Policy and Regulatory Framework for Governing Internet Applications

March 2014
Legal Disclaimer
This document contains information and statistics that have been obtained from sources believed to be reliable in regard to the subject matter covered.

This document does not however constitute commercial, legal or other advice however so described. The Telecommunications Regulatory Authority of the Kingdom of Bahrain (“the TRA”) and Detecon International GmbH (“DTC”) exclude any warranty and, or liability, expressed or implied, as to the quality, completeness, adequacy and accuracy of the information, statements and statistics contained within this document. This document is a study and it is a non-binding document. It has no legal effect. This document does not represent an official position of the TRA, but is intended to stimulate debate on the part of stakeholders and public. It does not prejudice the form or content of any future proposal by the TRA.

The TRA and DTC reserve the right to change and update the information, statements and statistics provided in this document at its discretion and without prior notification and assumes no obligation to update the document on the basis of suggestions, comments and/or queries made by third parties. The TRA and DTC assumes no responsibility for any consequences that may arise in the absence of such changes and/or updates.

To the fullest extent permitted by law, neither the TRA or any of its officers however so described or agents nor DTC will assume responsibility and/or liability for any loss or damage, including losses or damages such as loss of goodwill, income, profit or opportunity, or any other claim of third parties, arising from or related to the use of the content of this document.

This publication or parts there of may only be reproduced or copied with the prior written permission from Detecon International GmbH or TRA Bahrain.

Published by
Detecon International GmbH
www.detecon.com
Contents

1. Management Summary 5
2. Overview of Internet Application Business Models 6
   2.1 Introduction 6
   2.2 Impact of the internet 7
   2.3 Classification of internet applications 8
   2.4 Use Cases 9
3. Major Regulatory Issues 23
   3.1 Introduction 23
   3.2 Regulatory issues related to the use cases 24
   3.3 Summary of the most important regulatory issues 26
4. Deep Dives 28
   4.1 Security / Cyber Safety Issues 28
   4.2 Effects on the operators’ business models 37
   4.3 National Security 47
5. Conclusions and Recommendations 58
   5.1 Conclusions 58
   5.2 Recommendations 59
   5.3 Roadmap 66
6. The Authors 67
7. The Company 68
List of Figures

Figure 1: Global IP Traffic

Figure 2: Top 10 Internet Company IPO over the last decade

Figure 3: Use cases classification

Figure 4: Examples of OTT Voice/Video services

Figure 5: Global OTT mVoIP subscribers

Figure 6: Valuation and revenues of Skype

Figure 7: Examples of OTT Communications Messaging Services

Figure 8: Total in-bound and outbound messages processed per day

Figure 9: Examples of OTT Media Providers

Figure 10: Hours of Video uploaded per minute on Youtube

Figure 11: OTT Video Revenue Forecast

Figure 12: Mobile Network Data Traffic in the Middle East - Average Monthly Consumption per Wireless Subscription (Forecast)

Figure 13: Elements of eCommerce

Figure 14: eCommerce Sales worldwide

Figure 15: BitCoin price and Volume Fluctuations (2 month) until October 2013

Figure 16: Examples of Internet Services

Figure 17: Cloud Spending

Figure 18: Social networks

Figure 19: Facebook Users, Global Estimate

Figure 20: Time spent on Social Media (bn minutes, worldwide)

Figure 22: Number of photographs uploaded and shared per day (mn)

Figure 22: Other internet content

Figure 23: Internet Users

Figure 24: Growth in Online Gambling

Figure 25: What Happens In An Internet Minute? (Source: Intel)

Figure 26: Number of daily “Snaps” from Snapchat (Mn)

Figure 27: Malware Encounter Rate (October 2013)

Figure 28: Privacy and Data Protection

Figure 29: Business Continuity Management (Detecon 2013)

Figure 30: Top Web Malware Types (2012)

Figure 31: Top Ten Spam e-Mail Categories (2010-11)

Figure 32: Options for managing the use of OTT Services

Figure 33: Decoupling of Telecom Layers (Source: Detecon)

Figure 34: Summary of the international treatment of OTT voice providers

Figure 35: Business models of Internet Application Providers (Source: Detecon)

Figure 36: SMS versus OTT messaging

Figure 37: SMS decline with Smartphone Growth @ KPN89

Figure 38: User Traffic Share on Operators’ Internet Networks (Source: Telegeography)

Figure 39: Lawful Intercept in IMS-based Networks (Source: Safesoft)

Figure 40: Posting from NCSA’s National Cyber Security Awareness Campaign (Source: NCSA)

Figure 41: Twitter usage by country in 2012 (Source: globalwebindex.net)

Figure 42: Convergence of regulatory tasks and legal frameworks
1. Management Summary

The international dynamics of the internet will not be halted by national regulations. A major enabler of the net’s development has indeed been the lack of regulation that it has faced to date. The regulator’s objectives must be to catalyse additional opportunities offered by the internet to the benefit of the consumer and to support competition. While avoiding the trap of regarding the internet as a threat, a further regulatory task must be to facilitate the reduction or minimization of internet-driven risks in the areas of security and data protection – both from the consumers’ and from the nation’s point of view.

The proliferation of IP-based telecommunication networks has facilitated the decoupling of application and network layers and enabled OTT providers to deliver their content and applications directly to end users. Accusations that OTT providers are “free riders” in the transport market are not entirely accurate. The operators are paid for the transport of the data – albeit as a flat rate from the user.

While the competition provided by the OTT application providers does lead to disruption, a functional market should be able to adapt to the new situation: the telcos would be expected to change their business cases and prices in line with market demand. As this is not happening, competition is apparently dysfunctional.

A major motivation for GCC governments wishing to intervene in the internet application market is the surprising realization that the rollout of nationwide fixed broadband – often a political objective - has not occurred “naturally”. This is a further indication that the market is not functioning. The main recommendation of this study is that the fixed broadband markets should be analysed and the regulatory framework in which the SMP broadband providers must operate should be reviewed to identify the reasons behind such malfunction.

The individual recommendations are:

- Re-assess the broadband market to determine whether political rollout targets are commercially viable, develop/adapt policy as appropriate.
- Implement review of regulations faced by network operators to ensure that these reflect the changed market situation. Rebalance obligations as found to be necessary.
- Determine whether the provision of specific (free) OTT services represents unfair competition and is detrimental to the development of the market. Take action as required.
- Determine whether a lack of competitive pressure on the fixed broadband providers is preventing the market from functioning. If so, take steps to open up the market to more competition.
- Define a framework for net neutrality regulations to enable commercial service offers and cost-oriented market pricing while protecting the consumers’ interests.
- Update the license conditions of existing operators and service providers to reflect the findings of this study concerning net neutrality and growing data protection and security requirements.
- Establish coordination procedures between financial service regulation, data privacy and protection regulation, broadcasting/publishing regulation (e.g. PPP Law) and communications regulation to reflect the convergence resulting from the internet and to ensure that all regulatory measures are consistent and coherent.
- Combine broadcasting, communications (and publishing) regulation.
- Draft and ratify cybercrime legislation which is coordinated throughout the GCC.
- Draft and implement a new/updated data protection law which is coordinated throughout the GCC region and is in line with the leading edge work being implemented in the EU.
- Develop GCC-wide procedures to facilitate content regulation.
- Develop strategy for consistent and continuous user information concerning the risks and benefits of the internet.
- Investigate the feasibility of establishing a regional cybercrime center for GCC.
- Encourage development of the local CDN market with the objective of establishing a data center hub for the region.
2. Overview of Internet Application Business Models

2.1 Introduction

The internet is growing at a rapid pace, dramatically penetrating and in many cases transforming the way people work, play and live. This change is not restricted to the developed world, but is increasingly seen in emerging markets (Figure 1) and is fueled by the rise of the mobile internet. With growing availability of robust broadband networks, increased competition, and declining price-points, the internet is now available to a large segment of people.

Figure 1: Global IP Traffic

This growth of the internet has enabled the rise of firms like Google, Facebook and Amazon, who have taken advantage of its ubiquity and reach to develop into global enterprises. Figure 2 shows a strong emergence of Chinese internet giants over the past decade. What makes this industry unique is its pace of change and the often disruptive impact that it has on traditional industries.

---

1. Cisco Visual Networking Index (VNI) 2013
One of the strongest enablers of this growth has apparently been the lack of clear regulation in this sector – with standardization driven by user forums such as the IETF rather than by inter-governmental bodies such as the ITU. Even to this day, important components such as domain names are governed by quasi-official bodies such as ICANN, pointing to the non-affiliated structure of the internet. This relatively untethered approach has allowed for faster development, and has lowered the barriers to entry. Most existing regulations were developed with more static industries in mind so that, although the internet firms may infringe on the business of legacy industries, existing regulations aren’t designed to deal with such players. Moreover, the dynamic nature of the internet demands regulations which continuously evolve rather than being designed as static documents.

2.2 Impact of the internet

When considering how to best manage the internet, policy makers need to recognize the manifold positive impacts it has had on everyday lives. It is imperative that any move towards regulation should serve as a catalyst to drive additional opportunities and create effective competition – rather than viewing the technology as a threat.

From the purely financial perspective the rise of the internet can be correlated with strong economic growth. This can be gauged on three fronts:

- A strong contribution to GDP (the internet accounts for up to 3.4% of the total GDP in the 13 economies which make up 70% of global GDP);
- An increase in living standards in line with maturity of the internet ecosystem (a real per capita increase of USD 500 when examining “advanced” nations);
- Improved job opportunities and job creation (0.7 million net new jobs attributed to the internet over 15 years in France).

The internet is now responsible for up to 21% of economic growth in developed nations. There is also a major impact on society as internet applications re-define how we communicate, interact and work, and users’ average online time continues to increase.

---

2 Impact of Internet on Economic Growth, McKinsey Global Institute, 2011
3 Scandinavia, North America, the Netherlands, Switzerland, the UK and South Korea (McKinsey Global Institute e3 ranking)
4 www.wsc.org
In many other ways the internet can be seen as a source of creative destruction. It can be considered the dismantling force for several legacy industries (e.g. print news), but at the same time it brings about a new wave of opportunities, making services and content accessible to a larger audience. Since this is happening on a global scale, attempts made by individual nations to control or stop it has seen diverse effects – the most common effect of such attempts being a negative impact on the overall development of the country in question. On the other hand national authorities are of course justified in taking measures to prevent criminal activity and to ensure that public policy and moral standards are being upheld in the content and services available over the net.

