity of someone or defrauding consumers.***

*Risk: **Consumers can lose significant amounts of money, for example, in case of stolen online banking account data. Authenticity of phishing e-mails often is difficult to check.***

Phishing has been highlighted as one of the most critical and fastest-growing issues with respect to Privacy and Data Protection. As it is a technically complex phenomenon, creating the needed awareness and knowledge with consumers is a challenging task. It is getting even more challenging as phishing e-mails and websites become more professional and increasingly difficult to differentiate from the legitimate versions, even for experts knowing what to watch out for.

No phishing filter is 100-percent safe.

Therefore, education can only play an accompanying role in mitigating damage from phishing. Apart from intensifying the prosecution of individuals and companies responsible for phishing, the main remedy is to block phishing attacks via technical approaches.

Approaches to phishing blocking can be discussed along an adapted version of the Digital Confidence Positioning Framework (Exhibit 44), with the vertical axis differentiating whether the user needs to voluntarily decide on a solution (i.e., opt-in) or whether protection is on as long as she/he does not opt out and the horizontal axis differentiating how the solution can be circumvented.

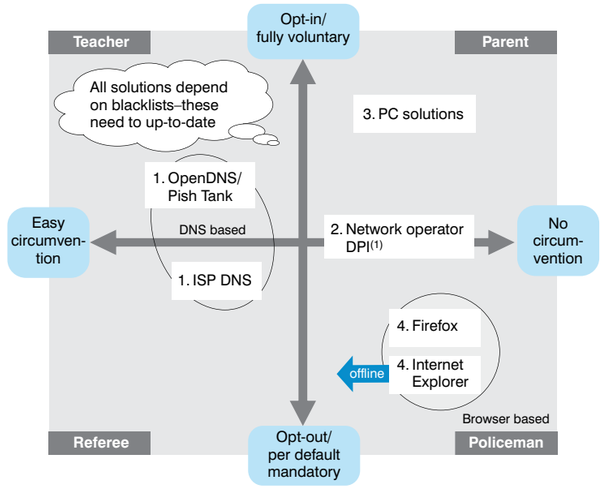
OpenDNS and PhishTank are an example of a community-based procedure for identifying phishing sites and blacklisting them (Exhibit 43). Due to a large community, phishing attacks are detected and verified very fast, in less than 12 hours.

This approach ties in with DNS filtering, leveraging the fact that specific domains can be blocked individually. It can be executed either on the ISP's DNS server or on third-party servers. The strong advantage of this solution is that it works for all applications, that is, it is not limited to Web traffic via an Internet browser but also covers e-mail, for example. At the same time, this blocking approach is useful for URL-based phishing only, limiting it to around 90 percent of all phishing attacks (10 percent are IP address-based, that is, they do not use domain names). Additional possible barriers are as follows: DNS-based blocking can require end-user system configuration, depending on the solution; and in the case of ISP-based DNS blocking, over-blocking can be a substantial problem as users have limited possibilities to access a site if it has been blacklisted incorrectly.

Second, ISPs can deploy DPI for blocking phishing attacks. DPI solutions inspect the content of every packet travelling on the network and can redirect malicious traffic, that is, also traffic to blacklisted phishing websites. This approach works for all applications and thus for most phishing attacks. Nevertheless, it triggers the usual privacy concerns associated with DPI in general: Consumers may dislike the amount of transparency service providers are generating

Technology is key to block phishing—it needs to be deployed at different levels: Network, PC, and browser.

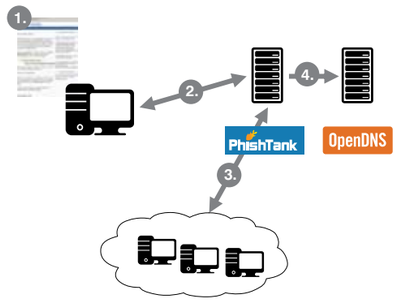
Exhibit 43: *Digital Confidence positioning—phishing blocking*



(1) E.g., solutions in conjunction with ad injection (Phorm)

1. DNS-based solutions can block the access to specific domains, this can be either on the ISPs DNS server or on third party servers
   - Pro: Works for all applications (not limited to browser but also in mail and others)
   - Con: Only useful for URL-based phishing
2. Deep Packet Inspection (DPI) solutions inspect the content of any packet and can redirect malicious traffic(1)
   - Pro: Works for all applications and many phishing attacks
   - Con: Privacy concerns and circumvented by encrypted traffic
3. PC-based security solutions normally also include a phishing filter
   - Pro: Depending on solution, it can protect all applications
   - Con: User has to install and configure solution
4. Current browser can check URLs against server or local blacklists (also heuristics possible)
   - Pro: Little privacy concerns (depending on implementation)
   - Con: No protection in other applications, e.g., mail or older browser versions

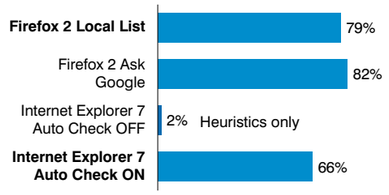
Exhibit 44: *Phishing blocking overview*



1. User receives fishing mail and goes to the phishing website–**User identifies the phishing attack (based on e-mail and website)**
2. User submits URL of phishing site to OpenDNS/ PhishTank as potential phish
3. OpenDNS/PhishTank community verifies the phishing attack
4. Domain is added to PhishTank Blacklist and blocked in OpenDNS
5. Further attempts to access the link are blocked

Source: OpenDNS.com, Phishtank.com

Exhibit 45: *Browser-based phishing blocking effectiveness test (2006)*



Bold: Default Mode
Source: Mozilla Foundation

in this case even if the resulting data is kept secure and not used for other purposes. Using DPI to prevent phishing is very effective and can be circumvented only by encrypting traffic (which can be seen only rarely in phishing attacks).

Third, the consumer's PC can be put in the centre: Many of today's PC-based security solutions include a phishing filter—for example, security suites from Norton, McAfee, Sophos, or others, which are also often provided to consumers by the ISP or network operator. Such filters can be very effective because, depending on the actual solution, they can protect all applications and thereby provide strong protection against phishing. A disadvantage of this approach is that it requires significant consumer contribution as solutions have to be installed, configured, and updated. Especially the regular update of local blacklists is crucial in guaranteeing good performance of the phishing filter.

An accurate blacklist is crucial: Only blacklisted phishing attempts can be blocked.

Lastly, phishing blocking can be executed on the browser layer. New browsers such as Internet Explorer 7 and Firefox 2 can check URLs against server or local blacklists to identify and act upon phishing attacks. In addition, heuristics can be used to detect phishing attacks (e.g., detecting phishing attacks based on patterns in URLs, formally used for phishing; but this approach has a very low success rate of only two percent). One advantage of this approach is that it does not trigger larger privacy concerns if the blocking is executed locally, that is, as with Firefox that downloads a list of phishing sites and checks against it automatically. One limitation is that browser-based blocking cannot help with phishing attacks in other applications, for example, e-mail (which is currently only a minor problem). In addition, it is vulnerable to malicious software on the user's machine, for example, a bot (see Chapter III) deactivating the feature or manipulating blacklists.

Browser-based phishing blocking reaches a high effectiveness if new browsers are used. With older browsers, such as Internet Explorer 6, third-party add-ons have to be used (which normally use similar blacklists).

Across all four approaches, blacklists are needed so that the blocking mechanism knows what to block. What is on the blacklist therefore is crucial for success and acceptance of phishing blocking on the whole: If a blacklist contains too many entries, overblocking occurs, that is, sites are blocked that should not get blocked (e.g., real login page for online banking that was mistakenly added to the blacklist); if a blacklist does not contain all entries or is not updated frequently enough, the protection is not very useful and can lead to liability issues for the blacklist provider.

KEY LESSONS

Five key lessons emerge from the discussion:

- Since phishing is difficult to understand for consumers, education is likely to be of limited power—it can only play a supporting role.

- Blocking phishing attacks is one of the central remedies—the various approaches all exhibit advantages and disadvantages around effectiveness, coverage (i.e., which applications are protected), privacy concerns, and required consumer activity—which need to be balanced carefully.

- The critical issue across all blocking approaches is the creation and management of blacklists depicting phishing sites to be blocked. Today, several effective blacklists are available (e.g., from Google, PhishTank) and in use.

- Browser-based solutions are most important today since they enable the richest user interaction and can include education about the issue seamlessly in case of an attack. A major problem are older browsers that do not include protection features—the software industry needs to cooperate with ISPs to push newer-version browsers into the market.

- Approaches seem to be most suitable that empower (experienced) users to opt out of or overrule the blocking mechanism, for example, in the case of content being blacklisted wrongly, and furthermore respect the consumer's privacy (e.g., with local blacklists).

CASE 4: TARGETED ADVERTISING

*Problem: **Consumers produce a lot of behavioural data when using the Internet, and businesses would like to use this for more targeted advertising.***

*Risk/upside: **Consumers are concerned about their privacy but business can significantly increase relevance of advertising (and thereby revenue).***

Web 2.0 brought the rise of many services based on social networking such as Facebook and MySpace. Many of these services broke records in terms of subscriber and usage growth—more often than not due to the fact that they are offered free to the consumer. This nevertheless increases the pressure on suppliers to monetise these services going forward. Advertising and in particular targeted advertising is expected to play a central role in the monetisation of Web 2.0 services—our market analysis shows that advertising will be the fastest-growing segment of the digital world (see Chapter II). Large Internet players like Google or Yahoo! have already started to capitalise on advertising—in fact, it's their main source of revenue. Consequently, the industry has seen some significant developments recently: Google purchased DoubleClick, one of the leading online advertising firms, for $3.1 billion in April 2007; AOL acquired Tacoda, which specialises in behavioural ads, in July 2007; and Yahoo bought Blue Lithium, which specialises in performance-based display ads, in September 2007. Also, network providers are increasingly relying on advertising-based business models to realise their growth ambitions.

If handled properly, targeted advertising can be win-win for consumers and industry: The advertising becomes more relevant and thus less annoying for consumers, whilst addressing specific target audiences is more cost-effective for advertisers.

The business rationale is straightforward: Younger consumer groups spend ever more time on the Web. Moreover, the Web makes additional information about the consumer accessible to the advertiser: What is he or she interested in? Where is he or she living? Some of this information is openly shared by the consumer on platforms like Facebook; other information can be obtained by collecting data on online behaviour.

Most if not all of these new business models require extensive data collection, and some recent implementations have raised privacy concerns. In the United States, for example, the Federal Trade Commission (FTC) hosted a conference in November 2007 to broadly discuss "Online Behavioural Advertising," with a special emphasis on privacy issues, and later on took the initiative to publicly suggest "Online Behavioural Advertising Principles."

From a Digital Confidence perspective, drivers and principles related to targeted advertising can be plotted along an adapted version of the generic Digital Confidence Positioning Framework (Exhibit 46). The horizontal axis differentiates as to whether the targeted advertising is website/application-driven (i.e., by Internet players such as social networks) or network-driven (i.e., by cable operators or ISPs). The vertical axis differentiates the degree to which the user can control whether his or her data is being used in such advertising, with the possibilities ranging from an "opt-in" that fully leaves the decision to the user to a "no opt-out" that uses data by default until the user removes the consent.

There are four distinct examples for how to implement targeted advertising. MySpace is testing a solution that is reported to be specifically opt-in. On the other hand, Facebook started Beacon in 2007, a solution that originally was implemented without user consent and only was turned into an opt-out solution in reaction to a big public debate. An example where targeted advertising has been successfully implemented is Gmail: Google offers a free

e-mail service but analyses the content of user e-mails to display targeted ads in the interface. These ads are an integral component of Google's e-mail offering: Users have to accept that the advertising shown is dependent on their e-mailing—judging by Gmail's success, users seem not to be too worried about this. Gmail did, however, cause a significant privacy-related controversy when it was first launched in 2004. Main privacy concerns ranged from unlimited storing of data and of non-Gmail subscribers' e-mails to Gmail users being analysed without their consent.

85 percent of users reject the idea of websites displaying ads based on previous websites.

The MySpace HyperTargeting solution classifies users based on their interests listed on the public profile (more than 100 categories). Advertisers can choose target classifications for their campaigns. In the initial tests, MySpace achieved a 300 percent increase in click-throughs, that is, three times as many customers clicked on an ad than before, and 50 percent extra cost for thousands impressions, or cost per mille (CPM). CPM is the standard model used to pay for advertising based on the number of consumers who view an ad. Although MySpace has only been testing so far, discussion around privacy concerns has already become intense. Still, with the solution set to be opt-in, MySpace apparently has understood the need to actively respect its users' concerns.

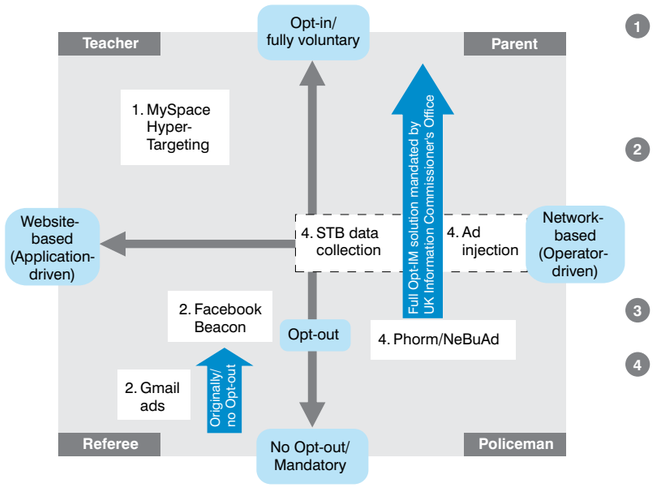
Several partners withdrew their participation after they realized that Facebook's Beacon is not an opt-in solution.

Facebook's Beacon, on the other hand, was initially enabled for all users without prior consent when it was launched in November 2007 with 44 partner sites. It integrated Facebook with the partner sites, allowing the exchange of extensive data collections and profiles as long as a user was logged in to Facebook. Originally intended to enable a more enhanced view in the Facebook stories ("your friend watched the video xyz at Joost"), it can also be used for targeted advertising. Significant privacy concerns were raised after introduction, including law suits against participating sites. In reaction, Facebook introduced an opt-out option as quickly as December 2007.

In the Gmail example, it stands out how openly potential concerns are addressed. Google has a detailed text on its website explaining in a transparent manner that targeted advertising alongside e-mails is more valuable to users than untargeted advertising: "Google believes that showing relevant advertising offers more value to users than displaying random pop-ups or untargeted banner ads." The Gmail solution is probably also seen as less controversial as users actually report finding the advertising useful and as the targeted data is used restrictively, only for ads to the user it relates to and only within the Gmail application.

Phorm and NebuAd provide network-based solutions for targeted advertising, allowing analysis of all Web surfing activities of users, so that display ads can be appropriately targeted.

Exhibit 46: *Digital Confidence positioning—targeted advertising*



1. MySpace's HyperTargeting categorises users based on their listed interests and shows ads based on these categorisations
   - Advertisers can choose categories
   - Currently in testing only but already raises privacy concerns
2. Facebook Beacon integrates Facebook profiles with other sites (actions on other sites are forwarded to Facebook)
   - Intended to enable a more enhanced view in the Facebook stories but can be used for targeted advertising
   - Privacy concerns raised after introduction, including lawsuits against participating sites (Harris vs. Blockbuster)
3. Google Mail displays ads based on the content of e-mails (automated content recognition)
4. Network based solutions like DPI analyse Web surfing activities of users (ad serving for participating sites or injecting in all sites(1))
   - Privacy concerns since traffic is inspected to derive profiles
   - BT trial without consumer consent triggered UK ICO to demand Phorm implementations to be opt-in in order to comply with UK laws

(1) Current solutions are focused on ad serving

Phorm will shortly be tested by major network providers, for example, by BT and Virgin in the UK. Phorm deploys DPI to analyse Web surfing activities, meaning that all traffic is inspected to derive profiles.

These highly advanced Internet monitoring capabilities of DPI, even where traffic data is anonymised for targeted advertising purposes, have intensified the attention and oversight of regulators in view of significant privacy risks. Indeed, rollout of these services in some markets has caused significant media backlash and user criticism, in particular of the way network operators have trialled, or intended to trial, these technologies. For example, BT began a pre-trial of Phorm-based targeted advertising without informing the relevant customer base, which triggered intervention by the UK Information Commissioner's Office (ICO), which demanded that customers eligible for the trial be duly informed about the technology and provide their consent by positively opting in to the trial, with an opt-out possibility being available thereafter at all times.

Charter Communications, the fourth-largest U.S. cable operator, stalled its announced targeted advertising trial within a month. Although Q&As on the company's website provided some transparency, users were unconvinced by the communicated benefit: An "enhanced browsing experience." Other concerns related to the use of DPI, which was considered too invasive. It also raised concerns about guarantees that personal profiles could not be compromised. Finally, Charter's opt-out solution was considered cumbersome. Users were required to fill out a form and have a special cookie placed. Clearing cookies or switching browsers would, however, enable targeted advertising again until the opt-out form had been filled out a second time.

Beyond solutions like Phorm, network-based targeted advertising can also be realised via the set-top box and as ad injection. This allows Web-community–type features to enter the DTV platform (aggregate popularity ratings) and cross-platform promotions, as well as better targeted advertising. The STB interface can, for example, be used to display ads interactively, such as to promote VoD offerings based on TV-watching habits ("you have watched 10 documentaries about wildlife in Africa, would you like to download a documentary about lions?"). The set-top box approach works on the basis of capturing data related to "zapping" behaviour and TV programmes watched.

KEY LESSONS

Six key lessons emerge from the discussion:

- Targeted advertising is clearly on the rise, supported by a set of central factors: Broadband as a mass market phenomenon, proliferation of highly advanced Internet monitoring technologies, and the general need for new business models of Internet players and network providers to monetise new Web 2.0 services and platforms.

- Targeted advertising will be key for Internet providers as well as network providers to finance next-generation services and innovation in particular to monetise many Web 2.0 services and applications—it can be a value-add for the consumer, if done properly (e.g., Gmail).

- Due to the rich data being generated as part of their very purpose, social networking sites strongly push into targeted advertising; network providers have only started to consider these opportunities.

- Early moves into targeted advertising based on technologies like DPI have experienced high visibility in the public and the media as well as raised strong privacy concerns and pushback in many cases.

- Achieving general user acceptance will transcend mere legal compliance with data privacy rules. Transparency to the user base about intended targeted advertising rollouts is key. Also crucial will be to clearly articulate the value-add targeted advertising will have for the consumer, that is, to convince users of "what's in it for them."

- With regard to actual implementation by network operators, it has already become clear that non-transparent practices may lead to regulated opt-in obligations. Easy-to-use opt-out tools with transparent communication to users may, however, find acceptance, particularly when coupled with a genuinely (free?) value-add service, as shown in the Gmail case.

CASE 5: BLOCKING CHILD SEXUAL ABUSE CONTENT

***Problem:** Block the access to websites showing child sexual abuse content (several thousand websites).*

***Risk:** Low real risk to unintentionally access a child sexual abuse content site, but these sites can be found if looked for; severe impact on life of victims.*

Child sexual abuse content is legally prohibited in most countries of the world (with a difference only in the definition of "child" or "minors" ranging between 14 and 18 in most countries). But still, thousands of sites on the Internet offer these types of content.

Countering child sexual abuse content emphasizes the prosecution of persons responsible for the actual existence of child sexual abuse content: Users/customers of child sexual abuse content material on the one hand and suppliers of such material on the other hand. The prosecution of contributing individuals or businesses is a task solely for law enforcement, which may demand assistance from other stakeholders (e.g., network providers) as deemed necessary and as applicable law allows. Governments are in fact increasing their activities in this area: Just recently, in May 2008, the U.S. Senate approved $1 billion over the next 8 years to broadly fight child sexual abuse content.

*In the United States, more than 1,500 individuals are arrested each year for the possession of Internet-related child sexual abuse content. The majority of them own several hundred pictures showing children between 6 and 12 years old.**

**National Centre for Missing & Exploited Children*

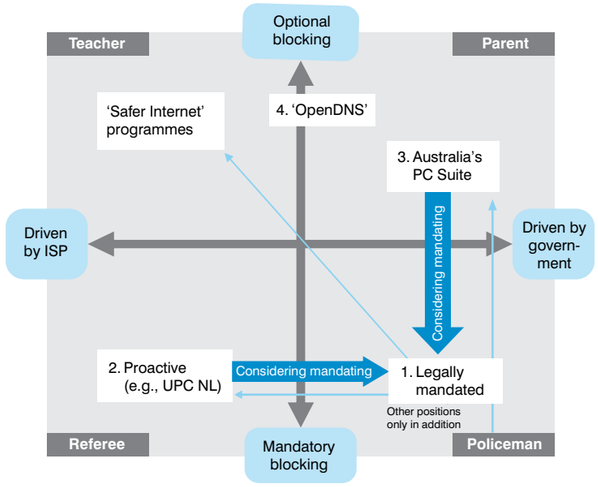
On the other hand, making sure that Internet users are not exposed to child sexual abuse content accidentally is a task that can be mainly performed by network providers. But this is also more difficult than first appears, since it is multi-faceted and truly controversial: Blocking makes the responsible institution subject to censorship criticism and liability claims, and waterproof blocking is difficult technically as the various techniques available for blocking can all be circumvented.

Current legislation does not cover all new Internet-related issues associated with sexual abuse content.

One problem is that child sexual abuse content needs to be defined in order to be criminalised and blocked: The border between pornography and art has sometimes proven to be blurry. Also, definition criteria need to be enforceable: Whether a young person being shown in a pornographic context should be protected or not (i.e., in most countries the question of being above or under a certain age) is difficult or impossible to determine. Furthermore, images created and modified with image manipulation software pose a different (legal) issue that was not relevant when most laws were created.

Approaches to blocking child sexual abuse content can be discussed along an adapted version of the Digital Confidence Positioning Framework, with the vertical axis differentiating whether the blocking is optional

Exhibit 47: *Digital Confidence positioning—child pornography blocking*



1. Standard Internet Service Providers (ISP) positioning normally is to block legally mandated content only
   - Pro: Basic protection given
   - Con: No additional protection possible
2. Proactive ISPs initiate filtering programmes without being legally obliged to
   - Pro: Prevent unintentional/accidental access
   - Con: Slippery slope into censorship should blacklists be extended beyond original objectives by third parties
3. Australia's government developed a PC-based solution for parents
   - Pro: Empower users to protect themselves
   - Con: Needs expertise to install and configure; costly but not hacker-proof
4. "OpenDNS" type solutions are industry-driven and empower users to choose the categories to be blocked
   - Pro: ISP not liable for selected content
   - Con: No uniform level of protection–dependent on individual action and preferences

(i.e., at consumer discretion), self-imposed (i.e., determined by the network operator), or mandatory, and the horizontal axis differentiating whether network operators or the regulator are the driving force behind such activity.

So far, the predominant approach beyond complying to legally required blocking of sites is self-imposed filtering of child sexual abuse content based on independent, third-party established, maintained, and verified lists of legally banned content. ISPs are generally hesitant to filter, principally because, as "mere conduit" operators, is it not their role to interfere with Internet freedoms. Moreover, they want to avoid legal liabilities in case legal content would get blocked unintentionally. Should filtering be implemented, voluntarily or upon threat of mandate, independent judicial controls are required with regard to establishing that the content to be filtered is indeed illegal under the relevant jurisdictions.

A prominent example of an ISP proactively taking initiative is the case of UPC Netherlands' child sexual abuse content filtering initiative of early 2007. UPC cooperates with the Dutch Justice ministry and the Dutch Police who blacklist over 3,000 websites containing child sexual abuse content and complicate access to these pages by showing a landing page that reads "you are trying to access a blacklisted website." Several thousand times a month, accidental access to child sexual abuse content sites was prevented with this solution.

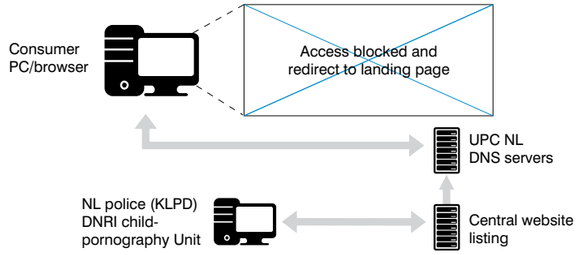
Tech-savvy users (even children) can easily circumvent most PC-based filters.

The public reaction on this implementation was very positive. In a dedicated poll, 95 percent of consumers said they were in favour of blacklisting child sexual abuse content, with 94 percent in favour of network operators filtering websites of undesirable content in general. The latter number seems very high, but may be influenced by the fact that the question has been asked in the context of child sexual abuse content rather than a neutral debate. Besides, the majority (63 percent) of the press coverage reported on the filtering activity was positive. Despite this, concerns were raised in the Dutch parliament about the effectiveness of DNS filtering and the fact that not all ISPs implemented filters. Parliament called on the government to investigate the feasibility of mandating (potentially more intrusive forms of) filtering on Dutch ISPs.

The big advantage of voluntary, ISP-led initiatives is that they can provide extended protection if strong institutions join forces to make up for law-making being either slow or not knowledgeable enough. The problem from the network provider and ISP perspective is that they make themselves vulnerable to requests to broaden filtering into other areas of content—a "slippery slope" into censorship and liability issues. Examples to illustrate this: In July 2007, the Swedish police intended to extend a child sexual abuse list to include the world's largest BitTorrent tracker, ThePirateBay. In Denmark, a court ordered extensions of a DNS-based child sexual abuse list to include popular music download sites (the Russian AllofMP3.com and ThePirateBay once again), provoking the spread of information regarding circumvention methods that undermined the effectiveness of the original filter.

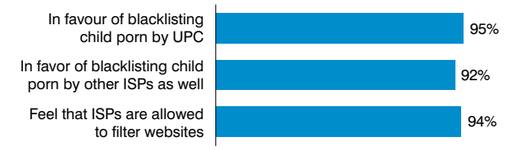
Another approach has been observed in Australia: Since 2007, the Australian government has contemplated a two-pronged approach whereby, on the one hand, ISPs would eventually be obliged to filter. So far, this part of the project is bogged down after a number of unsuccessful field trials where filtering solutions appeared not to be scalable to big ISPs. Moreover, there is great political controversy around the type and quality of content to be featured in the blacklist, administered by the Australian Communications and Media Authority (ACMA).

Exhibit 48: *Child pornography blocking—technical implementation*



Note: Technical solution simplified
Source: UPC

Exhibit 49: *Child pornography blocking—public opinion*



Source: NSS Interviews (n = 600)

On the other hand, the government developed NetAlert, a programme labelled "Protecting Australian Families Online," which included blocking of child sexual abuse content. This is a PC-based solution to filter content, comparable to multiple commercial solutions. This approach does put consumer choice and responsibility in the centre, but it also requires certain initiative and expertise from consumers to make it work. Since many users are not extremely tech-savvy, this solution is difficult to deploy (only a few hundred installations have been completed after the initial rollout) and for more experienced users easy to circumvent. Adding insult to injury, a teenager was reported to have circumvented this 84 million AU$ filter within 30 minutes.

As the Australian examples shows, no filtering methodology provides a 100 percent solution against deliberate circumvention. Moreover, a crucial role, in all instances of filtering, is played by the quality of the lists of illegal content, that is, the way in which they are governed, maintained/updated, and enforced. The speed by which listed illegal content is actually being removed is another issue. Reportedly, under "notice and takedown" schemes, child abuse sites remained online for an average of 30 days after being first reported. The challenge for national hotlines is getting international law enforcement (through Interpol or Eurojust) to take action rapidly to have content removed by hosting providers when hotlines have notified them of illegal content in their jurisdictions. According to the UK Internet Watch Foundation, two percent of commercial child sexual abuse sites worldwide were still active a year after being identified.

Lack of a 100 percent solution, differing quality of listing processes, and different enforcement standards are all factors to be taken into account when assessing the proportionality of mandated ISP filtering.

Last, a solution for blocking child sexual abuse content can rely entirely on empowering the consumer. A showcase example for this approach is the OpenDNS implementation[6]. OpenDNS is a free DNS server that allows users to choose categories of sites to be blocked in a Web interface. The DNS server then redirects the user to a landing page if blocked content is tried to be accessed. Empowering the consumer himself brings about big benefits: Consumers are free to choose what they see or block (beyond what is legally mandated, naturally); thereby, censorship and liability discussions vanish. Furthermore, a simple, network-based solution minimises the needed knowledge of users and is readily available for the "standard consumer." For a DNS server-based solution, very little configuration is necessary compared to using proxy servers or desktop-based systems. To achieve the desired results, though, consumers need to be educated and empowered with appropriate, easy-to-use tools, and the registers of content to be blocked need to be managed appropriately, ideally on the industry level.

Filtering to fight child sexual abuse content can be a slippery slope into censorship for ISPs and network providers.

(6)Note: OpenDNS can be found at http://www.opendns.com. We are referring to OpenDNS several times in this document as an example since it is a free solution that can be tested by all readers of the document

Existing Child Pornography Blacklists and NGO Cooperation

In the UK, ISPs have introduced URL-based filtering that is currently available to 96 percent of residential broadband customers. The URL list is provided by the UK Internet Watch Foundation (IWF) and contains several thousand URLs as well as an average of 250 to 300 domain names of commercial websites offering for sale images and videos of children being sexually abused. Six people work in the IWF Hotline processing reports, assessing and tracing content, and maintaining the IWF URL list. The IWF updates the list twice daily and requires its member ISPs to update their filters correspondingly, at least once every 24 hours. IWF shares its list with hotlines abroad (so far with the Danish, Australian, and Korean hotlines) based on an agreement that the list is re-assessed legally to ensure compliance under the respective jurisdictions.