This balancing of the pros and cons is an important general consideration for policy-makers talking about internet and internet service regulation. Each measure must be understood and the effects of interventions weighed up. Decisions must also take time into consideration – the fast moving, and changing nature of the internet make it futile to bring about regulation based only upon historical precedent. Future looking policies must be designed and operated so as to be ready to adapt to new technologies, trends and above all new business models.

2.3 Classification of internet applications

There is no international agreement on the classification or taxonomy of the myriad services that the internet has to offer. Even organizations such as the FCC summarily classify all internet services as “Title 1: information services”, as distinct from “Title 2: telecommunication services”.

Here we will segment applications based on a broad set of use cases (Figure 3) which cover a significant majority of the internet applications. Although not exhaustive, it provides a blue-print for examining regulatory approaches towards internet applications. This lack of completeness is also symbolic of how the internet continues to grow – new applications and use cases develop as technologies and needs evolve. In addition typical applications (e.g. Facebook) can span multiple use cases. Typically, providers’ business models initially focus on one or two use cases and begin horizontal expansion to encompass other cases later in their growth cycle.

For each use case, the market growth, business strategies and impact will be evaluated. This will be typified through an example of a major market representative of each case.

Figure 3: Use cases classification
2.4 Use Cases

2.4.1 OTT Communications

OTT Communication refers to services whose primary applications lie in communications but use the internet as the transport medium rather than the legacy telephony infrastructure (PATS). This is especially relevant to telecom operators since these services operate in a similar space as traditional voice and messaging services.

Voice/Video

Voice and video-based internet communication services are becoming increasingly popular facilitated by flat rate data plans, free options via WiFi and a host of features such as video calling which enhance user experience. This makes them a popular alternative to the traditional phone call – whether mobile or fixed.

<table>
<thead>
<tr>
<th>Service</th>
<th>Details</th>
</tr>
</thead>
</table>
| Skype   | 300 mn users (2013)  
|         | Allows for free voice/video skype to skype calling  
|         | Enables calling to POTS via skype-out service |
| Facetime| Allows for free video calling (using data when on mobile network) between iPhone users |
| Viber   | 200 mn users (May 2013)  
|         | Free calling between Viber users |

These services have witnessed strong growth over the past few years which can be attributed to several factors:

- The business models (calls are typically free) make it an attractive proposition, especially for international calling.
- Smartphone penetration has continued to increase - is expected to exceed 50% by 2016 globally - and lower cost models are entering the market, reducing barriers to entry. This trend is particularly apparent in countries with a large population of migrant blue collar workers.
- Data prices (both mobile and fixed) have fallen on a $/MB basis. Many of these services also work on WiFi networks, with no additional mobile data usage. Smartphones also work on WiFi and the proliferation of WiFi hotspots (often ‘free’) allows users to make and receive calls at no cost.

This is a departure from the hype and bust of Skype in the early part of the decade. At that time, although heralded to be the demise of telephony, it had limited impact since mobile networks were still evolving, data rates were slow and the smartphone was still in its infancy. Now, with the near ubiquitous presence of high speed broadband networks and the large number of mobile users, the shift from traditional telephony to OTT communications is in full flow.

---

5 Informa Telecoms and Media Report, 2013
OTT communication players’ business models are different to those of traditional telcos. A few examples include:

- Free services – often peer-to-peer services such as all Skype-to-Skype or Viber-to-Viber services;
- Bundled – Facetime is a feature available to all iPhone users; users can opt to use either the mobile network (consuming billed data) or wifi (for free);
- Freemium – where basic features are free but advanced features (such as group video-conferencing on Skype) are charged for – either as a one time fee or on a subscription basis;
- Paid for – especially where calls terminate on a third party PSTN network, such as Skype-out.

It is however justified to question the commercial motives of these models. Although these players are having a disruptive effect on the market, most are not profitable. An interesting example is that of Skype – which has been the bellweather in this market. Although the company valuation remains high – no owning entity has yet managed to make it into a profitable venture (Figure 6).
OTT communication services such as Skype are viewed skeptically and being carefully examined by both operators and regulators around the world. However it is important to view this trend in perspective. Voice is becoming increasingly commoditized and is moving towards all IP. With the advent of LTE, voice itself will be transported as packet switched (IP) based traffic rather than circuit switched. In effect, both traditional and OTT players will be offering Voice-over-IP. An important remaining distinction will be the QoS offered, it is likely that this will prove a more resilient classification criterium for future regulation than technology-based options.

Some predictions point out that OTT voice will cost the global telecoms industry $479bn in cumulative lost revenues. In many countries, licensing fees form an essential part of tax revenues. With firms such as Skype, who are not based in the home country, this revenue is not realized, leading to a loss to the exchequer.

**Messaging**

Even more than OTT voice, IP messaging has shown very strong growth, simply because of the low bandwidth use and better feature set (sending text, audio and graphical content) at a very low (even zero) price-point. Growth is also driven by the younger generation, who prefer the rich text and graphic messaging options provided.

<table>
<thead>
<tr>
<th>WhatsApp</th>
<th>Tencent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top selling app in 47 countries</td>
<td>800m active accounts (March 2013)</td>
</tr>
<tr>
<td>Processing 27bn messages daily (June 2013)</td>
<td>Available on all Smartphone platforms</td>
</tr>
<tr>
<td>300 m active users (May 2013)</td>
<td>Primarily China/ Asia based</td>
</tr>
<tr>
<td>Available on all Smartphone platforms</td>
<td></td>
</tr>
</tbody>
</table>

Figure 7: Examples of OTT Communications Messaging Services

Companies such as WhatsApp, Kakaotalk etc have fueled strong growth in this service over the past couple of years. Examining the total traffic (messages per day) of four players (iMessage, WhatsApp, Kakaotalk and WeChat) we see a CAGR of 108% over 4 quarters in 2012.

Although this exponential growth cannot continue indefinitely, it is expected that IP messaging will replace SMS to a large extent.

The IP-based messaging services business models are aligned to those of the voice players. Backed by high valuations, the current focus seems to be on establishing market presence rather than monetization.

---

9 Note: many of the VoIP players such as Skype also offer similar IM services
A few price examples include:

- WhatsApp yearly subscription charge of $0.99
- Free service by WeChat (owned by Tencent)

This free(mium) trend is bound to change in time as pressures on monetization begin to grow. However the global nature of these services allows the players to achieve economies of scale far beyond those of legacy operators.

The general shift away from SMS is denying telcos of one of their most profitable lines of business. Cut-throat pricing in the short term and scale economies in the longer term make competition based on price look like an uphill battle for these legacy providers.

### 2.4.2 OTT Media

As fixed networks become more robust, and mobile devices (including larger forms such as tablets) continue to proliferate, an increasing amount of internet traffic is made up of video. OTT Media refers to video and audio content being streamed and/or downloaded over the internet. This is not to be confused with IPTV, which uses dedicated IP channels for content and is not characterized as best effort. In a broad classification we can further categorize OTT media into

- **Video**
  - User generated video
  - Produced (curated) content
- **Audio**

Those listed below are among the players who comprise the legal market space. However, there is also a significant amount of illegal – primarily unlicensed - content. These are based off peer-to-peer private networks (e.g. BitTorrent), and although they significantly contribute to data traffic they have proven very difficult to police due to their distributed architectures.

---

10 Infonetics 2013 mVoIP subscribers
OTT Media has shown some of the strongest growth over the past few years as high speed broadband (in excess of 10 Mbps on fixed and >1 Mbps on mobile) has become a reality in many countries. This has not only been simple user generated content which continues to flourish, but also premium content being delivered over the internet from the likes of Netflix and Hulu. Over 30% of all internet traffic is now streaming media. In developed markets this is close to 50%.

Figure 10 shows the growth in the hours of videos uploaded on Youtube per minute. This has resulted in backend providers and operators investing heavily to be better able to carry this traffic.

---

11 Global Internet Phenomena Report 1H 2013
12 Youtube
The players in OTT media use several different business models depending upon the specific segment that is being targeted:

- Advertising is the main revenue source for YouTube, Vimeo and other players. Automated advertising placements based upon the user’s search history are common as well as sponsored advertisements.
- A second and increasingly prominent source of revenue is through subscriptions – especially for premium content. A prominent example is Netflix which provides the user with access to different levels of content depending upon their subscription level.
- Finally, we have transaction (or pay per view) content which is typically used for access to one time content (e.g. sports events or première of a new movie).

For premium production content, the use of OTT serves as a means to reach an increasingly wide audience, which has a strong preference for an ‘on demand’ experience rather than a push experience as seen in traditional broadcasting. Some of these players (such as Hulu) have been established by production houses themselves as they seek a way to directly access and interact with customers.

User generated content is not suitable for direct monetization, but it serves as a way to reach a broader audience and indirectly allows firms such as Google to capitalize and serve up advertisements.

![Figure 11: OTT Video Revenue Forecast](image)

The primary and largest impact that OTT media has had has been in the sizeable portion of internet traffic now solely concerned with streaming media. Infrastructure providers are having to invest massively in higher and higher capacity infrastructure (both access and core) to meet this demand. It also impacts telcos’ business models including flat rate data plans.

---

13 Informa 2013
One of the consequences to be expected is that operators will move away from unlimited (flat rate) data plans. It is already common practice (although rarely openly stated) for operators to throttle bandwidth in case of extreme data transfer volumes, and tiered pricing is the logical next step.\(^{15}\)

### 2.4.3 Internet Commerce

Internet Commerce (or e-Commerce as it is often called) is one of the most important elements underpinning the business models of different internet players and applications. Although more under the purview of financial rather than telco regulation it is a widely used and accepted internet application and thus its trends should be understood by regulators and operators. Within this complex space three elements are examined.

<table>
<thead>
<tr>
<th>PayPal</th>
<th>• Peer-to-Peer platform</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Acquired by eBay</td>
</tr>
<tr>
<td></td>
<td>• Can process through intermediary or via escrow account</td>
</tr>
</tbody>
</table>

| Web Shop      | • Online shopping via financial 3rd parties |
|---------------|• Prominent examples are Amazon, eBay etc |
|               |• Uses credit cards and banks as intermediaries |

| BitCoin       | • Alternative internet payment options |
|---------------|• Cryptocurrency |
|               |• Not pegged to any national currency |

---

\(^{14}\) ABI Research 2013  
\(^{15}\) In Germany Deutsche Telekom has just lost a court case covering their intention to throttle data speeds above a certain volume. The basis of the decision is however contention about calling the tariff a “flat rate”. It is to be expected that the name will be dropped and DTAG will still implement throttling tactics.
E-Commerce has seen strong and consistent growth as the internet facilitates easy and convenient transactions. The CAGR of 17% seen over the past years is expected to continue with strong growth coming from Asia and, to a certain extent, Africa as mobile commerce (e.g. m-Pesa) offers a viable alternative in the absence of established and well-defined financial institutions.

E-Commerce covers a myriad of business strategies ranging from direct peer-to-peer payment, payment via financial intermediaries (banks, credit cards etc) as well as pure electronic options like BitCoin.

Peer-to-peer payments and online shops typically fall under the aegis of the financial regulations of nation states. Cryptocurrency options such as BitCoin have emerged into prominence as niche and independent platforms since 2012. These occupy a grey area since they are purposely positioned beyond the reach of regulators. They have proven to be volatile and difficult to track. Although to date only occupying a miniscule niche in the marketplace, Ebay’s announcement that they intend to accept BitCoins as a payment method has reduced its reputation as a currency for illegal activities and increased its value significantly. The volatility of currencies such as Bitcoin is extremely high (Figure 15) and made worse due to a lack of control from central banks etc. Security doubts compound uncertainty about the medium to long term prospects of this application.

---

16 www.eMarketer.com, June 2013
17 www.bitcoincharts.com
2.4.4 Internet Services

Internet services relate to different applications where the end user device behaves more as a user interface rather than a computation and/or storage medium. These have become increasingly popular with advances in computing power, declining prices for storage, and the rise of cloud computing. Here third party companies function as service providers providing elements such as Platform as a Service (PaaS) or Software as a Service (SaaS) functionality, functions which in legacy systems were an integral part of the offline device itself. The perceived advantages stem from the fact that functionalities such as storage capacity, applications, computing power etc can be provided on an “on-demand” basis rather than once-off. For example: rather than buying a 500 GB hard-drive today, you could use cloud-based storage which can dynamically offer you storage capacity from 10 GB to 100 TB instantaneously - depending upon your needs.

| Dropbox | • Storage as a Service Provider  
| • 175m users (June 2013)  
| • > $500m in revenues (November 2012)  
| • Valuation $4bn (2011) |

| Office 365 | • Online, cloud based version of Microsoft Office  
| • Offered as a Software as a Service  
| • Subscription model |

The market for these services is expected to experience steady growth in both the private and public sectors over the next decade as (and only as long as) cloud-based services gain customer trust. This cloud services space consists of many sub-segments covering both B2B and B2C markets with differing growth rates per segment and market size. Within the big ticket areas of Infrastructure, Platform, Applications and Business Processes the growth is distributed as shown in the Figure 17 below.

Figure 16: Examples of Internet Services

Figure 17: Cloud Spending

18 Gartner 2013
The segment employs several different business models – the specific models depend on the addressed segment (e.g. B2C versus B2B) and the features being offered. A non-exhaustive list includes:

- **Free(mium):** aimed at capturing a large user base especially during the growth phase of the business. This offers basic functionality – however additional features (such as increased storage space) are offered at a price.
- **Subscription based:** the user pays a regular subscription fee to use the full feature set.
- **Usage based:** especially for dynamic computing applications where the users pay depending upon task (e.g. computing sources required, time required to complete the task etc).

The service providers are adept at integrating these cloud solutions into the normal user environment, making offline/online interaction as seamless as possible. In many cases they also lower the barriers to entry for new players who would have otherwise not been able to afford the high upfront costs of investments. Here, subscription and usage based models offer users the opportunity to scale based upon the performance of the business.

From a sheer usage perspective, cloud based services are increasingly relevant within private and small businesses where they offer similar features to large IT enterprises at a fraction of the cost. However, this is not without its risks since data is stored in the cloud and the provider security and reliability of data availability may be unknown quantities. These have a huge impact – fear of data theft and the dependence on reliable and resilient networks are worries which need to be addressed with high priority. This is even more important for public enterprises which can reduce costs when data is stored in the cloud – but run the risk of having systems infiltrated.

### 2.4.5 Social Media

Social Media is perhaps the fastest growing consumer internet phenomenon today – led by Facebook and others who have secured a worldwide following within a relatively short time-span. Measured by the level of engagement (daily time spent online) and perceived from their sky-high valuations (Facebook $100 bn at IPO), social media is firmly established as a part of daily life.

A classification of these networks can be done on the basis of purpose and customer type (e.g. LinkedIn as a professional network, MySpace for music and content etc). A few of the biggest players are provided as a reference – however, it is important to note that this market is still evolving fast, with new players continuously emerging to challenge the market leaders.

<table>
<thead>
<tr>
<th>Social Media</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Facebook</strong></td>
<td>1.15bn + users (750 mn users via mobile) (2013 est.)</td>
</tr>
<tr>
<td></td>
<td>250 bn photographs uploaded daily (2013 est.)</td>
</tr>
<tr>
<td></td>
<td>10mn + Facebook apps (2013 est.)</td>
</tr>
<tr>
<td><strong>Twitter</strong></td>
<td>500 mn + total users</td>
</tr>
<tr>
<td></td>
<td>288 mn monthly active users (2013 est.)</td>
</tr>
<tr>
<td></td>
<td>60% mobile users</td>
</tr>
<tr>
<td></td>
<td>400 mn tweets daily</td>
</tr>
<tr>
<td><strong>LinkedIn</strong></td>
<td>238 mn + users (2013 est.)</td>
</tr>
<tr>
<td></td>
<td>1.5mn groups</td>
</tr>
<tr>
<td></td>
<td>3 mn company pages</td>
</tr>
</tbody>
</table>

---

Social Media is a global phenomenon which has emerged over the past decade. Asia Pacific is forecasted to have the highest growth rate (both in terms of user numbers and engagement) over the next decade. This is not surprising since China and India are being increasingly targeted. MENA and Africa also show strong growth.

A majority of the Social Media firms use advertising as a major source of revenue. This is not surprising, since once users upload detailed profiles and use them as a basis for interaction, firms such as Facebook can engage in targeted advertisements. This has a greater dollar value from an advertiser’s perspective than conventional media (such as broadcast television). A minority of firms adopts alternative monetization routes such as subscription based and a one time fee – however, this remains the exception rather than the norm.

The emphasis on social media remains user engagement and firms continuously innovate in order to increase the time an average user remains on the site – thus increasing the value for the advertiser. This can be seen in Figure 19.

Figure 19: Facebook Users, Global Estimate

[Data table and chart showing Facebook users growth from 2011 to 2017, with regions categorized as Asia Pacific, MENA, Western Europe, Latin America, North America, and Central/Eastern Europe.]

---

20 www.eMarketer.com
Another impact of Social Media is its use to gather people together for a common cause, enabling grass-roots movements to spawn within a very short time-span. While this is prevalent in most societies it also raises the possibility of manipulating public opinion through social media channels – for whatever purpose. This is very difficult to track and regulate given the relative anonymity of the channels.

Finally, there is the impact on the data traffic caused by these sites – and as data is becoming more and more graphic this is leading to a significant increase in bandwidth hungry data traffic around the world. An example of this can be seen in Figure 21. It is important to note that not only is the amount of content increasing, the size per item (e.g. a photograph) is also increasing as new devices capture images or video in higher resolution.

---

21 Political Activism 2.0: Comparing the Role of Social Media in Egypt’s “Facebook Revolution” and Iran’s “Twitter Uprising”, El-Nawawy, Mohammed, Khamis, Sahar, Cyberorient, 2012
22 Nielsen 2012
2.4.6 Other Internet applications

There are a broad range of internet applications outside the gamut of what has already been addressed. Since the World Wide Web is so pervasive, it is impossible to categorize all the use cases. Those less easy to categorize include:

<table>
<thead>
<tr>
<th>Application</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Engines (Google, Yahoo etc.)</td>
<td>- Users: 1.162 bn (December 2012)</td>
</tr>
<tr>
<td></td>
<td>- Searches per month: 114.7 bn (December 2012)</td>
</tr>
<tr>
<td></td>
<td>- Advertising Revenue: USD 38.6bn (2013)</td>
</tr>
<tr>
<td>Statistics (for Google)</td>
<td></td>
</tr>
<tr>
<td>News and information sources (e.g. CNN, Al-Jazeera etc)</td>
<td></td>
</tr>
<tr>
<td>- Unique Monthly users: 74 mn</td>
<td></td>
</tr>
<tr>
<td>- 2nd most popular news source behind Yahoo</td>
<td></td>
</tr>
<tr>
<td>Crowd sourced content</td>
<td></td>
</tr>
<tr>
<td>- E.g. Wikipedia</td>
<td></td>
</tr>
<tr>
<td>- 36 mn pages</td>
<td></td>
</tr>
<tr>
<td>- 3 bn users (January 2013)</td>
<td></td>
</tr>
<tr>
<td>Gaming (including gambling)</td>
<td></td>
</tr>
<tr>
<td>- USD 92.5 bn market</td>
<td></td>
</tr>
<tr>
<td>- Significant rise in online gambling</td>
<td></td>
</tr>
<tr>
<td>Significant portion of the traffic on the internet</td>
<td></td>
</tr>
<tr>
<td>- 12% of all internet websites</td>
<td></td>
</tr>
<tr>
<td>- 25% of all user generated searches</td>
<td></td>
</tr>
<tr>
<td>- 35% of all internet downloads</td>
<td></td>
</tr>
</tbody>
</table>

Figure 22: Other internet content

If these sectors are considered together a few commonalities emerge:

- Although the internet has numerous sites, the traffic is disproportionately distributed – a few big sites (e.g. Yahoo etc.) command a significant share of all traffic and links.
- There is a large long tail catering to specific niches.
- An increasing number of sites carry video - which enriches the user experience but also significantly increases the bandwidth requirements at the backhaul.