In the United States, Verizon, Sprint, Time Warner Cable, AT&T, and AOL agreed in June/July 2008 to shut down access to websites and newsgroups that traffic in children sexual abuse images. The companies are requested to check against a registry of explicit sites maintained by the Centre for Missing and Exploited Children. The ambition with the agreement is to make it extremely difficult to find or disseminate the material online, whilst it is recognized that it cannot eliminate access entirely, as some third-party companies sell paid subscriptions, allowing customers to access newsgroups privately and preventing even their ISPs from tracking their activity. A library of some 11,400 illegal images was established allowing investigators to filter through tens of thousands of online files at a time. The system is based on using images with unique "hash values"—a kind of digital fingerprint—for identifying illegal images that could then be used to search for the same image anywhere else it appeared on the Web.

www.nystopchildporn.com, an initiative from New York State Attorney General Andrew Cuomo, provides details on which ISPs have signed agreements to eradicate access to child porn through their servers.

KEY LESSONS

Six key lessons emerge from the discussion:

- Blocking child sexual abuse content is commonly perceived as morally justified and therefore desirable—opinions on blocking other "undesired" content (e.g., racist and "bomb-making" websites) are not that unanimous, especially from a freedom-of-speech perspective.

- Flawless execution is challenging, both technically and in terms of meeting "burden-of-proof" requirements, that is, determining whether a young person shown in pornographic action is actually a child or what pornography actually is.

- Extending blacklists to other content like illegal music sites, that are popular and far from commonly denounced like child sexual abuse content, tends to backfire as it spurs the circulation of information on how to circumvent filters.

- Flawless execution is challenging both technically and legally, as legislation differs with regard to what constitutes illegal child sexual abuse content. International treaties to create common legal bases—like the 2007 Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse—have not been implemented in all member states.

- A concerted international law enforcement approach is called for to speed up the actual takedown of blacklisted sites.

- Expectations regarding filtering effectiveness need to be managed. No filter is 100 percent effective in providing a solution. Network-based filtering is merely instrumental in preventing accidental access to child sexual abuse content. This is an important trade-off against the proportionality of legally obliged filtering.

- Engaging in child sexual abuse content blocking consequently opens up strong controversies around censorship fears, liabilities, and cross-national differences.

- There are two main emerging remedies for network operators and ISPs:

– In those countries where there is no adequate, independent listing process: Empower the consumer to help himself (i.e., broadly nurture Open DNS-type solutions) and educate the consumer about the functionalities and the power of such solutions.

– In countries with established third-party listing support: Industry needs to decide on the level of filtering to apply voluntarily. To start with the least-intrusive form of intervention, a first step could be DNS-based filtering or a move to the next level of URL-based filtering only if adequate and legally verified lists exist.

- To avoid filtering extensions beyond the original objective of fighting child sexual abuse content, listing institutions should ideally be established as independent from judicial authorities like the police. The UK Internet Watch Foundation is a good example of this type of organisation.

CASE 6: SOCIAL NETWORKING/ INTERNET EDUCATION

Problem: ***Children and youths are not aware of the risks of online interaction (e.g., in social networks): Solicitation, grooming, etc.***
Risk: ***Due to the high anonymity made possible by the Internet, the risk is higher than in real life (most children know not to talk to strangers on the street; but who is a stranger on the Internet?).***

Beyond blocking child sexual abuse content (and possibly more harmful and undesired content), there is a second crucial lever for protecting minors: Educating them about the Internet's opportunities and threats so that minors can contribute to their protection themselves.

Internet stakeholders have diverse education measures for children and parents.

Internet-enabled social interaction, in parallel to its rapid growth, has triggered issues that had been largely unknown previously: Bullying, grooming, and solicitation as well as careless data

publishing.

Asking unprepared parents and schools to help may be asking too much of these "typical education protagonists." The more they struggle with covering digital life, two things need to happen:

1. Parents and schools need to be empowered (or empower themselves) in order to live up to the education expectations invested in them.

2. Other institutions—ISPs, network operators, and Internet businesses such as social networking platforms—need to be added to the overall education effort.

Approaches to such education can be discussed along an adapted version of the Digital Confidence Positioning Framework (Exhibit 50). The vertical axis differentiates the degree of activity, thereby making the lower half theoretical, as "no education" is not a viable option. The horizontal axis differentiates the individual discretion in such education, that is, whether approaches make education an optional offering or an obligatory duty.

Social networking requires a new level of user education—all players need to realize its importance and provide effective solutions.

First, social networking sites exhibit a clear dedication towards user education, as shown by the examples of Bebo, MySpace, and Facebook. They tend to be similar in taking a moderate position on the mandatory-optional dimension, but they differ quite notably in how proactive they are.

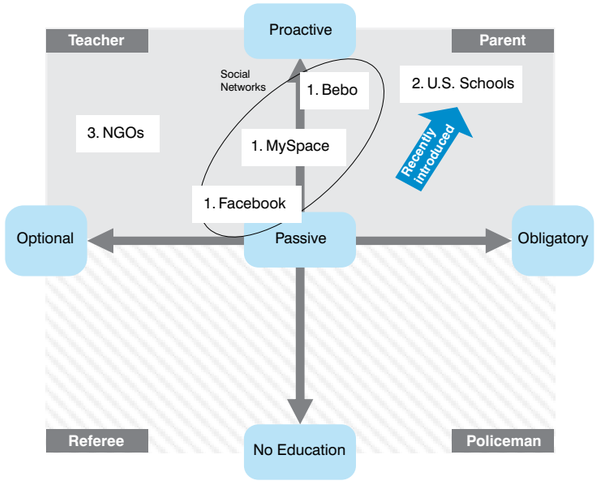
Bebo is a strongly minors-oriented offering and consequently takes a clearly proactive approach towards user education. For example, it offers an educational video focused on the dangers of social networking that uses a comic, entertaining, and intuitive style specifically targeted at children. In addition, Bebo offers written educational materials for teachers and parents; it cooperates with a number of NGOs in the development of such materials.

Facebook takes a more low-key approach to user education, presumably as its target groups consist of more experienced and older users. It offers an explanatory text about five safety tips and FAQs for users, but also for parents specifically, mainly focused on complaint processes.

Second, U.S. schools have recently started special classes about Internet and social network education. Virginia has already made Internet safety lessons mandatory in high schools.

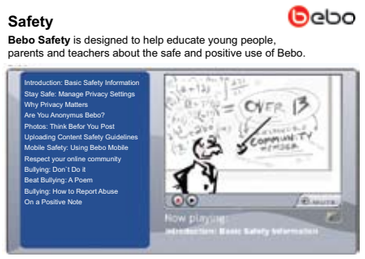
The focus is on risks in social networks, especially harassment and solicitation. Classes are run based on material developed by the NGO Web Wise Kids.

Exhibit 50: *Digital/Internet education confidence positioning—social networking*



1. Social networking sites educate their users about the threats and dangers of sharing personal data
   - Bebo is very conscious of threat to minors, with very restrictive settings as default
   - MySpace and Facebook less minors-focused and restrictive
2. U.S. schools start special classes about Internet and social network education
   - Focus on risks in social networks (harassment, solicitation)
   - In the state of Virginia, this is a mandatory class
   - Supported by nongovernmental organisations (NGOs), developing material, (e.g., Web Wise Kids)
3. NGOs, such as ConnectSafely, working to educate children, parents and teachers about the Internet

Exhibit 51: *Bebo social network education*



- Video targeting children and focused on the dangers of social networking (comic style videos)
- Written educational materials for teachers and parents
- Cooperation with several NGOs to develop educational materials

Third, a broad range of NGOs engage in Internet and social networking education, many of them with a clear focus on minors.

Reflecting the omnipresent trend towards social networking on the Internet, the very topic of safety in Internet socialising has its own Web 2.0 offering: ConnectSafely is a forum with the sole purpose "to discuss safe socialising on the fixed and mobile Web."

Web Wise Kids is a large, U.S.-based NGO that engages broadly with Internet safety issues. It has developed several digital games targeted at children to educate them about general behaviour best practices and issues covering online solicitation, predatory attacks, and illegal downloading. It also supports schools by providing "offline" classroom material and addresses the diverse stakeholders individually on its homepage, from parents to teachers to law enforcement and minors themselves.

Parents expect schools to be primarily responsible for Internet education.

In Europe, Insafe is a network of national nodes that coordinate Internet safety awareness. An exemplary activity is the family e-safety kit, published in European countries in early 2008. It discusses key e-safety themes in a design suitable for joint reading with children.

Despite these positive examples, there is still a long way to go in catching up with the rapid growth in minors' Internet and social networking usage. As shown, there already are many good initiatives. But there is room for greater concerted action bringing various stakeholders together to share lessons learnt, best practices, and proven education formats—resulting in limited leverage of the funds invested overall.

Especially, introduction into formal educational systems is just beginning. Surveys indicate that parents see schools as the primary source for getting informed about safety on the Internet. Interestingly, "ISP or the telephone company" follows a close second. Although only 7 percent mentioned software companies, the potential integration of educational measures in the primary user interface (i.e., the operating systems and browsers) would be a logical step to reach more users in an interactive manner.

KEY LESSONS

Six key lessons emerge from the discussion:

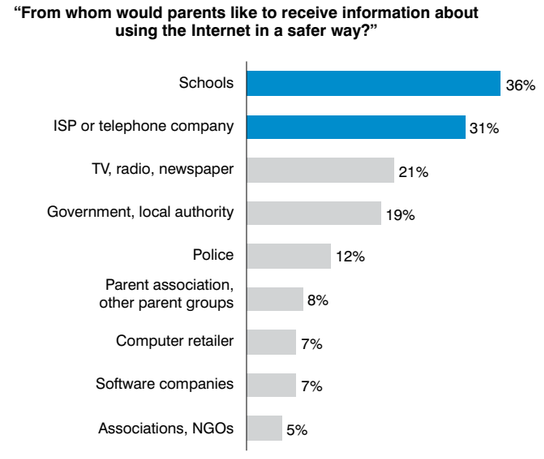
- Educating minors about the opportunities and threats of the Internet in general and particularly of social networking is getting more and more important.

- Social networks try to educate their users, but on a voluntary basis, at their own discretion—society therefore needs to watch and complement social networks' activities.

- Parents expect schools and ISPs to play an important role in education—it is a valuable opportunity for both to accept this role even more by intensifying activities they have already begun.

- NGOs have already developed broad activities in the field—these activities should be

Exhibit 52: *Parents information channel (UK, 2006)*



Source: Eurobarometer

consolidated in the near future to join forces and to intensify larger-scale cooperation, especially with schools.

- ISPs teaming up with NGOs can be a very useful combination to reach large audiences with education in an online and offline manner.

- All education needs to target the specific (age) groups on the Internet. For example, "born digitals" in their adolescence hardly need technological education but need to learn the potentially negative consequences of sharing data and sharing personal profiles online inappropriately; younger children need simple advice in an interactive manner; and parents should learn about the actual online behaviour of their children and need to be able to spot symptoms of exposure to potential dangers like grooming or solicitation in an early stage.

CASE 7: COPYRIGHTED CONTENT FILTERING

***Problem:** Pirated audio and video content is distributed massively on the Internet, and the content industry is severely challenged to find digital businesses models.*
***Risk:** Network operators are forced to restrict access to content offers, potentially not in accordance with current laws and limiting the user experience of the Internet.*

The proliferation of file sharing protocols and platforms, in combination with increased broadband speeds available to end users, has made the fight against online piracy one of the biggest current challenges for audiovisual rights holders and regulators.

Lately, the focus in regulatory policy on fighting piracy has turned on network providers and ISPs, whereby pressure is increasing on them to adopt a more pro-active role. Measures being contemplated to be deployed range from technological solutions (e.g., deep packet inspection and various forms of network-based filtering, digital fingerprinting by hosting providers up to watermarking by content providers) to non-technological measures (such as forwarding notices to customers who have been identified as infringers); see Case 8.

*"An Internet provider voluntarily giving up copyright immunity is like an astronaut on the moon taking off his space suit."**

**Tim Wu, Law Professor, Columbia University*

Under EU rules, network operators and ISPs, as "mere conduit" providers, are exempt from any general obligation to monitor traffic over their networks. They only have to engage in taking down illegal content that they host themselves after they have been notified to do so. They are generally opposed to engage in "active" Internet filtering to combat copyright infringement. The reason for this is that most technological filters are either overblocking—exposing network operators and ISPs to legal liabilities when legal content is blocked as collateral damage, or when limiting legitimate uses, which are exempted under copyright legislation and freedom of information—or underblocking, because copyright infringers and new technologies will always find ways around. Finding a voluntary, or even a regulatory, solution is therefore a challenge. It can be quite difficult (or even impossible) for a network operator or ISP to distinguish a legal offer from an illegal one, if both use exactly the same file. There cannot be a technological one-size-fits-all and a 100 percent effective approach.

Moreover, as opposed to the debate on child sexual abuse content filtering, there is no overarching political or public support for tolerating potentially overblocking measures that risk restricting basic Internet freedoms for the purposes of safeguarding commercial interests (however legitimate) of a particular stakeholder. When in January 2008 AT&T announced its intention to proactively monitor all the traffic it carried for potential violations of U.S. intellectual property laws, it triggered significant consumer backlash, alleging "Big Brother" type practices. Also, the fact that AT&T would voluntarily risk losing its immunity from copyright liability when taking an active role in selecting which content could travel over its networks was widely criticised.

Mandatory filtering of copyright protected content is therefore often imposed only by the courts—on a case-by-case basis.

In an adapted version of the generic Digital Confidence Positioning Framework, filtering can be seen as one form of reaction to illicit file sharing, which can be identified along two dimensions (Exhibit 53). The vertical axis differentiates what is actually done to combat illegal file sharing, ranging from ensuring that users do not engage in illegal activity to blocking illegal activity by filtering. The horizontal axis presents non-technical measures aimed to discipline user behaviour to deploying technical measures against illegal file sharers or downloaders. Filtering here falls into the Referee role when, for example, an individual ISP is mandated by a court to block access to a particular P2P site, or a Policeman role when a whole ISP sector is mandated to install filters by legislation.

ThePirateBay (TPB) has been a central "apple of discord" in this field over recent years. It is one of the most well-known and largest BitTorrent tracker and torrent search sites. TPB has a reputation of distributing a lot of copyright-protected (i.e., pirated) content like movies. Several ISPs, for example, the Danish Tele 2, were forced to block TPB recently, as discussed in Exhibit 54. This forced blocking has two major problems: Technical feasibility and legal backing. On the technical side, DNS rerouting can be used to restrict access to TPB—but users will find ways to get around this, or, as in the case of Denmark, TPB will just add another domain name pointing to the site. Alternatively, TPB could be blackholed—but this is a very "extreme" measure as, for example, all services at the same IP address would be cut off (and it would still be possible to circumvent this block).

In March 2008, the press reported that four music majors were suing Irish incumbent ISP Eircom to stop Internet users from illegally downloading music, the first case in the country whereby an ISP was alleged to be liable for the actions of its customers, instead of individual illegal downloaders being prosecuted. It comes after a ruling in a Belgian case of June 2007 in which Scarlet, one of Belgium's leading ISPs, was ordered to install a filtering solution within 6 months. The decision had fuelled an intense discussion whether network operators can be obliged to filter traffic.

Finally, combating piracy using high-tech filtering technologies, as part of network operators' network management toolbox, recently became a focal point in the U.S. net neutrality debate. Rights holders like MPAA and NBC have called for network operators to adopt a proactive role by using bandwidth management tools to prevent the transfer of pirated content. They argue that net neutrality must promote the protection of intellectual property and not prevent the development of new filtering technologies and identification technologies to detect copyright-infringing content. On the other side, consumer advocacy groups likened this practice to censorship.

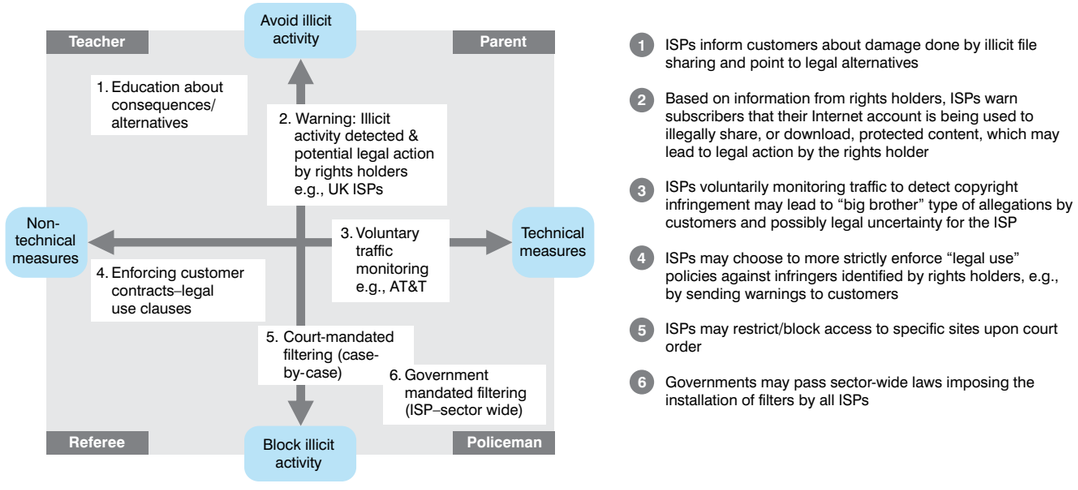
KEY LESSONS

A number of key lessons emerge from the discussion:

- ISPs are generally very hesitant to engage pro-actively in filtering Internet traffic to combat piracy. Inherently, an active role implies that ISPs intervene in traffic flows over their network, thereby undermining their "mere conduit" status that ensures their immunity for copyright liability and exposing them to significant legal claims.

- Content filtering is both technically and legally difficult to implement. It will most likely result in either over- or underblocking of copyright-infringing content and infringement of fair use. As opposed to the child sexual abuse content filtering, there are, to our knowledge, no dedicated independent third parties that provide, review, and update illegal P2P blacklists.

Exhibit 53: *Digital Confidence positioning—copyrighted content filtering*



Moreover, automated network filtering technologies based on, for example, fingerprinting may be able to red-flag protected content but cannot make reliable judgements as to whether that content is actually used illegally or if it falls under legitimate use exemptions. In addition, the fundamental question has to be addressed whether it is the network operators' responsibility to protect copyrighted content. The cost incurred to do so will then translate into higher prices for its own offerings.

- In the few instances where network operators announced intentions to proactively monitor Internet traffic, they faced significant consumer privacy criticism because of the intrusive nature of network-based filtering technologies (e.g., deep packet inspection or other forms of filtering). Companies risk putting themselves at a competitive disadvantage vis-à-vis other operators that do not filter this way.

- As opposed to the child sexual abuse content debate, filtering content to protect pure commercial interests of one particular stakeholder whilst limiting basic Internet freedoms does not carry broad support at a political level or from the public at large.

- Network-based filtering has been criticised as infringing net neutrality principles by discriminating between different sorts of Internet traffic and services. These technologies would limit legitimate use and lawful expression, stifle innovation, and threaten personal privacy whilst not addressing the underlying problem. At the same time, rights holders call for net neutrality to promote protection of intellectual property and to allow filtering and content identification technologies to develop into maturity.

- Consumer education also plays an important role, but has its limits since most users are already aware of what they are doing.

CASE 8: ADOPTION OF "THREE STRIKES"

Problem: In the attempt to fight piracy, the entertainment industry wants to introduce a "three strikes" rule—consumers infringing copyrights get disconnected from the Internet after the third offense.

Risk: Implementing a "three strikes" rule potentially disconnects several hundred thousand consumers from the Internet, severely inhibiting those individuals' personal rights and the growth of the digital economy.

As opposed to technological solutions to combat digital copyright violation, there is a range of non-technical mitigation measures at network operator and ISP levels being actively debated in the EU, the United States, and Japan. The most high-profile of these measures is the so-called "three strikes and you're out" rule, which has been actively campaigned for by rights holders across the three continents: It is the idea of actually banning persistent illegal downloaders from the Internet—and having such a rule as a major deterrent so that users do not engage in copyright violation in the first place.

Compared to targeted blocking of services like ThePirateBay that mainly enable (arguably illegal) file sharing or compared to filtering out copyrighted content, there is a high risk of overshooting the objective in actually banning individual users from the Internet completely "only" because of copyright violation. It is very debatable whether the business interests of one particular industry should be a reason to completely cut off individuals from digital life. Moreover, it is questionable whether network operators have the right to play such a role. Depriving someone of Internet access is a serious penalty and should perhaps only be levied once due process through legal safeguards has been exhausted. If network operators, as private actors, decide to cut someone off based on the evidence of rights holders, they act as judge and jury. Says Carphone Warehouse CEO Charles Dunstone: "Our position is very clear. We are the conduit that gives users access to the Internet. We do not control the Internet, nor do we control what our users do on the Internet. I cannot foresee any circumstances in which we would voluntarily disconnect a customer's account on the basis of a third party alleging a wrongdoing."

The "three strikes and you're out" rule is embedded in a number of possible reactions to the detection of illicit file sharing, as shown in Exhibit 54 and described in Case 7. The Teacher approach to detection of illicit file sharing would be just to inform the user of the damage done by illegal downloading or file sharing of copyright-protected content without permission, and to point out alternatives for legal content offers. Moving up one level of intervention, the Parent approach would entail that the network operator proactively warn individual subscribers on the basis of information from rights holders that a computer linked to the individual's Internet account is being used to download or share protected content. It is explained that this activity amounts to copyright infringement, which could lead to legal action by the rights holder. Under this approach, the network provider could also suggest security software solutions to prevent illegal downloads from the individual user's account going forward. This way, network operators can minimise liability and help the consumer understand that she or he is not 100 percent anonymous on the Internet.

This approach is currently being implemented by the six leading ISPs in the UK. First trialled by Virgin Media and the British Phonographic Industry (BPI) to see the effect of warning letters, in July 2008 this led to a co-regulatory solution based on a Memorandum of Understanding and facilitated by the regulator OFCOM. This MoU aims to provide an agreed industry framework for action to combat illicit use of P2P technology only—not the issue of commercial piracy. It is signed by the BPI and MPAA representing the content industry; by Virgin Media, BSkyB, BT, Orange, Tiscali, and Carphone Warehouse for the ISPs; and by three relevant government departments. The ISP signatories agree to put in place a 3-month trial to send notifications to, initially, 1,000 subscribers per week identified for them by music rights holders. In addition, they will draw up a Code of Practice—requiring the approval of OFCOM—on standards of evidence; actions against alleged infringers and against repeat or criminal infringers; indemnity resulting from incorrect allegations of file sharing; and routes of appeal for consumers. So far, the UK ISPs have stopped short of threatening subscribers with disconnection. Their warning letters will, however, be accompanied by a written warning from the BPI, which will threaten both disconnection and a court appearance for those who continue to download illegally. Remedies to deal with repeat infringers who appear insensitive to the warning letters are still up for debate. Solutions to be discussed include technical measures such as traffic management or filtering, and marking of content to facilitate its identification.

*Guy Bono, Member of the European Parliament: "On this subject, I am firmly opposed to the position of some Member States, whose repressive measures are dictated by industries that have been unable to change their business model to face necessities imposed by the information society. The cut of Internet access is a disproportionate measure regarding the objectives. It is a sanction with powerful effects, which could have profound repercussions in a society where access to the Internet is an imperative right for social inclusion."**

The third approach, filtering of specific copyright infringing content or file sharing sites, has been discussed in more detail in the previous case.

The most interventionist approach, disconnection, is currently being discussed and actually already introduced in some countries as a "three strikes and you're out" policy. Specifically, the following has been discussed (for example, in France, where the proposal came to be known as the "Olivennes Agreement," so named for Denis Olivennes, CEO of the major French media retailer FNAC and chair of the

**http://www.cablefo-rum.co.uk/article/397/european-parliament-rejects-3-strikes-rule-is-vm-listening*

Exhibit 54: *The Pirate Bay—recent activities*

The Pirate Bay

- 1 million torrents
- 12 million peers (simultaneous active connections)
- 2.5 million registered site users

- May 2006: Police Raid against The Pirate Bay (TPB)
  - Servers and other equipment confiscated
  - Founders questioned by the policed but not charged
  - Allegedly Motion Picture Association of America (MPAA) was driving force of the raid
  - In June 2006 TBP was online again
- July 2007: Sweden wants to put TPB on child pornography blacklist
  - Would have blocked access from Sweden
  - Decision revoked-child pornography reproaches never proven
- September 2007: MediaDefener-leaked e-mails show entertainment companies hired hackers for DoS attacks against TPB
- January 2008: TPB operators charged with "promoting other people's infringements of copyright laws"
- February 2008: Danish Tele2 ordered to cut off customers from TPB
  - IFPI claims Tele2 violates copyright with granting access to TPB
  - Order appealed-violates EU law according to Tele2, since copying in routers is explicitly allowed in the EU Infosec Directive (Article 5.1)
  - Traffic from Denmark to TPB increased by 12% based on public discussion
- March 2008: Swedish ISPs sued by IFPI to block TPB access
  - TeliaSonera refuses since they are not allows to wiretap customers
  - Telia feels not responsible for actions of its customers
- April 2008: TPB sues IFPI for compensation for traffic blocked by Tele2 DK

Sources: News Article, ThePirateBay, Wikipedia

Anti-Piracy Commission that drafted the agreement and presented it to French President Sarkozy): ISPs must send warnings and implement sanctions as required by the newly established anti-piracy authority HADOPI, which assesses infringement notifications from rights holders and instructs ISPs to act accordingly. ISPs would need to send two warnings to alleged offenders, the first by e-mail. In case of no response and continued infringement, a second warning would be sent 1 week later by recorded delivery letter. If there is still no response and illegal activity continues, the account would be suspended for 15 days. Should there still be no reaction and infringement continues after the service is resumed, the account will be suspended for (up to) 1 year.

*"Britain's six leading Internet providers have signed a Government-led agreement to stamp out illegal music file sharing. The six providers—BT, Virgin Media, Orange, Tiscali, Sky, and Carphone Warehouse—will implement a series of measures against those found to be file sharing. The ISPs are reportedly reluctant to impose the BPI's preferred 'three strikes and you're out' approach of cutting off users' broadband connections."**

Generally speaking, significant confusion still exists as to how exactly "three strikes" needs to be implemented, for example, differing views on the duration of disconnecting users, the unclear monitoring process (France is discussing a statewide register for offenders), responsibility discussions varying across countries (especially if network operators and ISPs have to detect all infringements or if they only have to react at copyright owner request), liability issues (in case of false claims regarding alleged infringers), and finally who is to pay for such implementations.

Countries take varying positions on the "three strikes" idea. France seems to be most advanced in formulating the approach in the form of a bill to be discussed in parliament in Autumn 2008. In France, cooperation of major ISPs has been secured for a "deal" ensuring in exchange that, among others, music will be offered DRM-free for legal download. The UK appeared to be following the French lead and was actively contemplating the idea, in early 2008, should ISPs and rights holders not come to an agreement. With the aforementioned MoU, however, disconnecting repeat infringers has not been included as one of the remedies to be discussed among the signatory parties. The approach in the UK is also coupled with a commitment by the signatory parties to make available more attractive commercial content offers (e.g., subscription, on-demand, legal sharing) as alternatives to unlawful file sharing. In Japan, the four major ISP associations have agreed on implementing "three strikes" in reaction to pressure from government and the content industry. In April 2008, the European Parliament rejected the "three strikes" approach when it voted on a report about promoting European cultural industries.

Finally, "three strikes" features as one of the possible technological mandates for ISPs that are being discussed in the context of the G8's Anti-Counterfeiting Trade Agreement (ACTA), which the G8 aims to finalise before the end of 2008. ACTA is in large part about updating legal frameworks to take account of P2P and developments on the Internet. Although these negotiations are taking place behind closed doors, leaked information on proposals being discussed shows that "three strikes" and also mandatory ISP filtering are on the agenda.

One aspect often overlooked in public discussions on the merits of "three strikes" is the damage to the overall digital economy as the result of disconnecting significant numbers of users from the Internet. Implications of "three strikes" would need to be understood more holistically. A high-level sensitivity calculation, for the UK as an example, estimates "three strikes" to result in the disconnection of 500,000 users and a revenue loss of €180 million for the network operators (Exhibit 56). In comparison, the music industry assesses an upside of only €33 million in revenue—this total revenue loss of about €150 million is likely to be only a minor share of the downside for other stakeholders, for example, through the reduction of e-Commerce volume.

In addition to the fact that users would be disconnected from digital life, the potential economic damage caused across the digital economy value chain makes "three strikes" a challenging concept in terms of finding a proportional remedy to combat piracy.

KEY LESSONS

Four key lessons emerge from the discussion:

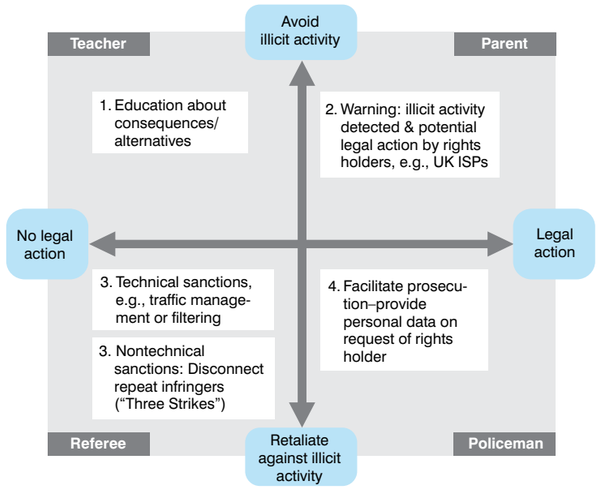
- With the "three strikes" regime, mitigation of copyright violations is being taken to the next level of interventionism, with a substantial danger of "overshooting" if the implications are not weighed in a balanced manner.

- It is very doubtful that the business interests of one particular industry should be a reason to completely cut off individuals from digital life—especially in light of the implementation and opportunity costs involved for other stakeholders in the digital economy.