The growth in the overall internet is commensurate with the number of users – which is now over a third of the world's population.

---

23 Wikimedia Foundation
24 Estimated at USD 30bn in 2012 (H2 Gambling Capital)
If we go one level deeper and examine the select areas of interest we find similar trends. In many cases revenue from online sources has already bypassed those from traditional business – the internet simplifies international transactions. An example is that of gaming (gambling revenue) where the online component continues to exhibit a continuous upward trend (Figure 24).

The business models employed vary widely and depend heavily upon the market, customer segment and competition. Different approaches include:

- Subscription based – e.g. for online gaming platforms
- Transaction – e.g. for gambling
- Advertisements – e.g. for many news sites
- Donations – e.g. for many crowd funded platforms (such as Wikipedia)
- Freemium – when basic feature sets are free and advanced functionalities have to be paid for.

---

26 Internet World Statistics
27 Betable, H2 Gambling Capital
3. Major Regulatory Issues

3.1 Introduction

IP technology separates the applications and services described in the use cases from the means of transport. At the transport level major changes have also taken place. The first stage of the internet revolution took place in the wireline environment – the web became available on laptops and PCs, applications such as OTT voice and eCommerce entered the home and the office. The second stage is wireless, and is being driven by the emergence and increasing domination of smart phones. Previously inconceivable capabilities are offered by the internet and its applications to users wherever they are, and there is no end in sight. Market boundaries are breaking down and new players are entering the playing field with innovative business models that were technologically unthinkable until very recently. The sheer volumes being dealt with by the internet are illustrated in the figure below.

This market dynamism has the regulatory world struggling to keep ahead. Just as one issue has been identified the next comes up; a market is finally defined just in time to watch it morphing into something else. The main regulatory challenge is to provide a future-proof framework which maintains its relevance no matter how the market develops. Key words here are technology-neutrality and ex-post rather than ex-ante regulation. Competitive imbalances between traditional providers and new market players must be evaluated and, as far as necessary and possible, be reflected in new regulation. Further, the effects of the convergence of the ICT and broadcasting markets must be examined. A further regulatory trend is towards simplification – the maxime of regulation is that it should only be applied where necessary, and as the markets develop this is less often the case.

Alongside facilitating the development of the communications market to the benefit of the country, the basic rights of individuals and society must also be protected by legal and regulatory measures.

And a last, but vital, aspect of regulation is that it should provide the market players with business security – they must be able to understand and trust the framework in which they work.
3.2 Regulatory issues related to the use cases

OTT Communications

Regulators have weighed in on OTT communications. The main reason for this is that the operators are demanding a regulatory solution to their revenue difficulties and the policy makers are searching for the reason behind the lack of investment in broadband. The big regulatory question has been whether OTT communications are to be defined as telecom services (voice or data) or telecom infrastructure, and thus whether they should be subject to licencing and regulatory obligations (such as legal intercept and emergency call access) or not.

OTT communications make regulators nervous because they are out of control. As long as they are not regarded as telco services, the OTT communication providers also raise a security concern as they are not obliged to facilitate legal intercept. This has led to them being outright banned in a number of countries and to attempts to force the service providers to manage and maintain data traffic in other countries. These tactics have however met with limited success.

Recent revelations that firms such as Microsoft (which owns Skype) gave US governmental authorities access to their applications and data traffic have raised further security issues. Nations see their data sovereignty endangered, but have little leverage over the OTT providers which are registered abroad and thus out of jurisdictive reach.

Newer services such as Snapchat are now emerging where messages (text and graphics) are only available for a limited time-span after which they are deleted from the server. Snapchat, which was launched in 2011, had had over a billion pictures shared by November 2012. This is a new challenge in the context of content regulation due to the time bound nature of the message.

![Figure 26: Number of daily “Snaps” from Snapchat (Mn)](image-url)

[29 Techcrunch, December 2012](http://techcrunch.com/2012/12/05/snapchat/)
[31 Snapchat](http://snapchat.com)
OTT Media
This use case is mainly concerned with the distribution of videos and audio data. This is not a traditional subject for ICT regulation and illustrates a further issue concerning the organization of regulation - the need for a converged regulatory framework for converged service offerings.

In terms of the content being transmitted, copyright issues play an important role. Legacy laws regarding ownership, where content (e.g. DVD, CD) was bought once and then owned (and could be resold), are inappropriate for digital content. While a sizeable share of distributed content is still unauthorized (illegal uploads etc) the percentage of legal content is increasing – thanks in part to simpler, cost effective options offered by the OTT players, and available across multiple devices. Implementation of digital watermarks and limited distribution options have had limited impact. France has introduced tough legislation to try and deal with online transgressions concerning intellectual property rights – content providers are given two warnings and then their internet connection is blocked.

OTT media has also led to a well-publicised consumer protection problem: Most flat rate data plans have a limit on the maximum volume of data allowed, after which a (generally high) volume tariff or throttled transmission speed applies. As improved HD capable devices come on the market and better content is available the streaming of data means that these limits are quickly reached. This has led to cases of “bill-shock” – where users receive astronomical bills as a result of streaming data. How best to resolve this issue is presently an open debate.

eCommerce
In order to be able to participate in online commerce, individuals and organizations have to submit personal data online, which can be of great value to criminal elements. The number and methods of illegally accessing this data are growing rapidly, and the protection of consumer information is an important regulatory issue. Availability is also of great relevance here – interruptions in commercial transactions, or delays in time-relevant transactions, can be costly. These issues can, on a larger scale, also become issues of national security. If hackers access the database of large enterprises, or the availability of the net for commerce is prevented for a significant length of time by a denial of service attack, the very stability of the economy may be endangered.

The convergence of communications and financial services lead here to the question of how to ensure that the requirements of the different regulatory authorities are combined into one joint path of action.

As not just honest citizens can benefit from eCommerce, a further national security issue here is that of surveillance (legal intercept). Where law enforcement agencies previously had warrants to examine the bank accounts of suspects, now access to online financial transactions is vital.

(Cloud) Services
The outsourcing of data storage and/or the use of Software/Infrastructure as a Service expose users to risks as they no longer have physical control of their assets. The resilience of the network is absolutely vital – loss of access to data, or its deletion, can endanger the survival of an enterprise. Where software or infrastructure is purchased as a cloud service this means that network down time is equivalent to down time for the entire company. These aspects represent most significant consumer protection issues.

Data protection is a further issue here – access to the cloud by third parties must be prevented, and the regulator needs to assess whether this is an issue for them or for more general consumer protection legislation. Here again the convergence of different areas of responsibility (communications and data protection), may lead to the need for heightened coordination between different regulatory authorities.

Cloud services are often offered by providers which are located in another country. This may raise sovereignty questions which require adaptations in commercial law. Coordination between the different authorities may also be an issue here.
Social Media
Social media is playing a significant role in defining social interactions. Users are voluntarily disclosing personal data (photographs, preferences etc) which are then mined to serve targeted advertisements. This presents opportunities for new enterprises but at the same time raises concerns about privacy, ownership of data and longevity of data among others. Recent changes by Facebook and Google are examples of such issues – e.g. Google with its latest notification indicates that it would have the right to use an individual’s photograph to endorse a product in advertising to others if the user has recommended a product elsewhere in their search. Additional complexity arises from social media players’ ever-changing terms of use in tandem with their lock-in effect – which forces many users to continue usage and give up ownership of their content. This issue of data portability must be given regulatory attention.

Social media sites have also been the target of sophisticated hacking attacks where personal details including credit card numbers have been stolen. Although hacking is a phenomenon not exclusive to social media, the large amount of personal data stored makes the trend here an especially worrying phenomenon.

Other
The proliferation of internet services is part of a large trend towards an online world. Many of these services are used for entertainment, information and commerce and have been subject to little or no regulation. Where regulatory concerns abound the service providers simply host the site in “friendly” nations e.g. most gambling websites are hosted in small European and Asian countries with less stringent regulations. The same is applicable to adult content. Due to the absence of any consistent world wide standards, anyone with access to a VPN tunnel and an international credit card is able to access the website of his/ her choice – irrespective of the existing laws in their country of residence.

3.3 Summary of the most important regulatory issues
In a recent study the BSA identified seven requirements for internet services and applications to develop optimally in a society. These prerequisites are: privacy protection, information security, cybercrime measures, protection of intellectual property, ensuring data portability, liberalized trade rules, and the availability of the necessary IT infrastructure. Providing the framework to enable these pre-requisites is a government task, implemented to a large extent by the regulatory authority.

We have summarized these seven prerequisites into three main issues. These will be looked at in detail to provide the basis for recommendations concerning regulatory action to be taken in the area of internet applications in the GCC region:
- Consumer security (covering privacy, information security, intellectual property rights, data portability);
- Sustainable business models for telecommunications operators (covering liberalized trade rules, availability of the necessary IT infrastructure);
- National security (covering information security, cybercrime measures).

These issues may have more or less relevance for the individual defined use cases. An overview is given in the table below.

In Chapter 4 each issue is examined in detail. References are used to illustrate leading edge responses to arising problems, in some cases a wide range of international reactions can be seen and here assessments are made as to which alternative is believed to be most appropriate for the environment in the GCC.

---

12 http://www.onenewspage.com/n/Business/74w2qvnfl/Google-to-include-user-photos-in-web-advertising.htm
13 BSA (Broadband Software Alliance) Global Cloud Computing Scorecard Study 2013, www.bsa.org
Summary of the major issues related to each use case.