- The public debate around "three strikes" has concentrated on the appropriateness of the regime itself—prerequisites, especially the difficulties around correctly detecting copyright infringement, and implications in a broader sense have not been addressed enough.

*BBC News, 24th July 2008

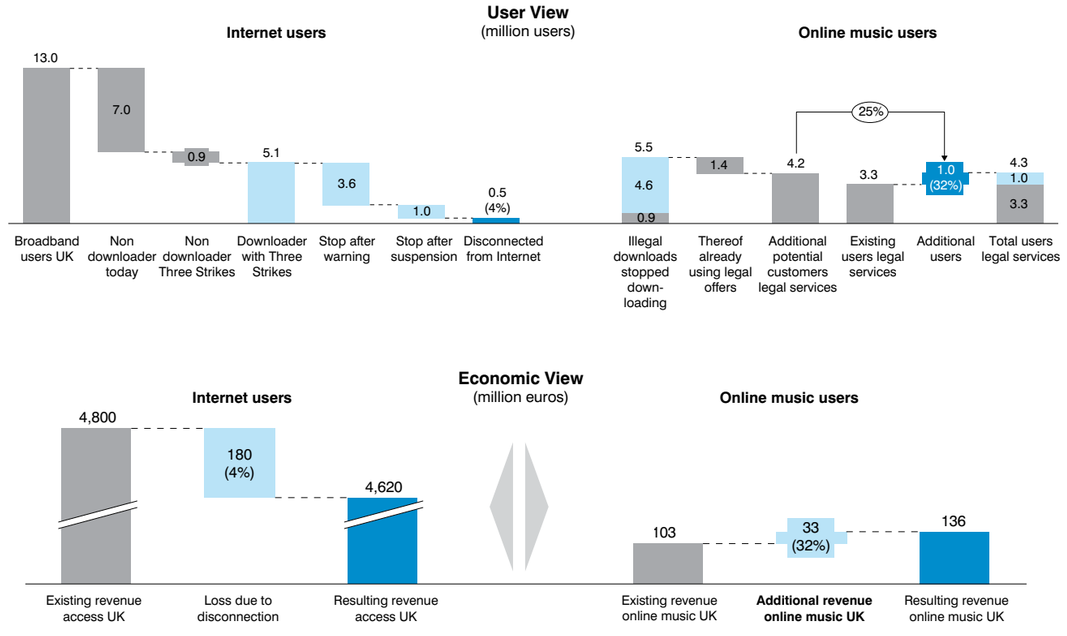
Exhibit 55: *Digital Confidence positioning—Three Strikes rule*



1. ISPs inform customers of damage done by illegal file sharing and point to legal alternatives
2. Based on information from rights holders, ISPs warn subscribers that their Internet account is being used for illegal file sharing, which may lead to legal action by the rights holder
3. ISP obliged (by co-regulation or legislation) to enforce Legal Use contractual terms against copyright infringers (identified by rights holders) and take direct action:
   - Apply technical measures such as filters, traffic management
   - Apply nontechnical measures: (Temporarily) disconnect Internet access–Three Strikes is a combination of warning process and active intervention
4. ISP required by law to provide personal data relating to given IP address on rights holder's request–without Court order–for civil action
   - Needs compatibility check with Data Protection Legislation

Note: For a detailed discussion of filtering copyrighted content see case 7

Exhibit 56: *Implementing Three Strikes in the UK—high-level sensitivity analysis*



Source: News Reports, European Commission

• Across geographies, governments and network op-erators have acted divergently. The European Par-liament in its April 2008 Resolution on "Cultural Industries in Europe" calls on content owners to col-laborate with network operators and specifically de-nounces measures criminalising consumers who are not seeking to make a profit as not being the right solution to combat digital piracy. Strongly hinting at the French approach, Parliament calls for avoiding measures "conflicting with civil liberties and human rights, and with the principles of proportionality, ef-fectiveness and dissuasiveness, such as the inter-ruption of Internet access."

2. THE REGULATORS' AGENDA

The various governmental and regulatory activities at EU and national level related to Digital Confidence can be grouped into six buckets:

• Activities related to the review of the existing legal framework for providers of electronic communications infrastructure and communications services.

• Activities related to the reinterpretation of legal principles such as the EU Data Protection Directive.

• Activities skewed towards facilitating cross-industry stakeholder cooperation.

• Co-sponsored initiatives

• Law-making activities at decisively national level.

• Activities aimed at driving international coordination.

2.1 ADAPTATION OF THE LEGAL FRAMEWORK AND PUBLIC POLICY

In November 2007, the European Commission proposed a "Review of the European Regulatory Framework" for providers of electronic communications infrastructure and services. The Commission envisages that the proposals will become law before the end of 2009.

Against the background of growing threats such as spam, spyware, viruses, and phishing attacks, the Review seeks to strengthen the resilience of existing networks, whilst complementing earlier legislation that criminalises certain activities. With regard to Digital Confidence, the objectives of the Review mainly relate to:

• Increasing consumer awareness and recourse, specifically with regards to network security breaches and e-privacy. For example, the Commission introduces the concept of mandatory reporting of security breaches by network operators and ISPs.

• Enhancing the user experience by promoting unobstructed access to digital and online services by enabling national regulatory authorities to impose minimum requirements regarding quality of service.

With regard to network security and user privacy, the Review specifically proposes that:

• Consumers are informed by ISPs if their personal data are compromised as a result of network security breaches.

• Operators and regulators are given more responsibility regarding the security and integrity of e-Communications networks and services.

• Enforcement and implementation powers for the competent authorities are strengthened, particularly in the fight against spam.

• Application of EU rules on data collection and identification devices using e-Communications networks is clarified.

With regard to safeguarding consumer access to high-quality digital and online services going forward, the Review proposes that:

• National regulatory authorities may set minimum quality of service requirements on e-Communications network providers based on standards developed at the EU level.

The aim is to prevent degradation of service and slowing of traffic over networks to such levels that basic connectivity would be seriously under threat. According to Information Society Commissioner Reding, there will, however, still be room to manage and shape traffic over networks in order to optimise the user experience, on the condition that this is done in a transparent, proportionate, and non-discriminatory manner.

The Review also addresses the independence of the European Network and Information Security Agency (ENISA), based in Crete. Established in 2004 in view of ever-increasing reliance on ICT in critical business processes, ENISA seeks to, inter alia, stimulate business continuity by benchmarking best practices and developing risk mitigation standards to deal with disruptive incidents across different infrastructures such as malicious IT attacks or loss of critical data. To date, ENISA has released a number of recommendations, for example, on security issues for online social networks, botnets, and reputation-based systems. Reflecting concerns regarding the effectiveness of ENISA in providing active operational support to business, the Commission proposed merging ENISA with a new, yet-to-be-established European Regulatory Authority. As this proposal for a new European regulatory body has proved very controversial, it is unclear whether ENISA will actually be merged or remain independent. The EU nevertheless decided that ENISA's mandate will be extended until 2011 when the new European Regulatory Authority, if it were indeed to be established, would take over.

2.2 REINTERPRETATION OF EXISTING LEGAL PRINCIPLES

Reinterpretation of legal principles is particularly prevalent in the area of Data Protection and Privacy. Current developments in Web 2.0 services and corresponding business models, for example behavioural and viral marketing, search technologies and social networking, challenge upholding basic data protection principles such as transparency, informed consent, purpose limitation, and the right to rectification as established in the 1995 EU Data Protection Directive.

The Article 29 Data Protection Working Party is constantly reviewing the application of existing legal principles of the EU Data Protection Directive to new technological developments. Recently, it adopted a new Opinion on data protection issues related to search engines. A key conclusion of this Opinion is that the Data Protection Directive generally applies to the processing of personal data by search engines. Search engine providers must delete or irreversibly anonymise personal data once they no longer serve the specified and legitimate purpose they were collected for and be capable of justifying retention and the longevity of cookies deployed at all times. The consent of the user must be sought for all planned cross-relation of user data and for user profile enrichment exercises. website editor opt-outs must be respected by search engines and requests from users to update/refresh caches must be complied with immediately. Controversy arose particularly around the notion that the Working Party interpreted IP addresses as personal data.

The Working Party's priorities going forward include work on ensuring data protection in relation to new technologies, including a focus on, inter alia, online social networks (especially for children and teenagers), behavioural profiling, data mining (online or offline), and digital broadcasting.

2.3 FACILITATING STAKEHOLDER COOPERATION

In view of the fast changing nature of markets, business models, and technologies, concerted stakeholder efforts to find fast and efficient solutions are increasingly being preferred over new legislative approaches. In the area of fighting piracy of online copyrighted content, the Commission intends to establish a stakeholders' discussion and cooperation platform, the so-called "Content Online Platform." Consumers will be given a strong voice in this platform.

Following the 2008 Communication on "Creative Content Online in the Single Market," the Commission further envisages stimulating codes of conduct between access/service providers, rights holders, and consumers to ensure adequate protection of copyrighted works and close cooperation in the fight against piracy and unauthorised file sharing.

2.4 SPONSORED INITIATIVES IN SUPPORT OF DIGITAL CONFIDENCE

In early 2008, the Commission proposed a new Safer Internet programme to enhance the safety of children in the online environment. The programme builds on the Safer Internet programme started in 2005 and will also encompass recent communications services from the Web 2.0 era, such as social networking. The proposed new programme will co-fund projects to:

• Provide national contact points for reporting illegal and harmful content online, in particular on child abuse material and grooming.

• Foster self-regulatory initiatives in this field and stimulate the involvement of children in creating a safer online environment.

• Raise awareness of children, parents, and teachers and support contact points where they can receive advice on how to stay safe online.

• Establish a knowledge base on the use of new technologies and related risks by bringing together researchers engaged in child safety online at the European level.

These proposals include recommendations made by children themselves during a European Youth forum held on Safer Internet Day in February 2008. The proposed new Safer Internet programme (2009 to 2013) is expected to be adopted in 2009. Co-funding of new projects should begin from 2010.

Example projects funded under the 2005 Safer Internet programme include "Insafe" (to empower citizens to use the Internet positively and safely by sharing best practice, information and resources in interaction with industry, schools, and families) and "INHOPE" (supporting Internet hotlines globally to report illegal content such as child sexual abuse content; see the minors' protection discussion in Chapter IV-1).

EXAMPLES FOR ONGOING REGULATION DISCUSSION

Japan: "Guidelines for Traffic Shaping," May 2008

In Japan, often referred to one of the world's most advanced markets in terms of available speeds and NGN roll-out, four telecom business associations (Japan Internet Providers Association, Telecommunications Carriers Association, Telecom Service Association, Japan Cable and Telecommunications Association) adopted "Guidelines for Traffic Shaping" in May 2008. According to a Japanese Communications Ministry survey conducted in November 2007, about 40 percent of Japanese ISPs had implemented speed regulations.

Spurred by P2P file sharing use leading to large traffic increases, the guidelines aim to curb speeds for heavy users The Interior & Communications Ministry is observing the Guidelines that establish minimum basic standards for traffic shaping on top of which each ISP will establish and implement its own operating policy. The Guidelines are voluntary—the principles identified are intended to map out a safe harbour of conduct that would be deemed lawful.

The Guidelines state that, in principle, ISPs should handle surges in communication volume by enhancing their facilities.

Restricting communication speed should be considered only in exceptional cases. For example, providers can restrict the communication speed for heavy users of certain software, such as P2P programmes, or those trying to upload an enormous amount of data exceeding a certain level, if their actions occupy much of the network and hinder the communications of other users. In such cases, however, the ISPs need to disclose information on the restrictive measures to the users.

The minimum basic standards relate to (i) scope of information necessary to put into the contract agreement; (ii) basic requirements to operate traffic shaping; and (iii) relevant legal interpretation:

It examines the basis for restricting bandwidth for specific applications or specific users who disproportionately impact the network to the detriment of general users.

It recognizes that there are privacy considerations related to the DPI involved in packet shaping (i.e., "secrecy of communications") and explains the potential for certain "consent-of-user" requirements but presents the legal basis for an exemption from the privacy and consent requirements, where there is a "lawfully justifiable" basis for the packet shaping.

Examples are given of where a practice would be lawfully justifiable—either to restrict a specific application, or to restrict a specific heavy user—focusing on: (i) legitimacy of purpose; (ii) necessity of action; and (iii) validity of means.

These examples are not exhaustive; it is recognized that practices will evolve, and accordingly the principles are kept at a high level and focused on ensuring a stable network operation.

The Guidelines recommend widespread notification of a packet shaping practice (i.e., as opposed to requiring consent), and recommends that this notification be clear to end users, non-end users, and other ISPs (i.e., particularly downstream ISPs).

UK: Ofcom "Voluntary Code of Practice: Broadband Speeds," May 2008

In the UK, broadband Internet providers are today advertising their "headlight" speeds that can be transported over the network as a maximum. Depending on technology, infrastructure, and environment, this advertised bandwidth cannot be achieved for a specific consumer.

The new code requires network operators to provide an accurate estimate of maximum achievable speed on their lines. Furthermore, the code demands the publication on the application of traffic shaping and relevant policies (e.g., affected protocols and applications, fair use limits).

Ofcom will further investigate broadband speeds and already acknowledges that speeds can significantly deviate from maximum speeds. In the future, publication of average speed might also be part of the code.

2.5 NATIONAL APPROACHES

Significant divergence in the approach to combat threats to Digital Confidence can be observed between individual countries. This becomes especially evident in the fight against piracy. France's approach, the Olivennes Agreement to prevent illegal downloaders from accessing the Internet temporarily based on "three strikes and you're out," represents one end of the continuum of national approaches, whereas, for example, the Dutch Notice and Takedown approach based on ISP self-regulation represents the other. The French approach to punishing illicit downloaders is also the converse of what is contemplated in the United States, where uploaders instead of downloaders are the target on the basis of "notice-and-takedown" procedures. Unauthorised uploading of copyrighted works is also illegal in France, but the agreement does not provide legal support for technological measures to catch uploaders. Under the Olivennes Agreement, ISPs are to implement content identification (fingerprinting and/or watermarking) and issue notices to a regulatory authority that lead to actions against users.

Earlier, in January 2008, the European Court of Justice ruled in a case involving the enforcement of IPR that EU directives on data protection and e-privacy do not require obligations being imposed on network operators to disclose personal data of illegal downloaders in civil proceedings allowing right holders to prosecute these individuals. In this case, the Spanish rightholders association Promusicae asked a Spanish court to order Telefónica to provide identities and physical addresses of customers who had used the Kazaa P2P service for illegal music file sharing. As with the European Parliament Resolution, the trade-off between protection of fundamental rights versus protection of (intellectual) property, swung in favour of safeguarding fundamental citizen rights, in this case, the right to privacy.

France, in its role of EU presidency in the second half of 2008, has announced that its IPR policy goals will not include a push for an exact replication of the Olivennes Agreement at the European level. Rather, the French presidency aims to bring all the stakeholders to the table in order to encourage negotiations.

Finally, "three strikes" is among the proposals actively being discussed at the G8 level. The Anti-Counterfeiting Trade Agreement (ACTA), which the G8 aims to adopt by the end of 2008, could include "three strikes" and mandatory ISP filtering in an attempt to address the latest P2P and Internet challenges in the fight against piracy and impose corresponding criminal sanctions.

2.6 INTERNATIONAL COORDINATION

Following the DoS attacks against Estonia (see Case 6), the NATO Bucharest Summit agreed in early April 2008 upon a common policy for cyber defence and made a commitment to establish a new authority with the primary task of coordinating NATO's "political and technical" reactions to cyber attacks.

Apart from a new body, a genuine common European approach to cyber defence also requires every member state to establish a national structure for the prevention of and defence against cyber attacks, like the U.S. Computer Emergency Readiness Team (US-CERT), a partnership among the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the country's Internet infrastructure, US-CERT coordinates defence against and responses to cyber attacks across the country. Currently, only a few European states have such structures.

Information Society Commissioner Reding announced that, in early 2009, the Commission will present a Communication on the protection of critical telecoms infrastructure. This would

be aimed at improving the preparation and the response capability at the European level in case of cyber attacks. The Commissioner underlined the importance of technical developments without forgetting the necessity of increased education regarding the advantages and risks of the Information Society. This line appears to be strongly supported by industry.

Military Botnets for Information Warfare

In May 2008, Col. Charles W. Williamson III proposed that the Air Force should build its own zombie network, so that it can launch distributed DoS attacks on foreign enemies. He recommends that the Air Force should deliberately install bots on its unclassified computers as well as civilian government machines.

Initially, other Navy officers proposed installing bots even on existing information security systems, and reusing machines that would normally be discarded to build a "bot army."

Civilian commentators from Wired considered this the "most lunatic idea to come out of the military since the gay bomb." On the other hand, the effectiveness of large DoS attacks cannot be denied—as also recently seen in Russia, where hackers brought down most of Russia's nuclear power websites with a DoS attack.

Source: Wired, Darkreading

2.7 CONCLUSION

The main legal bases for mitigating Digital Confidence challenges seem largely in place, with some need, nevertheless, for reinterpretation of existing regulatory concepts to take account of new technology, market(ing), and usage realities. The cross-border nature of Digital Confidence threats places particular emphasis on international (judicial) cooperation, increasing awareness of the urgency to act and, for governments and enforcement authorities, to allocate appropriate resources for establishing effective mitigation structures and partnerships with industry. There appears to be a trend in politics and regulatory policies to put greater emphasis on stakeholder cooperation instead of greater legislative activity—in fact, not only in Europe, but with recent moves of the FCC in the United States as well. At the same time, there is a need for continued review of the proportionality of any regulatory activity, particularly in case of highly interventionist approaches (such as "three strikes" or mandatory filtering) that may infringe on basic Internet freedoms, basic consumer rights (e.g., to privacy) and undermine vested legal certainties for industry players.

Nevertheless, industry has an opportunity to step up its responsibilities in this area with activities to educate and empower consumers to increase their confidence in using new online and digital services. Complementing industry-led corporate responsibility initiatives, when it comes to enforcement, increased sector cooperation and with governmental and regulatory bodies is required to provide a sound legal basis to support each level of intervention planned. An example would be the various levels of filtering and blocking of content, where network operators will want to ensure that their liabilities are covered. Also in the area of network security, public-private partnerships may be needed to ensure effective collection of often highly sensitive and confidential data as the basis for coherent and effective mitigation strategies.

V. RISK/BENEFIT ANALYSIS: DIGITAL CONFIDENCE PAYS OFF

As described in the last few chapters, Digital Confidence is exceedingly complex. Not only is it a major "feel good, be safe factor" for consumers, but Digital Confidence also has a relevant economic impact. For example, online piracy today has an economic impact of several billions Euro in Europe. For each of the key areas of Digital Confidence, there are trade-offs to manage, all with societal and most with economic impact. For example, protecting consumer privacy very restrictively may impact new business models based on targeted and personalised advertising—a major contributor to the €57 billion online advertising market in Europe in 2012. It is important to realise that already today many useful and innovative online services such as tour-planners or city maps can only be offered for free to a mass audience because advertising allows financing. These services may come under strong pressure and new ones may not be realised.

Furthermore, roles and responsibilities in Digital Confidence among all stakeholders in the digital economy value chain need to be defined to ensure a coherent approach is realised that is value-creating for the industry as well as delivering on users' expectations with regard to industry's performance across all pillars of Digital Confidence. These roles and responsibilities need to reflect a fair sharing of burden and be proportionate to the respective roles of the various stakeholders in the value chain. As key enablers of growth, both as carriers and providers of Internet and digital services over their networks, there is no doubt that network operators need to continue a central and important role to foster Digital Confidence; their core "conduit" business is significantly challenged as is future value that is largely generated with commerce and value-added services.

For instance, a "three strikes and you're out" rule advocated by content owners and their associations requires network providers to take a role in monitoring and policing the use of copyrighted material over their networks. However, this approach could lead to a direct overall loss of about €150 million per year in revenue to the digital economy of the UK alone—in addition to implications for consumer data privacy.

To understand the economic impact of getting Digital Confidence right or wrong, we have conducted an analysis intended to look holistically at the digital economy and its revenues in Europe, now and especially into the future, and to estimate the effects of solid or weak Digital Confidence with concrete numbers. Up to now, several studies and reports have shown and estimated the impact of single measures in the area of Digital Confidence, all of them with different assumptions and only for limited geographies. For our assessment we leveraged all these inputs and built a consistent holistic model for the whole of Europe and all Digital Confidence measures.

This risk/benefit analysis provides a comprehensive view of which Digital Confidence pillars have the greatest financial impact. It assesses the revenue impact on the European digital economy of two alternative scenarios compared to a base case. Concretely, it details to what degree revenue pools of the digital economy are at risk from Digital Confidence concerns, thereby providing a perspective on financial incentives for industry to focus its attention in developing Digital Confidence solutions. Understanding this, governments and regulators can support industry's endeavours in areas that are more driven by societal rather than financial interests.

The risk of getting Digital Confidence wrong is high: Market value of €124 billion by 2012—equivalent to about 1 percent of the European GDP—could be destroyed.

Input to the analysis were a baseline market sizing built from multiple statistics and forecasts, and Booz & Company expert reconciliation and findings from a programme of over 50 interviews with industry experts as well as in-depth examination of industry best practices and perspectives.

Based on a thorough review of the gathered input, key drivers for the analysis were identified and used as the starting point for model development. The model was developed iteratively, placing sensitivity analyses against driver variation. Stabilised outcome of the modelling was finally summarised into the coherent scenarios needed for surfacing an aggregate view on Digital Confidence up- and downsides.

1. FINANCIAL SUMMARY: DOWNSIDE RISKS OF DIGITAL CONFIDENCE OUTWEIGH POTENTIAL BENEFITS

As a reference point for the analysis, the European[7] digital economy is sized at €436 billion in revenue volume across the four major categories of access, commerce, content, and advertising for 2012, with an overall compound annual growth rate of 18 percent (2007–2012).

Privacy and Data Protection as well as Network Integrity and Quality of Service have the most significant economic impact.

The worst-case scenario—getting Digital Confidence wrong, and defined as an "Industry Divergence" scenario—provides greater downside risk than the upside of getting Digital Confidence right—defined as the "One Direction" scenario: While the downside amounts to €78 billion, there is an upside of €46 billion. Adding these up shows a delta in industry revenue of €124 billion, which is equivalent to approximately 1 percent of European GDP, with corresponding effects on investment and employment impulses.

The revenue at risk illustrates the potential loss in value to the entire digital life ecosystem—from consumers through to advertisers, content providers, and network operators. In the worst case, there will be fewer users doing less and spending less compared to the best case. Although most of this revenue is not completely lost (e.g., just shifts from Amazon to brick-and-mortar book stores), some business models and their revenue might be completely lost (e.g., online auctions are more difficult to shift to the offline world).

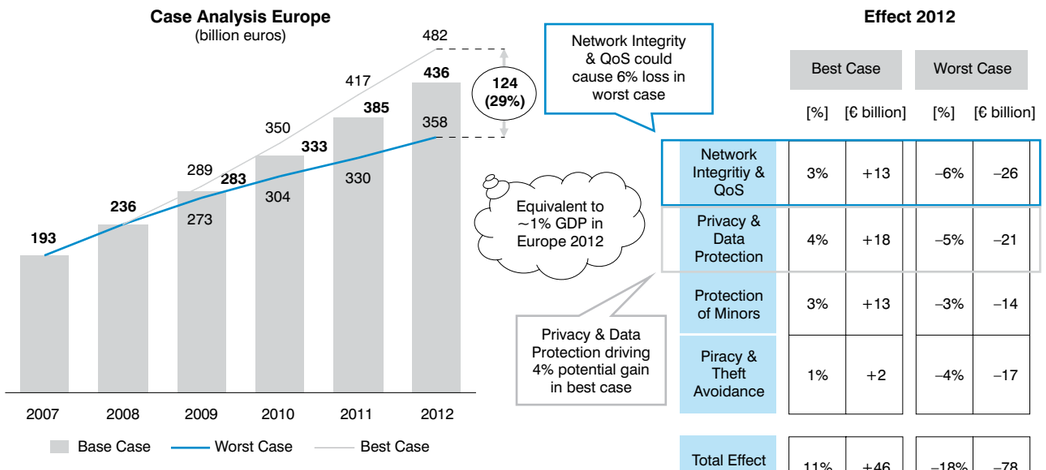
Two pillars cutting across all revenue categories have the greatest financial impact. First, there is Privacy and Data Protection, which relates to consumer concerns over security of digital data. For instance, in the worst-case scenario, consumers will be less willing to share information with third parties, thereby putting strong pressure on the innovative advertising models that the digital industry and marketers are placing significant hopes in, and which not only act as the cornerstones of many B2C business models, but also offer tangible advantages to consumers, for example, in providing better targeted information for their purchase considerations. In addition, consumers may be less willing to undertake e-Commerce and digital content purchases if there is a lack of trust in how their data is being handled and managed. Second, Network Integrity and Quality of Service also has a major impact on revenue, as it relates to the protection of the technology platforms and to ensuring optimal Internet connectivity supporting digital life. Managed well, the network can be used to deliver high bandwidth to end users at a QoS that allows all users to benefit from the full richness of digital life—from voice and Internet browsing to multimedia services and video on demand. As such, Network Integrity and Quality of Service directly impacts the level of use and number of users across the major revenue categories.

The other Digital Confidence pillars, whilst important, have less impact in pure economic terms as they only affect certain revenue categories. Piracy and Theft Avoidance primarily impacts revenue of content owners. In addition, there is a sizeable downside risk related to the negative impact on e-Commerce transactions due to people substituting online purchases for traditional media (e.g., CDs/DVDs). Minors' Protection has an indirect effect on usage to the extent that parents control how much their children use the Internet and children themselves may refrain from using certain offerings (e.g., social networking sites) if they persistently hear about negative experiences.

The introduction of more interactive, bandwidth-hungry services is most sensitive to Digital Confidence.

(7) Europe is defined in this context as the EU-27 plus Norway and Switzerland.

Exhibit 57: *Digital Confidence impact*



Effect 2012

	Best Case [%]	Best Case [€ billion]	Worst Case [%]	Worst Case [€ billion]
Network Integritiy & QoS	3%	+13	–6%	–26
Privacy & Data Protection	4%	+18	–5%	–21
Protection of Minors	3%	+13	–3%	–14
Piracy & Theft Avoidance	1%	+2	–4%	–17
Total Effect in 2012	11%	+46	–18%	–78

Note: GDP Europe 2012 estimated at roughly 12.5–13.5 tn EUR (Europe: EU-27 + Norway + Switzerland)
Source: European Union, Booz & Company Analysis

2. DIGITAL CONFIDENCE SCENARIOS—FROM DIVERGENCE TO CONVERGENCE

The scenarios used to model the impact of Digital Confidence have been derived from the general industry understanding of the issue and in particular the case examples that illustrate practices relating to the most pressing concerns.

The three scenarios vary along the overarching motto and the respective characteristics:

- "Business as usual" is the starting point or base reference for the analysis. The scenario is characterised as following the current trajectory, with only incremental improvements in certain areas and measures being more or less synchronised across stakeholders. Educational activities would continue on their current level; transparency on data use would be improved gradually, but there would be no significant improvements with respect to phishing and malware; due to mitigation being relatively effective, QoS would be acceptable, with occasional problems due to network congestion; and the challenges to contain copyright-protected content would largely remain as today (i.e., existing piracy damage is part of the base case).

- "One direction" is the best case where the industry adopts a harmonised approach towards Digital Confidence, with all players working coherently towards a common vision. Education is improved significantly across the board, often in joint efforts across stakeholders; consumers'

Exhibit 58: *Digital Confidence impact—scenario description*

	Worst Case Scenario	Base Case Scenario	Best Case Scenario
Motto	"Industry Divergence": Different measures taken	"Business as usual": Measures more or less in sync	"One direction": Convergence across stakeholders
Network Integrity & QOS	• Uncoordinated use of the network leading to systemic congestion and degraded user experience	• Occasional network congestion, especially in peak hours, increasingly requiring network operator attention to effective traffic management measures	• Significantly higher bandwidth than today coupled with constantly reliable user experience
Privacy & Data Protection	• Consumers give increasing amounts of data leading to profiling risks	• Improved transparency on data use, but no significant improvement in phishing and identity theft threat	• Education, transparency and effective opt-in and opt-out mechanisms leading to increased data sharing willingness (e.g., innovative advertising)
Protection of Minors	• Scattered educational efforts around threats on the Internet for children and parents	• Existing educational and filtering measures continued with slight process improvements	• Improved and coherent education of parents and minors by all players • More disciplined approach of minors, social networks
Piracy & Theft Avoidance	• Continued piracy, and a reduction in available legal content propositions	• Significant share of illicit file sharing and downloading of copyrighted content	• Better DRM solutions for traditional business models
Regulator Position	• Does not provide a coherent vision, tends to over-regulate (e.g., with regards to QoS requirements, piracy prosecution)	• Generally focuses on the most burning issues, especially those with divergent industry interests (e.g., privacy, minors protection), but selectively allows unbalanced interventions such as "Three Strikes"	• Strongly contributes to the "one direction" approach, stimulates industry led collaborative governance

better understanding of strengths and weaknesses of targeted advertising fosters its take-off; leveraging a broad array of accepted measures, network operators and service providers succeed in providing very reliable QoS, at higher speeds than today; and illegal file sharing diminishes as consumer awareness increases and convenient content offerings paired with new, intelligent business models emerge.

- "Industry divergence" is the worst case for the digital economy as it inhibits the continued growth of digital life. In such a scenario, players operate in an independent manner, lacking a common vision resulting in various measures being applied inconsistently. There are only limited and often contradictory measures to protect minors in digital environments; as consumers experience unwanted privacy issues they grow more sceptical about digital life in general; uncontrolled traffic management leads to frequent QoS issues and net neutrality complaints; problems around copyrighted content soar; and general content industry "depression" leads to reduction in legal content propositions in the digital world as well.

Almost €80 billion in e-Commerce revenue is at risk in relation to Digital Confidence.