<table>
<thead>
<tr>
<th></th>
<th>Consumer security issues</th>
<th>Operator business model issues</th>
<th>National security issues</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OTT Communications:</strong></td>
<td>• Reconnaissance</td>
<td>• Uneven regulatory</td>
<td>• Online Surveillance/</td>
</tr>
<tr>
<td></td>
<td>• Denial of Service</td>
<td>playing field</td>
<td>LI</td>
</tr>
<tr>
<td></td>
<td>• Loss of Privacy</td>
<td>• Revenue loss</td>
<td>Content Regulation</td>
</tr>
<tr>
<td></td>
<td>• Malware/Exploits</td>
<td></td>
<td>(e.g. Apps/Service</td>
</tr>
<tr>
<td></td>
<td>• Social Engineering</td>
<td></td>
<td>Blocking)</td>
</tr>
<tr>
<td><strong>OTT media</strong></td>
<td>• Reconnaissance</td>
<td>• Uneven regulatory</td>
<td>• Online Surveillance/</td>
</tr>
<tr>
<td></td>
<td>• Voice: Skype, Viber</td>
<td>playing field</td>
<td>LI</td>
</tr>
<tr>
<td></td>
<td>• Messaging: WhatsApp</td>
<td>• Investment insecurity</td>
<td>Content Regulation</td>
</tr>
<tr>
<td></td>
<td>• Video: Youtube,</td>
<td></td>
<td>(e.g. Service Blocking,</td>
</tr>
<tr>
<td></td>
<td>Vimeo, BBC iPlayer</td>
<td></td>
<td>Content Protection)</td>
</tr>
<tr>
<td></td>
<td>• Audio: Spotify,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Pandora</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Content</strong></td>
<td>• Search</td>
<td>• Revenue loss</td>
<td>• Online Surveillance/</td>
</tr>
<tr>
<td></td>
<td>• News/ articles</td>
<td>• Investment insecurity</td>
<td>LI</td>
</tr>
<tr>
<td></td>
<td>• Crowd-sourced content</td>
<td>• Loss of customer contact</td>
<td>Content Regulation</td>
</tr>
<tr>
<td></td>
<td>• Informative content:</td>
<td></td>
<td>(e.g. Site and Content</td>
</tr>
<tr>
<td></td>
<td>regular websites</td>
<td></td>
<td>Filtering, Blocking)</td>
</tr>
<tr>
<td></td>
<td>• Gaming</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• User-generated content</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Commerce</strong></td>
<td>• Data protection</td>
<td>• Online Surveillance/</td>
<td>• Online Surveillance/</td>
</tr>
<tr>
<td></td>
<td>• Data security</td>
<td>LI</td>
<td>LI</td>
</tr>
<tr>
<td></td>
<td>• Availability</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Services</strong></td>
<td>• Data Protection</td>
<td>• Uneven regulatory</td>
<td>• Online Surveillance/</td>
</tr>
<tr>
<td></td>
<td>• Data security</td>
<td>playing field</td>
<td>LI</td>
</tr>
<tr>
<td></td>
<td>• Availability</td>
<td>• Revenue loss</td>
<td>Content Regulation</td>
</tr>
<tr>
<td></td>
<td>• Data portability/kill</td>
<td>• Investment uncertainty</td>
<td>(e.g. Content Filtering)</td>
</tr>
<tr>
<td></td>
<td>functions</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Social media</strong></td>
<td>• Loss of Privacy</td>
<td>• (Revenue loss)</td>
<td>• Online Surveillance/</td>
</tr>
<tr>
<td></td>
<td>• Malware/Exploits</td>
<td>• (Investment uncertainty).</td>
<td>LI</td>
</tr>
<tr>
<td></td>
<td>• Social Engineering</td>
<td></td>
<td>Content Regulation</td>
</tr>
<tr>
<td></td>
<td>• Social Engineering</td>
<td></td>
<td>(e.g. Content Filtering,</td>
</tr>
<tr>
<td></td>
<td>• Web/ mobile: Facebook</td>
<td></td>
<td>Blocking)</td>
</tr>
<tr>
<td></td>
<td>• Mobile/ IM: Twitter</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© Detecon International GmbH/TRA Bahrain

27
4. Deep Dives

4.1 Security / Cyber Safety Issues

Initially, the internet was designed to create standardized communication between computers, so security was not considered to be a decisive aspect and seemed to inhibit the idea of borderfree communication. However, the net’s architecture, complexity and growing amount of data create vulnerabilities which can be exploited by cyber criminals.\textsuperscript{34} Attackers can, among others, harvest customer data, record conversations or conduct Denial-of-Service (DoS) attacks. In particular, issues around Privacy and Data Protection, continuous Service Availability and the growing threat of Malicious Software (Malware) constitute a real challenge to internet applications and many industry sectors.

\begin{center}
\begin{table}
\centering
\begin{tabular}{|c|c|c|}
\hline
\textbf{Position} & \textbf{Industry} & \textbf{Rate} \\
\hline
1 & Food and Beverage & 205\% \\
2 & IT and Telecommunication & 142\% \\
3 & Retail and Wholesale & 111\% \\
4 & Health Care & 84\% \\
5 & Banking and Finance & 68\% \\
6 & Education & 63\% \\
7 & Government & 58\% \\
\hline
\end{tabular}
\end{table}
\end{center}

\textit{Figure 27: Malware Encounter Rate (October 2013)}


4.1.1 Privacy and Data Protection

One of the negative side effects of the Information Revolution is a loss of data control. As more and more data is processed by information systems the likelihood of accidental or intentional disclosure increases. With regular security breaches of customer records, the erosion of privacy and unauthorized access to individuals’ most sensitive data is now commonplace.
Privacy and Data Protection Laws - international overview

<table>
<thead>
<tr>
<th>Country</th>
<th>Legal Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saudi Arabia</td>
<td>Anchored in Constitution, Telecommunications Law and Anti-cyber Law</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>In Penal code, Cybercrime Law (2005), Telecommunications Law and Constitution</td>
</tr>
<tr>
<td>Egypt</td>
<td>No specific legislation.</td>
</tr>
<tr>
<td>US</td>
<td>A variety of individual laws exist, but most recent attempts to improve data protection for the individual (similar to the EU draft) were blocked and are now frozen.</td>
</tr>
<tr>
<td>EU</td>
<td>Data protection package has been agreed by the European Parliament and regulations and directive now being discussed. This draft is leading edge in its current state. How much of it remains intact after negotiations between the Member States remains to be seen.</td>
</tr>
</tbody>
</table>

Privacy and data protection issues arise particularly with the use of OTT Communication (VoIP/IM), eCommerce, Cloud Computing Services and Social Media. These will be described in the following sections.

Attackers can easily eavesdrop into Voice over IP (VoIP) conversations and Instant Messaging (IM) services, as many OTT Communication solutions do not support encryption. In addition to the obvious problem of confidential information being accessed, the use of unencrypted VoIP and IM communication channels also facilitates identity theft or fraud. Another threat concerns traffic analysis, which involves determining who is talking to whom. Such information can be beneficial to cyber criminals preparing an attack, e.g. for committing corporate espionage.

The best technical protection from eavesdropping is the encryption of the VoIP and IM traffic. Off-the-Record (OTR) Messaging, a cryptographic protocol, allows private instant messaging conversations. Several applications offer IM self destruction features. Intrusion Prevention Systems (IPS) are useful in detecting an attack and blocking traffic from an attacker.35

Privacy and data protection issues are of increasing concern in the United States (US), where the White House and the Federal Trade Commission (FTC) have issued several significant documents since 2011. While these policy proposals do not particularly focus on OTT Communication, they aim to protect personal information processed by internet services in general.36 In October 2013, a General Data Protection Package was agreed on by the Civil Liberties Commission in the Parliament of the European Union (EU) to achieve better harmonization and strengthening of the data protection framework. The package consists of two draft laws: a general regulation covering most personal data processing and a directive for transposition into national law covering the prevention, detection and prosecution of criminal offences related to data processing. The drafts set privacy/data protection guidelines for new technological developments, which also includes a dedicated “right to be deleted”. In particular, this regulation extends the scope of the EU data protection law to organizations outside the EU if they process personal data of EU residents. Negotiations are now to take place with the Member States and agreement is hoped to be reached in Spring 2014. Following this the Member States will have 2 years to bring the regulation into effect and transpose the directive into their national law.37

36 Further details on these policy proposals are outlined in the section regarding “Social Media” in this chapter.
In order to participate in eCommerce users must register and consequently companies offering eCommerce services are in possession of vast amounts of online data about customers. This data is a valuable asset for implementing targeted marketing promotions. The main threat scenarios involve customer databases being hacked, careless handling of sensitive data, or the misuse of data intended for other purposes. eBanking services are subject to specific financial sector regulations/ licensing procedures which are beyond the scope of this report.

For data security the technical measures given above can also be applied here, with the addition of authentication and anonymisation tools. Furthermore, organizations must set up a secure environment for conducting electronic business, which needs to be protected by a state-of-the-art security architecture (e.g. firewall, virus scanner, encryption).

Provisions for privacy and data protection can reinforce user confidence in eCommerce, and can be used as a competitive advantage for enterprises. The proposed EU General Data Protection Regulation (GDPR) regulates the processing of personal data, balancing the need for a free flow of data within the EU and security requirements using the legal principles of transparency (right for information and consent), legitimate purpose, and proportionality (regulating excessive collection of personal data). Similarly, the Swiss Data Protection Law lays down rules for the processing of personal data by companies, allowing certification of personal data processing systems and encouraging companies to designate a data protection officer.

The Telecommunications Regulatory Authority (TRA) of UAE last published a “Privacy of Consumer Information Policy” in May 2005. While aspects considering protection of personal data and privacy are specified within the Penal Code, Cyber Crime Law, Telecoms Law and the Constitution of the United Arab Emirates (UAE) at a federal level, there is no specific data protection regulation in place.

The telephony market in Egypt is mainly governed by the Telecommunications Regulation Act (Law No. 10/2003), introduced in February 2003 to oversee the development of the market and the introduction of competition. There is no law or regulation in place concerning cyberattacks / malicious hacking. There are some general articles in the laws (e.g. Penal Code) which cover data protection and data privacy and a “Consumer Protection” policy on the TRA Egypt website. Still there is neither a law regulating protection of personal data nor is personal data defined.

The Sharia (Islamic law), as interpreted and applied in Saudi Arabia, establishes privacy as a right based on the dignity of the individual. Moreover, the Saudi Constitution (Basic Law of Governance) repeatedly makes mention of the right to privacy. The Constitution guarantees, for example, the privacy of telegraphic and postal communications, as well as that of telephonic and other means of communication. At the same time, it prohibits surveillance or eavesdropping of such communications (Art. 40), except as provided by law (e.g. in the case of a threat to national security).

Based on the Saudi Constitution, and elaborating on basic Sharia, data-related legislation in Saudi Arabia has focused on privacy violations relating to telecommunications and information technology. For example, the Telecommunications Act, issued under the Council of Ministers Resolution no. 74 (2001), prohibits internet service providers and telecommunications companies from intercepting telephone calls or data carried on public telecommunications networks (Art. 37.7). It also prohibits intentionally disclosing the information or contents of any message intercepted in the course of its transmission, other than in the course of duty (Art. 37.13), e.g. where law enforcement is required to investigate criminal activity. Similarly, the Anti-Cyber Crime Law (2007) and The Basic

---

Law of Governance (1992) impose heavy civil and criminal sanctions for spying on or intercepting personal data, including the reception of data transmitted through an information network without legitimate authorization and illegal access to databases or computers to modify, delete, damage, or redistribute private data. The laws should guarantee that the privacy of all means of communication shall be inviolate, and their contents are reflected closely in the draft Information Technology Crimes Law being discussed in Bahrain at present.

However, legal provisions alone are not sufficient to ensure privacy and data protection in eCommerce. An important aspect is heightening users’ awareness – here we see an important role to be played by the application services providers and the regulator.

While Cloud Computing provides many performance, accessibility and cost advantages, it also raises major privacy and data protection issues. In some cases, a lack of transparency makes it impossible for the cloud customer to effectively check the data handling practices of the cloud provider and thus to be sure that these are in line with the law. The security concerns affect both private use and outsourcing for organizations:

1. Loss of control over data: Because of the cloud services’ global network architecture the exact location of the data is often not known to the user.
2. Unauthorized access to data: In many cases, data in the cloud is not located in the data owner’s country of residence, making prevention of access very difficult.
3. Lacking isolation of data: The concept of cloud computing allows that different users process their data in the same cloud (multi-tenant architecture).
4. Deletion of data: Adequate and timely deletion or wiping of data is difficult to control, and may be impossible because the disk to be destroyed also stores data from other clients.

From a technical point of view, cloud customers need assurance that providers are following sound security practices. These practices should include personal and operational security, identity and access management as well as Business Continuity Management (BCM). Cloud users should make sure that they are given the right to audit the cloud provider’s premises.

From a regulatory point of view, attention should be paid that cloud service providers (which are often also network operators) offer sufficient technical and organisational security and are compliant with local law. Each country has unique legal requirements concerning access to and storage of data. Swiss data protection law, whose basic principles are in line with EU law, highlights three issues with regard to Cloud Computing: (1) the conditions under which the transfer of personal data processing to third parties is permissible; (2) the conditions under which personal data may be sent abroad; and (3) data security. It is permissible to enlist the support of third parties for data processing, but the data controller remains responsible for the processing of data. Transfer of personal data abroad is permitted if the target country legislation ensures standards in line with Swiss law. Over and above these legal measures, increasing awareness of the risks among users is a regulatory task. In the UAE personal data may be transferred to third parties outside of the UAE if the affected residents have agreed in writing. There are no specific provisions under UAE Federal Law regarding security measures to prevent unauthorized disclosure of personal data. In Saudi Arabia, there is no specific law dealing with privacy or personal data and there are no restrictions on the transfer of personal data out of the country.

---

Many of the most popular Social Media (such as Facebook, LinkedIn or MySpace) have significant data privacy problems, as shown in a recent study conducted by the German based Fraunhofer Institute. By providing personal information online users expose themselves to multiple risks e.g. identity theft, stalking, publication of personal or confidential information. Another issue in the context of data privacy is the ownership of data. Many Social Media providers view fan pages and the data provided there as their property. As a result some industry watchdogs now recommend that enterprises shut down their Facebook fan pages and remove “like” buttons from their websites.

As most of the data protection issues related to social networks result from the input of personal data by the users themselves, technical prevention methods are generally not practicable.

In the US, privacy laws and principles of self-regulation usually require a precollection notice and an opt-out choice for the use and disclosure of personal information. Several policy proposals aiming at better protecting users’ right to choose whether or not to be tracked by a third-party website have been made since 2011, commonly known as “Do Not Track” proposals. In 2011 and 2012, there were several bills introduced around this issue. All proposals aim at improving and protecting consumer online privacy. Despite pressure from the Federal Trade Commission (FTC) and Congress, the US online advertising industry has missed the finalization of a Do Not Track proposal, describing an opt-out solution regarding the use of personal data, further postponing its implementation. The revised data protection framework which is being negotiated in the EU includes proposals to harmonize data protection standards throughout Europe, give users of internet services the right to determine whether their data can be tracked/profiled or not, provide them with the transparency to see what happens to data that they input, and the ability to correct information stored.

Maybe the most important regulatory policy here is to encourage self-regulation and support activities to raise users’ awareness of the consequences of careless data handling. Apart from understanding and adapting the security and privacy settings on Social Media websites, several privacy software and web browser extensions are available which help users to maintain privacy online. These applications encrypt communication, prevent tracking, allow adjustment of the notification settings on profiles and accounts, and scan web browsers to determine what information is being shared with websites.

4.1.2 Service Availability

Human error, criminal acts (fraud, theft or espionage) or natural disasters (such as floods, earthquakes or pandemics) can cause the failure of production services and, in extreme cases, the loss of customer service or sensitive data. In July 2001, for example, Microsoft experienced a three-day outage of its Instant Messaging Service (MSN Messenger), which affected more than 10 million users. According to Microsoft, the reason for the outage was a very rare set of circumstances and it took a week to fully resolve the problem. With the growing dependency on the internet, the number of possible threats to individual users and organizations increases. Risk is compounded further because business partners, customers, employees, contractors and hackers have increased access to an organization’s IT infrastructure.

49 https://www.datenschutzzentrum.de/presse/20110930-facebook-enforce-privacy.html
The loss of availability of Internet services is most critical with regard to OTT Communication (VoIP/IM), but also eCommerce and Cloud Services. The impact on the other use cases is of little regulatory significance and therefore not covered in this report.

Apart from physical disasters impacting the technical infrastructure, targeted attacks on OTT communication services have become a serious threat. With a so-called “Denial of Service” (DoS) attack, an attacker can shut down an organization’s services, by directing large volumes of traffic in order to exhaust processing resources or network bandwidth. By gaining control of a large number of VoIP-capable hosts and forming a network, an attacker can launch a so-called “distributed Denial of Service” (dDoS) attack. Each computer under their control directs thousands of messages to a single server, which disables the victim’s computer due to resource exhaustion.56

Alongside the security issues, there are particular business continuity issues that apply to the eCommerce environment. The focus is on preventing interruptions in the customer or business partner’s service or process. On 20 August 2013, the European Union Agency for Network and Information Security (ENISA) issued a report summarizing major outage incidents on electronic communication networks: of 80 reported incidents in the EU in 2012, almost 40 percent concerned problems with accessing the emergency service number.57

Despite employing architectures designed for high service reliability and availability, cloud computing services experience outages. In 2011/2012 major cloud service providers suffered significant outages which led to data loss and down time for their users. Besides loss of reputation, the damage caused a loss of customers.58 In such cases the remedy for the customer may well be to change the cloud service provider, but currently there is a lack of tools, procedures, standard data formats or service interfaces that could guarantee data, application and service portability.59

---

59 This makes it difficult for the customer to migrate from one provider to another or back to an in-house IT environment – a so-called lock-in effect.
In order to prevent outages, Business Continuity Management (BCM) can help ensure the reliability of infrastructure, processes and detection potential. International organisations and governmental bodies in various countries have drawn up regulations, guidelines and recommendations in the area BCM. In April 2013, the Swiss Financial Market Supervisory Authority (FINMA) determined appropriate BCM as a prerequisite for granting an operating licence according to the Banking Act. In Switzerland, responsibility for BCM lies with the Board of Directors and Senior Management of each individual organization. In the UAE, the local TRA has issued a Business Continuity Directive requiring that licensees have business continuity planning measures in place. The Saudi Arabian Money Agency also defines business continuity requirements for financial service providers.

4.1.3 Malicious Software

The threat of malicious software (malware) has changed dramatically as attacks have become more targeted, more frequent and harder to detect. Malware includes programs such as viruses, worms, spyware or trojan horses that are covertly inserted into programs to destroy data, run destructive programs, steal sensitive information, or compromise the security of a victim’s data. The sources of malware or phishing attempts are varied, but one of the biggest problems is spam email. Not only are attacks growing in number, but they are becoming increasingly targeted. Although most attacks still target PCs, mobile devices, smart phones and tablets have come under increasing pressure in recent years.


Figure 30: Top Web Malware Types (2012)

---

60 In the US, several bodies, like the National Fire Protection Association (NFPA), Federal Financial Institutions Examination Council (FFIEC) or the North American Electric Reliability Corporation (NERC), provide BCM guidelines.


64 Internet Security Threat Report 2013: 7


With the growing popularity of VoIP and IM services, the spread of malware has become an increasing problem for **OTT communications**. The substitution of PSTN telephony by VoIP means that these security threats cause even more concern.\(^6^7\) Malware can spread over VoIP as easily as email and it can be assumed that it can spread even more readily via IM.\(^6^8\) The Skype worm, for example, is malware spread through IM over Skype which stops access to security tools and blocks the infected user.\(^6^9\) Service theft can be conducted by “Phreaking” (Phone hacking), a type of hacking that steals service from a service provider, or uses services while passing the cost to another user. Another threat stems from Spam over Internet Telephony (SPIT) which, as it is classified as social engineering, is hard to identify. A subtle variation of SPIT called Vishing (VoIP phishing) collects personal data by redirecting users toward an interactive voice responder that asks for personal information.\(^7^0\)

**Social media** networks have become a major channel for the dissemination of malware. Current security research reports show a significant increase in spam and phishing on social media sites, enabling the rapid spreading of malware.\(^7^1\) Cyber criminals use very sophisticated ways to persuade social media users to unconsciously download a virus. Some malware attacks create dangerous domino effects, such as hacked Twitter accounts sending malicious links to followers. This type of malware can also be found in recent Facebook survey scams.\(^7^2\)

Technical measures for regulating VoIP/IM services and social media websites include their filtering, blocking or cutting off certain unwanted functionalities on the part of the Internet Service Providers (ISPs). With firewall settings or proxies, the ISPs can regulate the access to certain OTT services. Apart from implementing technical measures legal actions can help contain this security issue, but the question of net neutrality requires consideration. In 2007, a new paragraph was added to the German criminal code, stating that the production, acquisition or dissemination of measures enabling access to data or software for committing an offence, shall be liable to imprisonment or a


\(^{72}\) One of the most effective social malware menace was the Koobface program. Koobface targets social media users with fake messages from friends or other contacts, which contain links to malicious web sites where they will be offered a Flash update. By way of downloading the update, the user's system will become infected with malware that allows cyber criminals to use the computers resources to their botnets. [http://www.faronics.com/news/blog/study-social-media-malware-on-the-rise/](http://www.faronics.com/news/blog/study-social-media-malware-on-the-rise/) (accessed 11.10.2013).
Saudi Arabia’s Anti-Cyber Crime Law (2007) also punishes unlawful access to computer systems. In the UAE, the Cyber Crime Law of 2006 defines any action which destroys or unveils secrets and discloses personal or official data, as illegal. The TRA in the UAE has issued policies, rules and regulations to guarantee the end users’ privacy, security, quality of service and content access management. Examples are “Quality of Service Regulatory Policy” or “Privacy of Consumer Information Policy”. In 2008 the TRA (UAE) issued their regulation policy on “Internet Access Management”. This consists of certain frameworks and categories which must be taken into consideration by internet service providers to ensure the security of the internet and protect end users from harmful websites containing materials that are contrary to religious and ethical values of the community of the United Arab Emirates.