The key distinction between the scenarios is the level of alignment between the industry players in the approach to Digital Confidence. Alignment does not necessarily mean players do all things in an identical way; it is rather the level of agreement across the industry to follow the same direction. It refers to the extent to which there is a common understanding of such a direction and the overall priorities as well as the resulting responsibilities of each of the stakeholders.

Higher levels of joint responsibility—for instance, in the best case—result in an improvement in the execution of Digital Confidence within each of the pillars and thereby support usage and subsequently revenue growth.

3. KEY FINANCIAL DRIVERS: ADVERTISING AND CONTENT ARE MOST EXPOSED TO DIGITAL CONFIDENCE

The revenue categories at the greatest threat from Digital Confidence are content and advertising.

Content is highly sensitive to levels of Digital Confidence. This can already be seen for example from the financial impact of video piracy today—off- and online. For 2007, the Motion Picture Association of America (MPAA) estimates a worldwide loss of more than $18 billion due to piracy, only accounting for direct damage without considering the potentially larger indirect economic impact. With 31 percent of revenues at risk in a Digital Confidence worst case, businesses and consumers must trust that online content platforms cater to content owners, whilst providing a safe and secure environment for users' personal data (e.g., usage history, credit card records, etc). Furthermore, as content in many instances requires real-time delivery (for example, BBC's iPlayer and other streaming video on demand solutions), it is highly dependent on the quality of the underlying network infrastructure. The ability to derive and grow content revenue will be dependent on the quality of the network provided by network operators. As such, network and content providers will need to find a model that shares cost and revenue in an equitable way, thereby providing the appropriate incentives for infrastructure investment needed to make the Internet a mass market delivery medium for content. In the best case, €4 billion additional revenue are in reach, compared to a downside of €6 billion.

e-Commerce, content, and advertising are most exposed to risks created by a lack of Digital Confidence.

Advertising is also highly dependent on the confidence of consumers, as advertisers will only continue to shift investments from traditional to digital environments if usage and time spent online continue to grow. For advertising, the upside is €9 billion, the downside €14 billion. This means that nearly 25 percent of advertising revenue is at risk in the worst-case scenario.

In absolute terms, e-Commerce is most at risk to Digital Confidence as it is by far the largest revenue category. The downside comes out at €52 billion, with the upside being half of that. In relative terms, however, e-Commerce is less affected as confidence is already reasonably high in established players (e.g., Amazon) and goods are delivered physically, thereby not being dependent on the Internet for the actual fulfilment.

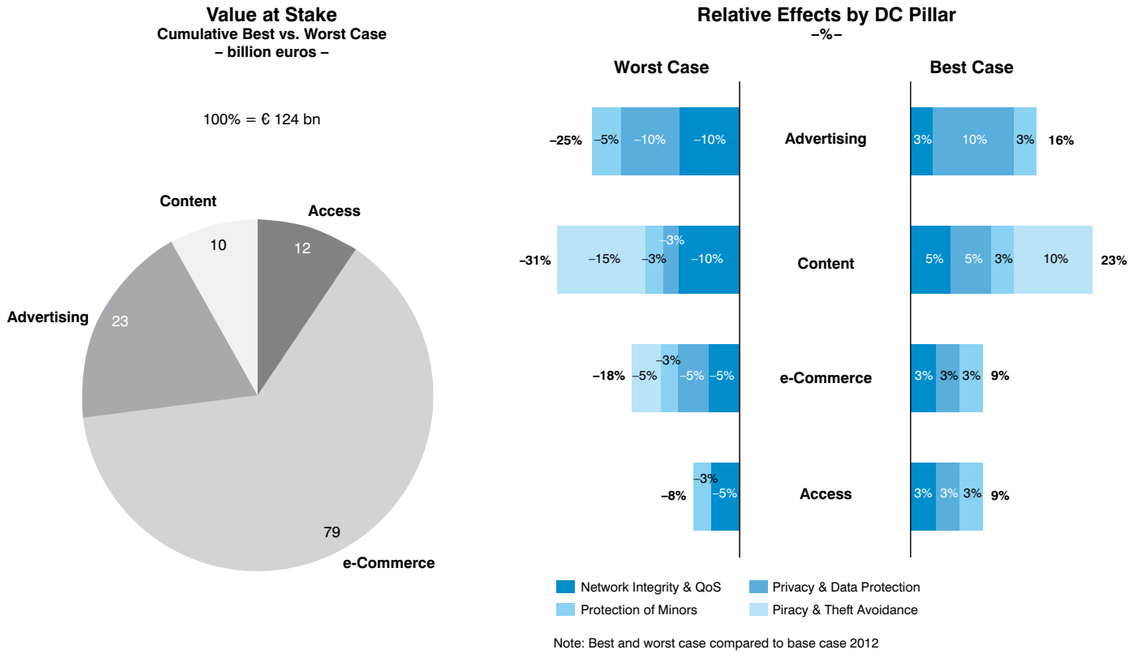
As the underlying revenue category, access is least influenced by Digital Confidence. There are lower growth expectations for access as it increasingly becomes commoditised. Digital Confidence success or failure is unlikely to actually influence user numbers significantly. Upside and downside both show the same value of €6 billion. Exhibit 58 summarises the upside and downside for the best and worst cases.

4. CONCLUSION

The risk/benefit analysis shows that, in purely economic terms and disregarding the wider societal aspect for a moment, the digital industry has a significant economic incentive in coherently addressing certain areas of Digital Confidence in order to at least avoid worst-case revenue scenarios and ideally to strive for best-case revenue potential. First, Privacy and Data Protection is financially important, especially, but not limited to, its implications for innovative (targeted) advertising business models. Second, Network Integrity and Quality of Service will be required to support the continued growth of content and video services. Third, the area of Piracy and Theft Avoidance is relevant for content owners as well as for e-Commerce. Apart from the obvious revenue implications for the content industry in protecting the existing value of their rights portfolios as well as in introducing innovative digital and online content business models, there is an additional sizeable downside risk related to the negative impact on e-Commerce transactions due to people shifting consumption to offline channels, which is not possible for many new business models (e.g., online auctions).

In summary, network providers need to continue to play an important role as their core business is a key enabler for the identified economic growth drivers. The level of network integrity has a major economic impact even if their own core access business seems least exposed to the benefits/risks of getting Digital Confidence right or wrong.

Exhibit 59: *Digital Confidence Impact—growth areas and pillars*



VI. FRAMEWORK FOR ACTION

1. INDUSTRY NEEDS TO DEVELOP LEADERSHIP IN DIGITAL CONFIDENCE

Europe's digital economy has a realistic perspective of growth spurred by Web 2.0-type services having become mainstream using the functionality, ubiquity, and increased capacity of broadband networks. Migration to next-generation access networks, proliferation of highly sophisticated network-based technologies, and the new generation of increasingly assertive "born digital" consumers are potentially disruptive forces for the digital economy ecosystem. This new paradigm is a significant challenge for policymakers, regulators, and industry at large. The level of trust that consumers place in service- and platform providers in terms of business conduct and providing secure services and network environments, as well as in the ability of governments and regulatory authorities to enforce consumer protection standards, is rapidly becoming a major factor affecting the potential growth of the digital economy.

The industry is at a watershed moment in the further development of digital life. The risk/benefit analysis shows how industry is financially impacted by Digital Confidence. There is clearly a financial imperative for action, with €124 billion at risk across the industry. However, in addition to the financial incentives, building up digital confidence credentials is also a social responsibility since it is an area of concern for consumers, regulators, and society as a whole.

The case studies in this report confirm that concerns are today addressed by various industry stakeholders. However, these actions are mostly reactive and born out of the need to respond to public outcry and media and regulatory pressure resulting from high-profile incidents involving security, privacy, or other kinds of trust breaches. Trust breaches have so far been provoked by, inter alia:

- Unmanaged service level expectations, for example, by over-promising on performance when the ability to deliver is not under the network operator's control, as in the case of the U.S. ISPs that conveyed the impression that no child sexual abuse content would be accessible over their networks. Another example is when users experienced degradation of popular bandwidth-hungry services like P2P file sharing sites by the deployment of network management technologies.

- Unmanaged expectations around the effectiveness of filtering in the case of child sexual abuse content.

- Use of intrusive Internet monitoring technologies for commercial purposes.

Despite the complexity and diversity of current approaches, several guidelines for best practices take shape, from a consumer acceptance perspective:

- Consumers accept practices that are transparent and unobtrusive—network providers and content and platform players, jointly with the regulator, are required to drive such communication forward.

- Consumers are concerned about how ISPs and cable operators manage and police consumers' digital data—clear statements and a consistent and reliable regulatory framework on this should be key priorities.

- Consumers require control over the risks they are exposed to—this asks for access to the appropriate tools, opt-in/opt-out mechanisms, and education.

- Consumers accept measures that guarantee quality of service—if this requires active traffic management, they are open to it, provided there are openly communicated terms of service, fair and transparent pricing schemes, and non-discriminatory access.

The case analyses also show the level of complexity involved in getting Digital Confidence right. Even the best-intended solutions, focused on preventing certain behaviour by blocking or filtering content, can be deemed to be at odds with civil liberties and net neutrality requirements. Solutions that focus on educating and

All four pillars of Digital Confidence need to be addressed to sustain the growth of digital life.

empowering the consumer to understand the risks and take responsibility for actions to manage these risks require a high level of industry involvement to build awareness. The software tools are available to support both approaches, but a common definition of standards and policies with respect to inappropriate content is still required.

To avoid regionally dispersed and fragmented answers to Digital Confidence issues, which are increasingly becoming global and broad, we have called for a holistic approach and industry-wide alignment. This will ultimately lead to more transparency and guidance for the consumer around the risks and benefits of digital life.

Each of the Digital Confidence pillars has complexity around the threats and solutions as well as the various stakeholder positions and interests.

The issue is mainly explored from the perspective of the cable operator. Its recommended positioning with respect to Digital Confidence is defined, and the appropriate measures are detailed accordingly. The discussion is then brought back to the industry level by identifying the implications for other stakeholders, including regulators in particular.

2. NETWORK OPERATORS AND ISPS NEED TO TAKE A CLEAR POSITION ON DIGITAL CONFIDENCE

The general self-conception of a network provider and ISP plays an important role in defining the level of engagement in building proactive Digital Confidence policies: Are we just "mere conduits"—do we only pave and operate the highways? Or do we actually engage in setting the rules for how to travel on these highways and police the rules?

However, there is no single answer—the position a network operator or ISP takes is often different across the Digital Confidence pillars.

The Digital Confidence Positioning Framework is a structure to determine positions both for individual Digital Confidence pillars and overall. The vertical axis differentiates the underlying principles, with "voluntary" and "mandatory" as the two poles. The horizontal axis differentiates how measures are taken, passively in a "hands-off" manner or actively in a "full-control" approach. The resulting four quadrants can symbolically be connected to archetypes of societal roles. The teacher educates users about opportunities and threats as much as possible, but will normally not take active corrective measures. The parent educates users about threats and measures, similarly to a teacher, but will take measures proactively if deemed necessary. The referee relies on self-imposed enforcement of rules and guidelines on a case-by-case basis rather than on education only, but rules are based on mutual agreement. The policeman is naturally inclined towards strong enforcement, takes all measures necessary to do so, and does so based on strict rules, for example, to block all illegal activities.

Based on our research and industry understanding and confirmed through our interview programme, it is clear that the natural home ground for the ISP has so far been the upper left quadrant—the Teacher role. The characteristics associated with this quadrant are aligned with the original self-conception of a network operator: Its core business purpose has been and still is to provide a secure, reliable, and powerful network for Internet traffic, without engaging in what happens over its network. From this, an educator role making consumers aware of digital confidence issues whilst providing them the tools to manage them based on a hands-off approach can be derived. Such positioning will limit risks and liabilities with respect to issues that the ISP has no primary responsibility for. In general, the ISP would by default not be responsible for defining or policing Digital Confidence standards, for example, prosecuting copyright violation. Our analysis, however, also shows that this is not enough. As a significant proportion of future growth is linked with greater usage of existing and new value-added digital and online services, the level of trust that consumers place in their provider is becoming a major precondition for growth and success in the digital marketplace going forward. As an ISP, putting ones' faith in education, corporate responsibility programmes, and legal compliance is not sufficient for finding user acceptance and building trust. Legislation can often not keep up with the speed, scope. and scale of the changes in, for example, new traffic monitoring technologies or increased security risks related to sophisticated cybercrimes that impact on Digital Confidence. Hence, successful companies do more than just comply; they stay ahead of the curve by adopting some key approaches to drive Digital Confidence:

- They internalise confidence building procedures and protocols.
- They are as open and transparent as possible in their communications with consumers.
- They make an extra effort to educate and enable consumers about how to protect their interests in the digital world.
- They use a graded, proactive approach following the E3 paradigm: Educate first, Empower second, Enforce only where feasible

As such, MNOs must be proactive in shaping the industry agenda, by seeking to develop solutions and approaches that will inevitably lead them to take new positions in both the Parent and Referee roles. There are a number of motivations for network operators and ISPs to step outside the home ground.

First, strong strategic or business reasons could drive the network operator or ISP to leave its home ground, for example, to ensure consumers' goodwill. For example, if parents are comfortable with the level of protection provided for their children, they will allow them to use the Internet more. Also, traffic management is of strategic value as it ensures that all customers benefit from investments in next-generation access networks and its higher bandwidths, not just the heavy users. The extent to which a network operator is able to guarantee quality of service and optimal broadband experience for all users is a major competitive edge in infrastructure competition going forward.

Second, potentially disproportionate regulatory intervention can be pre-empted by fostering better industry self-regulation and cooperation, for example, as announced in the UK where the leading ISPs cooperate with the British Phonographic Industry to actively approach customers warning them about piracy. In the United States, Comcast constructively reached agreement with BitTorrent on a mutually acceptable traffic management policy.

However, ISPs need to be very careful when assuming roles outside of their field of primary responsibility. Any move that may undermine their safe harbor of "mere conduit" and expose them to uncontrollable liabilities will ultimately not contribute to enhancing Digital Confidence—whilst expectations among the public would have been raised to the contrary, not to mention the negative signals this would send to their investors and shareholders.

Industry should use the E³ paradigm: Educate, Empower, Enforce.

ISPs should in any case avoid moving into the Policeman role unless legally mandated. The Policeman role is a highly oppressive approach that would have a negative impact on consumer acceptance. When legally mandated, not only are network operators and ISPs actually obliged to take on such a role—they are in addition protected against legal liabilities when they do so. For instance, if they are mandated by law to block certain Internet sites—due to content concerns—then they are less at risk over accusations of copyright infringement, civil liberties, freedom of speech, and net neutrality.

In summary, this positioning translates into a clear paradigm: E3—Educate, Empower, Enforce. The positioning in the matrix determines the level to which these roles are applied in the network operator case.

3. NETWORK OPERATOR CALL FOR ACTION: THE FIVE KEY INITIATIVES FOR DIGITAL CONFIDENCE

The E3 paradigm defines on a summary level what to do as a network operator and ISP but is equally applicable to all other stakeholders of digital life.