While the UAE obliges the ISPs to eliminate the transmission of spam, no regulations are imposed on sending unsolicited e-mails (spam) in Saudi Arabia. Several media websites, government portals and organizations in Saudi Arabia have been subject to cyber attacks in recent years. In 2012, Saudi Arabia’s national oil company, Aramco, was the subject of a cyber attack aimed at stopping oil and gas production at the biggest OPEC exporter. There is an Anti-Cyber Crime Law currently in place which is enforced by the CITC (8 Rabi 11428 / 26 March 2007), still it seems more effort is needed to empower the law and identify security measures to efficiently and rapidly counter potential attacks. To reduce the extent of malware attacks, it is possible for ISPs to block access to specific services or websites known for the dissemination and provision of malware. Similarly, companies can block specific services, like OTT voice or social media websites or their IM services. Here again, it is key that the users understand the social media environment and how the various social media platforms work. A big part of minimizing risk is educating users and providing guidance on how to avoid or minimize dangers.

4.1.4 Options for managing the use of OTT from a security point of view

OTT applications present a particular security challenge. A number of options concerning their regulation from a security perspective are outlined below.
• **Absolute ban.** Banning the use of OTT services is one possible approach. While a strict enforcement of such a ban may indeed contribute to a reduction of risk, it also deprives the economy of the benefits of OTT services (see chapter 2). Strict enforcement is also easier said than done in the internet world – where finding workarounds is seen as sport. As such, this measure is hardly feasible to implement and also conflicts with the concept of a free market economy.

• **Technical measures.** Restrictions on the use of OTT services are often enforced using technical measures. This may be the simple blocking of relevant web sites or more complex OTT-specific tailored solutions. For instance, access to specific VoIP services can be allowed while blocking the sending of file sharing services via Instant Messaging. Content-based filters are very effective in preventing the leakage of sensitive information.

• **Monitoring and audits.** In order to determine whether OTT services are being used according to the requirements of existing regulations, monitoring and audits are very effective. Companies should be encouraged to monitor activities within their networks to detect any violations and prevent their recurrence or reduce damage caused. Proper documentation of the monitoring/ control of OTT services can be used as evidence of compliance. Monitoring the private use of OTT services at home is not recommended as it conflicts with basic human rights (freedom of speech).

• **Legal and Regulatory Framework.** The nature of the OTT providers’ business models makes them extremely difficult to regulate specifically as communications providers. As international companies they are also often beyond the jurisdiction of the country in which they do business. General civil and criminal law can be applied to control their behavior within a particular jurisdiction and the international trend is towards the introduction of more far-reaching data protection and cybersecurity laws which address the new challenges posed by the internet – specifically its international nature. In Bahrain, a specific law has even been introduced to deal with the regulation of Bulk Messages (i.e. spam).  

• **Awareness Measures.** Trust in the users’ own sense of responsibility is justified when they know how to use OTT services safely. Lack of knowledge, misunderstanding and inadequate awareness of security risks can lead to the unintended leakage of critical data. The threat from the inappropriate use of OTT services can be greater than that of malicious intent. Ensuring that users are sufficiently aware of the opportunities and risks is regarded as one of the most vital and practicable measures that the regulator can take. The development of an overall awareness program to cover all user groups and including continuous, repeated activities is recommended.

4.2 Effects on the operators’ business models

The proliferation of IP-based telecommunication networks has facilitated the decoupling of application and network layers and enabled OTT providers to deliver their content and applications directly to end users - circumventing the owner and operator of the underlying ICT infrastructures, reducing their function to the well-known term “bitpipe provider”.

---

Thus telecommunications operators ("telcos") not only have decreasing knowledge and control of the kind of content and applications their networks are carrying, but the amount of data going through their pipes is growing exponentially, forcing them to build even faster networks, which opens them up to even more OTT traffic, eventually trapping them in an endless loop.

4.2.1 The uneven regulatory playing field

The speed with which the internet application market has developed has created an imbalance in the regulation of different actors competing in the market, particularly concerning the application providers with the OTT communications use case.

A common complaint from network operators is that their business models are determined to a large extent by regulatory requirements, whereas those of the internet application providers (and particularly the OTT players) are free of such limitations. The table below summarises the regulatory imbalances as seen today.

<table>
<thead>
<tr>
<th>Area of regulation</th>
<th>Network operators</th>
<th>Application providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Licensing</td>
<td>Yes, individual licences – sometimes still technology-specific, but often subject to reform. As operators are generally defined as having SMP, the need for licences is expected to persist.</td>
<td>Class licences common. OTT providers often exempted.</td>
</tr>
<tr>
<td>Interconnection</td>
<td>Yes, due to general definition of operators as having SMP. Requirement to interconnect produces costs.</td>
<td>No. OTT providers are per definition “over the top” of the network, and don’t require interconnection.</td>
</tr>
<tr>
<td>Provision of legal intercept</td>
<td>Required as a licence condition.</td>
<td>Required in some cases. Legislation introduced or being developed in nearly all countries.</td>
</tr>
<tr>
<td>Access to emergency services</td>
<td>Required as a licence condition for basic service offers (PATS).</td>
<td>Required in some cases. Peer-to-peer providers generally exempted.</td>
</tr>
<tr>
<td>Quality of service</td>
<td>Yes. Licences include requirements for SLAs.</td>
<td>No. The internet technology makes contractually determined QoS difficult. QoS (specifically speed) problems generally blamed on network provider, not service provider.</td>
</tr>
<tr>
<td>Net neutrality</td>
<td>Assumes “best effort” transport of data without discrimination, independent of source or nature of data. Concept not applied in MENA and being reviewed at present in other regions (eg EU).</td>
<td>No obligations. Their control over the content and freedom of choice concerning customers releases them from restrictions here.</td>
</tr>
</tbody>
</table>

The question of if and how to license new market players has occupied regulators for more than a decade. The clear distinctions between different technologies and players are a thing of the past and basic assumptions which were valid for licensing in the 1990s are irrelevant now. Definitions are the name of the game when determining who should be regulated and how. Is, for example, an OTT voice provider a provider of voice services? Skype has a very clear position here: “Skype does not have any operations in Singapore [author’s note: or anywhere except Luxembourg]. Users of Skype simply download the Skype software from our Luxembourg operated website...”

---

80 Letter from Skype to the iDA on the subject of network neutrality, 27.12.2010
Many regulatory authorities agree on the condition that no connection to the PSTN is made. Canada has chosen a technology-neutral policy, equating VoIP providers with traditional voice operators as long as the service is offered through access to the public switched telephone network. In Singapore the iDA has opted to introduce specific service licences which cover VoIP services connected to the PSTN network. Peer-to-peer providers are not included here – they are simply subject to normal competition law. In the US the FCC has made an active decision not to licence ISPs or service providers to encourage the further development of the internet application market, but they do subject these providers to certain requirements – such as the supply of emergency call access by VoIP suppliers whose customers can receive calls from or place calls to the PSTN, and an obligation to inform their customers of their capabilities/limitations concerning emergency service access (known as E911).81

In the EU long discussions have taken place concerning the definition of Electronic Communications Networks and Services in the converged world and the treatment of VoIP providers. The EU’s new regulatory framework82 has loosened regulations on the players and these are generally technology-neutral, but a wider range of players are subject to the remaining obligations. More recently a slight withdrawal from the “light” regulation trend in Europe can be seen, as the subject of security is becoming more prevalent.

According to the UAE TRA’s VoIP policy V2.0 (2009), VoIP companies need to approach and collaborate with the licensees to legally provide their services. The same applies for the provision of OTT services. The new guidelines deem IP telephony as a regulated activity as per the Federal Law by Decree No. 3 of 2003 (Telecom Law), and as such the provision of services is restricted to the country’s licensed telecoms companies. Only OTTs which partner with the ISPs can provide their services, all other OTT voice services are banned.

---

82 2002 New Regulatory Framework, EU

---

<table>
<thead>
<tr>
<th>Treatment of OTT Voice Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Singapore</strong></td>
</tr>
<tr>
<td><strong>US</strong></td>
</tr>
<tr>
<td><strong>EU</strong></td>
</tr>
<tr>
<td><strong>UAE</strong></td>
</tr>
<tr>
<td><strong>Egypt</strong></td>
</tr>
<tr>
<td><strong>Saudi Arabia</strong></td>
</tr>
<tr>
<td><strong>Kingdom of Bahrain</strong></td>
</tr>
</tbody>
</table>

Figure 34: Summary of the international treatment of OTT voice providers
In Egypt, there is no specific legislation for the provision of IP telephony services and voice over internet protocol (VoIP) is currently treated as a standard fixed line telephony service. The National Telecommunications Regulatory Authority (NTRA) is understood to be in the process of formulating new legislation for the governance of VoIP services which is expected to provide for licensed ISPs to offer full VoIP. In March 2010 the NTRA confirmed that the country had begun enforcing a ban on international calls made via mobile internet connections. Clarifying the situation, Amr Badawy, executive president of the NTRA, said: ‘The ban is on Skype on mobile internet, not on fixed, and this is due to the fact it is against the law since it bypasses the legal gateway.’ Under existing regulations all international calls must be routed via Telecom Egypt’s network. Despite mentioning Skype by name, it was suggested that the regulator could extend the ban to other services, with the authorities noting: “We are targeting any illegal voice traffic on the mobile (internet)... outside the international gateway...” It remains unclear whether such a restriction will be extended to fixed line internet connections.”