Educate. Network operators and ISPs should ensure that their customers understand the threats surrounding digital life and provide them with the knowledge to deal with these threats and hence operate safely. Policies should be clear and transparent to end users. This includes transparency about the company's policies in the area of Digital Confidence.

Empower. Network operators and ISPs should enable their customers as much as possible to control digital threats and problems themselves, for example, through an opt-in or opt-out approach to blocking undesired content. Specifically, network operators and ISPs should provide

Exhibit 60: *"Home Ground" positioning for Network operators*

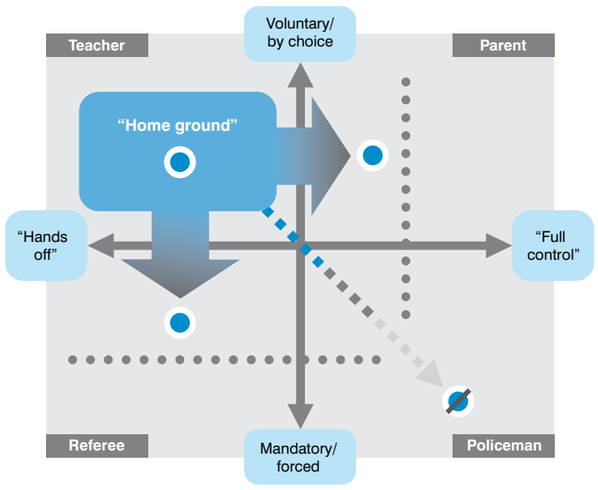
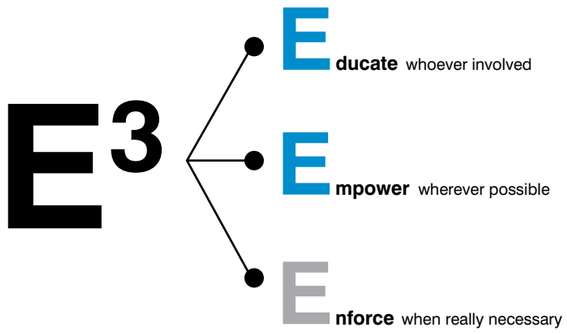


Exhibit 61: *The E³ paradigm*



such processes and tools to customers and support third parties developing and operating these tools and services.

Enforce. Network operators and ISPs should proactively intervene and steer user behaviour in areas of specific public interest vital to preserve Digital Confidence. ISPs should in such cases seek sector-wide alignment and share best practices.

Placing strong emphasis on education and empowerment effectively picks up changes in consumers' self-conception and the way consumers inform themselves and address issues. A recent survey (Edelman's 2008 Trust Barometer) analysing European "Info-entials," young opinion elites aged 25 to 34, concluded that these Info-entials gather information in a profoundly different manner than their older peers, relying on multiple sources of information, with their views shaped by continuous participation, reflection, and sharing. As such, Info-entials are open or even demand to be educated well and to be empowered to act for themselves. The survey finds that—despite being "historically cynical about business"—they today tend to show a comparatively high level of trust in business. But the most trusted source of information for Info-entials in most EU countries are "people like you and me" and NGOs. Network operators and ISPs can build on this not only to address Digital Confidence concerns, but also leverage it as a contribution to classic customer retention.

Network operators and ISPs have to specify concrete measures.

Building on this general guideline, a company-oriented view is used to derive and specify concrete measures. Measures have been defined in five initiative areas:

1. POLICIES

Network operators and ISPs must have a Digital Confidence positioning statement defining their strategy and position for each confidence pillar. This needs to be the basis for all Digital Confidence-related policies in four areas: Minors' Protection, Data Protection and Privacy, Traffic Management, and Piracy. The positioning statement needs to be precise enough to provide tangible guidance on the underlying questions related to these issues, that is, how does a company balance the trade-off between inappropriate content and freedom of expression.

As a next step these policies need to be embedded in the core processes of the company. In most cases this will have direct impact on the way network operators think about product development, for example, by making sure that all products and services released meet the standards.

In addition, network operators must keep Digital Confidence policies and procedures up to date, by conducting regular legal, public policy, and technical reviews of existing policies and procedures.

Last but not least, the cases analysed in this report point to one very important lesson learnt: Confidence requires trust, and trust can best be built on open communication; transparency pays off. As a consequence, companies should be open about the policies they apply and the rationales behind them—including business rationales. Experience shows that consumer acceptance is generally high if rules and the underlying rationale are openly communicated—for example, with Google's Gmail displaying targeted advertising—and this also opens a dialogue with the consumer, which can be very helpful to improve solutions.

2. GOVERNANCE

Digital Confidence issues are complex, very sensitive, and cross-functional in nature and often require the company to define fundamental positions—for example, how do we deal with sexual abuse content? Getting it wrong bears high reputational and financial risks. Hence, it is of utmost importance to devote sufficient top management attention to the subject. Digital Confidence should be clearly embedded in the organisational structure, through, for example, a Digital Confidence steering committee with senior oversight including the authority to oversee and implement all related activities.

3. TECHNOLOGY

Enabling technologies are largely in place for Digital Confidence, and the focus of attention turns to deciding individual positioning, defining appropriate policies, and establishing the supporting governance structures. Nevertheless, there are certain technology-related investments that will need to be made by the majority of network operators to prepare for the future. They relate to ensuring that the quality of service can be maintained despite the increasing levels of multimedia traffic. Network operators will need to make investment decisions by managing the trade-off between adding further transport capacity and active traffic management, that is, via tiered pricing or technical measures. Network operators need to work with content providers to optimise their networks for multimedia content delivery through technologies such as peer-to-peer caches (e.g., P4P initiative) or content delivery networks.

They need to make sure regulators understand that they address the issue appropriately.

Another major technology risk area currently relates to end-user equipment. Such equipment is generally not sufficiently protected from threats such as viruses, botnets, and other forms of malware. Software solutions already exist; however, network operators and ISPs should be even more active in encouraging customers to use them. Network operators and ISPs must also deploy tools and solutions that empower consumers to control and manage their own exposure, for example, via an opt-in/opt-out facility. This will require a step change in the level of activities: Offering solutions for download on the website is not good enough; ISPs should launch programmes to drive and track the number of installed solutions (essentially extending their Teacher role into a more "parent" position).

4. CONSUMER EDUCATION

Cable and telecom network operators and ISPs should engage in industry programmes jointly with NGOs and undertake their own appropriate education initiatives (e.g., information campaigns on their own websites).

These programmes need to cover threats related to data publication, targeted advertising, piracy, and online behaviour overall (including what constitutes bullying, solicitation, and unacceptable content).

Education should be targeted with messages tuned in to specific user groups, including parents and children. The parents' programme should focus on how to monitor children's activities and build awareness of the threats of the environment—and showcase the tools available to them to manage their children's online environment. Children's education should focus on recognising and dealing with threats.

5. REGULATION

Network operators need to encourage regulators to focus on specific action areas to support industry's endeavours in proactively building confidence in areas that clearly fall outside the orbit of network operator or ISP activity (like blacklisting of illegal content or law enforcement). Regulators should be careful not to proactively create regulation in these areas unless the proportionality of those measures can be ensured. The regulator would only need to be involved directly if consumer interests were genuinely being compromised.

In response, industry needs to demonstrate that it is serious about Digital Confidence by taking the initiative to develop coherent solutions. Such solutions must have the commitment of all players and need to proportionately allocate the cost of implementation and the resulting financial rewards. Regulators must allow industry to develop such solutions and foster stakeholder cooperation and financial support programmes, whilst allowing competitive pressures to work in favour of consumer interests being upheld rather than applying regulation. Although well-intentioned, the regulation may in fact be counterproductive from a consumer point of view and cause economic damage.

In executing measures across these five initiative areas, network operators and ISPs are overall well advised to cooperate with NGOs as broadly as possible. Many aspects can be addressed a lot more effectively if one operator takes the initiative jointly with an NGO as the latter can ensure neutrality and industry-wide applicability, leveraging the good reputation NGOs have. Recent surveys show that NGOs rate highly in consumer trust.

4. IMPLICATIONS FOR OTHER STAKEHOLDERS

This network operator position also sets clear expectations towards the other stakeholders in the digital life ecosystem. The three most important groups are:

- Consumers.
- Other suppliers along the digital value chain (including content providers, software and application developers, and distributors, for example, e-shops).
- Regulators and governments.

CONSUMERS

Consumers must understand the need to apply common sense in digital life as they naturally do in the offline world. In addition, they need to learn how to operate the consumer-oriented solutions that network operators, ISPs, and others develop to allow them to manage and control the threats of digital life themselves. In support of these requirements, they should accept and make use of education offers from public bodies (e.g., schools, universities, governmental agencies).

Consumers have to learn to use the resources provided by the industry.

SUPPLIERS OF COPYRIGHTED CONTENT SHOULD USE TWO MAIN ROADS TO DRIVE THEIR AGENDA

Content owners should take responsibility for ensuring their copyrighted content is adequately protected. The music industry has struggled for some time to develop business models that incorporate the necessary controls to prevent piracy. This issue is now also affecting the film and television industries due to the availability of higher bandwidths and compression technologies. Content owners need to jointly develop solutions to realise fair value from the content they own. To achieve this, they need to develop copyright protection solutions at an industry level. The content industry cannot rely solely on network players to protect content on their behalf. Furthermore, consumers are less likely to accept Internet players' solutions (e.g., filtering or content blocking) motivated purely by business reasons, as would be the case for piracy protection, compared to those that also have a moral or social aspect (e.g., blocking child sexual abuse content). Piracy solutions need to encompass both innovative business models as well as supporting digital rights management techniques.

OTHER THIRD-PARTY PLAYERS SHOULD COOPERATE WITH THE INTERNET INDUSTRY

e-Commerce companies should work together with operators and ISPs on joint education programmes around topics of mutual interest (e.g., phishing). The intention of such programmes must be to improve consumer confidence through improved knowledge of the threats and issues. Consumers must also be provided the tools to manage these risks. Therefore, network operators and ISPs need cooperation from software and application providers for jointly developing solutions and activities, for example, OpenDNS/PhishTank including the required blacklists.

5. PRIORITIES FOR REGULATORS

The main legal bases for mitigating Digital Confidence challenges seem largely in place, with, nevertheless, a continued need for reinterpretation of existing regulatory concepts to take account of new technology, market(ing), and usage realities. The cross-border nature of Digital Confidence threats places particular emphasis on fostering international (judicial) cooperation, increasing awareness of the urgency to act, and, for governments and enforcement authorities, allocating appropriate resources to establishing effective mitigation structures and partnerships with industry. There appears to be a trend in politics and regulatory policies to put greater emphasis on stakeholder cooperation instead of on greater legislative activity—in fact, not only in Europe, but with recent moves of the FCC in the United States as well. At the same time, there is a need for continued review of the proportionality of any regulatory activity, particularly in case of highly interventionist approaches (such as "three strikes" or mandatory filtering) that may infringe on basic Internet freedoms and basic consumer rights (e.g., to privacy) and undermine vested legal certainties for industry players.

Regulators have to understand the roles of the network operator/ISP and the impact of potential regulation on these roles.

In other cases, such as the enforcement of very strict quality of service requirements, regulatory intervention could have unintended consequences, such as creating significant costs for the industry for network upgrades. As a consequence, regulators should put a special focus on the interdependencies of the different areas of Digital Confidence for the different stakeholders and balance their decisions accordingly.

Undoubtedly, regulators have an important role to play to secure Digital Confidence. Given the high complexity of the issues affecting Digital Confidence, the role of regulators to foster increased stakeholder cooperation could be an important means to that end. Based on the analysis in this report, the following areas will reward the continuous attention of regulators:

Implementing rules without considering all consequences can lead to significant revenue losses for all stakeholders.

- Encourage network operators and ISPs to establish Digital Confidence policies and procedures as well as code-of-conduct–based self-regulation on the industry level, in particular in areas where more intrusive regulatory intervention, could lead to negative economic results (e.g., on traffic management) or infringe basic consumer rights (e.g., "three strikes and you're out" rule).

- Consider measures to limit the legal and, in some instances, reputational risk for network operators and ISPs introducing Digital Confidence policies and procedures, for example, lead the development and foster the industry-wide deployment of a register of sites banned in the interest of minors' protection—and, in Europe, harmonise the current approaches scattered across countries, including establishing structures for internationally coordinated minors' protection.

- Incentivise industry players to take a more active role in consumer education—provide funding and establish umbrella initiatives to leverage scale, building on experiences gathered from the Safer Internet program, for example.

- Increase the effort for international cooperation to develop global solutions or frameworks for solutions for essentially global problems, for example, in the area of copyright protection.

In summary, Digital Confidence does not necessarily cost a lot—in terms of required investments—to get right. On the other hand, the cost of getting it wrong would be substantial. However, getting a Digital Confidence programme right is neither easy nor free. Most CEOs are under the impression that their organisations are engaged in many of the activities suggested above—and rightly so. But in most cases, this will not be enough. Digital Confidence transcends making educational materials available on the website. It is about engaging with the leading institutions in this field—private or public—on a senior level and launching serious campaigns that make a difference. This will require funding and potentially new skills in the organisations. Digital Confidence is not just about having a data privacy policy on file; it is about changing the way a company thinks and communicates about these topics with its customers and the community at large. In short, Digital Confidence requires leadership from the top in order to prevail.

The importance of the issue is unquestioned. And there is a long way to go to address all the concerns, with no single entity in digital life either having all the answers or being capable of solving all the issues alone. Digital Confidence needs to be addressed at the industry level, with active participation from the major stakeholders following a common framework with clear roles and responsibilities. In this way Digital Confidence can unfold all its power and thereby support value-creating opportunities in the digital environments for everyone.

AUTHORS OF THE STUDY

Thomas Künstner
Vice President
thomas.kuenstner@booz.com
+49 211 3890 143

Michael Fischer
Principal
michael.fischer@booz.com
+49 211 3890 168

John Ward
Senior Associate
john.ward@booz.com
+44 20 7393 3782

Martin F. Brunner
Senior Associate
martin.brunner@booz.com
+49 30 88705 842

Florian Pötscher
Senior Consultant
florian.poetscher@booz.com
+43 1 51822 900

BOOZ & COMPANY WORLDWIDE OFFICES

Asia
Beijing
Hong Kong
Seoul
Shanghai
Taipei
Tokyo

Australia, New Zealand, and Southeast Asia
Adelaide
Auckland
Bangkok
Brisbane
Canberra
Jakarta
Kuala Lumpur
Melbourne
Sydney

Europe
Amsterdam
Berlin
Copenhagen
Dublin
Düsseldorf
Frankfurt
Helsinki
London
Madrid
Milan
Moscow
Munich
Oslo
Paris
Rome
Stockholm
Stuttgart
Vienna
Warsaw
Zurich

Middle East
Abu Dhabi
Beirut
Cairo
Dubai
Riyadh

North America
Atlanta
Chicago
Cleveland
Dallas
Detroit
Florham Park
Houston
Los Angeles
McLean
Mexico City
New York City
Parsippany
San Francisco

South America
Buenos Aires
Rio de Janeiro
Santiago
São Paulo

09/08 Printed in Germany