In Saudi Arabia, there have recently been discussions about banning some OTT providers. The telecoms regulator (CITC) has threatened to block messaging apps over security concerns according to local news magazines. The CITC is pushing the country’s mobile operators to work with the app providers so that messaging can be monitored. In June 2013, the authorities in Saudi Arabia did ban use of communications app Viber, warning that it will “take appropriate action against any other applications or services if they fail to comply with regulatory requirements and rules in force in the Kingdom”, according to Reuters. Saudi Arabia’s three main operators were reportedly asked by CITC whether they were able to monitor or block such applications.

Bahrain’s present attitude towards OTT voice is liberal in comparison to its neighbours. Although not officially permitted by organizations other than voice license holders (international or national), legal consequences are only to be expected if the foreign provider actively markets services in Bahrain.

Attempts to impose regulatory obligations on application providers reveal that there are technical differences which work against attempts to unify approaches.

The very nature of IP communications means that the VoIP connections are often location-independent and the reliance on a functional electricity supply makes them inferior in some disaster scenarios. In an attempt to encourage OTT voice providers to participate in legal intercept and emergency call access the UK offers them geographic numbering if they agree to behave like telcos and provide these services – otherwise they are assigned numbers from a specific range which is clearly identifiable as not being “normal” telephone numbers (as is the standard in Singapore). It is questionable whether the OTT providers regard the different numbering as a real problem, or reason enough to take on the costs of the obligations. The European Regulator Group’s common position on VoIP recommends that geographical numbers for traditional telephony services and geographical numbers for VoIP services should share the same number range, i.e. come from a common “number pool”.

Transmission over the internet is completely different to that via a PSTN and the provision of end-to-end quality of service cannot be guaranteed. The concept of best effort provision has generally been accepted by the customers, but as dependence on online services grows it is doubtful that this will remain the case.

Here the issue of net neutrality must be considered. This has always been a given for the internet – all traffic is to be treated equally, irrespective of source, destination or content – and is generally the solution that the content providers prefer. But it means that most operators are not allowed to differentiate between traffic for which they receive income and traffic which brings them no economic benefit, nor can they differentiate their products by offering superior quality of service with faster transmission rates and reduced latency. This is of limited relevance as

---

81 The Reuters report commented that the decision made by the CITC is also because these applications remove revenue for calls and texts from licensed operators.
84 ERG COMMON POSITION ON VoIP ERG (07) S6rev2 December, 2007
long as there is over-capacity, but in the case of bottlenecks the story is different. This issue has been recognized as a priority and first changes have been made – OFCOM (UK) has announced its intention to allow managed services in the case of network congestion – but then all services of a particular type (eg video) must be stopped at the same time to prevent competitive disadvantage. This approach suggests great regulatory involvement – how, for example, is “congestion” to be defined? In 2010 the iDA in Singapore reviewed its stance on network neutrality and came up with the following policy framework:85

1) Operators are not allowed to block legal content;
2) They must always comply with competition and interconnection rules;
3) They must disclose information to the end-users about their network management practices and typical internet broadband download speeds:
4) They must meet minimum QoS standards as defined in their licences; and
5) They are allowed to provide niche or differentiated services.

In accompanying commentaries it is emphasized that these niche or differentiated services (which may include network management services) are not a replacement for non-discriminatory internet access, but an additional service. An interesting comment from Skype86 was that the regulator should where possible “put network management in the hands of the user” The technical practicality of such an option would have to be assessed in detail. The network operating company in Singapore now offers 4 Classes of service: A. Real time; B. Near real time; C. Mission critical and D. Best effort. The regulator puts a special emphasis on the need to educate and inform the end-users, and is also considering a so-called “cooling down” period post contract signature, which enables end-users to withdraw from a service provision agreement within (say) 2 weeks should they be dissatisfied with the traffic management offered by the supplier.

A further use case benefitting from regulatory imbalance is OTT media. Here it is the traditional broadcasting companies which are subject to strict content and copyright restrictions while the OTT media providers enjoy comparative freedom. The situation here is further complicated by the convergence of ICT and broadcasting issues – which is leading to the logical convergence of the different regulatory instances e.g. in the UK – where OFCOM has been established as the result of the convergence of the ICT regulator (Oftel), spectrum management (RA), the regulator for private television (ITC), the standards commission (BSC), the regulator of independent radio services (Radio Authority) and the overseers of the BBC. In this way consistency in the treatment of different cases can be guaranteed and competence discussions avoided from the outset. In Singapore there are still separate authorities regulating communications and broadcasting, but both are under the auspices of the same ministry.

Finally, data portability is a regulatory aspect which may aggravate present imbalances if not correctly handled. This concept is akin to that of number portability and is intended to protect consumers from lock-in effects, especially in the case of cloud data services. Although a positive concept in terms of consumer protection, its implementation must be planned carefully to ensure that all market players, whether network operators, ISPs or application service providers, are subject to data portability requirements and thus to prevent a distortion of competition. The EU is dealing with this by including data portability as a consumer right in revised data protection legislation – in this way all companies will be equally subject to the legal requirements.87

While some of the imbalances felt by the network operators stem from imposed regulatory obligations, others are in fact simply normal market developments for which regulatory action is inappropriate. Regulatory action which distorts competition is contrary to international developments in regulatory practice and its justification must be examined in detail.

85 www.ida.gov.sg/.../Consultation-on-Policy-Framework-for-Net-Neutrality
86 Letter from Skype to the IDA on the subject of network neutrality, 27.12.2010
4.2.2 Revenue loss

One of the bigger challenges of the internet is that since it lowers barriers to entry and leverages global economies of scale it is increasingly difficult for traditional firms as well as localized entities to compete with the new market players. For example – an OTT Media player who has a global presence will benefit from lower costs per MB for storage and hosting and be able to negotiate better content deals with providers in comparison to small specialized local players. However, the OTT media player’s business model is only possible using access provided by regulated operators and thus this revenue loss must be part of any equation concerning wholesale price levels.

A further problem for some nations’ economies arises since the internet application provider can be located anywhere in the world – independent of geography - and the macroeconomic benefits of the business are only enjoyed in their land of domicile. National governments which raise corporate tax (Bahrain and UAE are excepted here) are losing tax revenue since users are purchasing services from global players rather than local entities, there are no employment benefits in the host country and also no knock-on effects from the business as such. Although the tax issues are being debated at an international level and can be seen as a globalization and structural shift problem – they are not a subject that should be the focus of regulators.

<table>
<thead>
<tr>
<th>OTT Comms</th>
<th>OTT Media</th>
<th>Content</th>
<th>Commerce</th>
<th>Services</th>
<th>Social Media</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategy</strong></td>
<td>Substitute trad. Telco services with low/no pricing strategy – once market share gained, pricing models expected to change</td>
<td>New services enabled by internet. Provide videos and music on demand. Substitute for MP3/CDs/radio/video shops/payTV</td>
<td>New services enabled by internet network effects. Gaming substitute for &quot;trad&quot; gaming</td>
<td>Marketplaces. Substitute/add’l sales channel for trad. Shops; Facilitate intra-commerce. Facilitate int'l payment</td>
<td>Outsource IT storage and provide alternative bus. models for software/platform/infrastructure provision. Substitute trad. business models</td>
</tr>
<tr>
<td><strong>Target customers</strong></td>
<td>Private users; Expanding into business users with VoIP now</td>
<td>Private users</td>
<td>Private and corporate users.</td>
<td>Businesses and private users B2C</td>
<td>Mainly Businesses B2B; Private users too</td>
</tr>
<tr>
<td><strong>Revenue sources</strong></td>
<td>Services often free of charge; Connection to PSTN against payment; M’annual subscription fee</td>
<td>Basic services often free of charge; Advertising; Subscriptions; Pay per use</td>
<td>Advertising (targeted due to knowledge of user); Pay per click; Auctioned key work references</td>
<td>Margins</td>
<td>Volume-based pricing; Time-based pricing; Subscriptions</td>
</tr>
</tbody>
</table>

![Figure 35: Business models of Internet Application Providers (Source: Detecon)](image_url)

As illustrated in the above summary of the business models behind the OTT use cases – the majority of providers presently concentrate more on winning customers than on making money. By using infrastructure paid for by the consumer within the framework of flat-rate data plans the costs are kept to a minimum and the investors’ valuation of the business models ensures that capital is available. This model is the kiss of death for many more traditional telco services for which the consumer has to pay on a per-use basis, but which offer no apparent advantages over their free alternative. This is particularly so in the case of VoIP services (competing with voice services – specifically with international voice) and messaging services such as WhatsApp (competing with SMS). When Skype first took off in the UK, several network operators blocked its use as they saw their revenues in danger – but OFCOM and the EU intervened and used net neutrality as the argument to make them provide access again. Recently OFCOM and other regulators have begun to distance themselves from absolute net neutrality by publically acknowledging the need for capacity management through both price differentiation and traffic differentiation in peak periods – which
indicates that they recognize the issues that the network operators are facing. International voice has long been an important source of income for telcos, often cross-subsidizing local calls subject to tariff regulation. SMS is often quoted as THE killer application – but now the “free” alternative is undermining revenues dramatically.

In Figure 33 it can be seen that worldwide SMS traffic is forecasted to peak by 2014 and then decline. If the same analysis is limited to developed markets, the SMS/IP substitution has already crossed 25%. A clear impact can be seen in the case of the Dutch operator KPN who analyzed this trend in the Netherlands.

According to research, every 10% increase in smart-phone penetration reduces voice and messaging revenues by 0.5 – 0.6%
The telcos are losing revenues, but no one is gaining them. This is destructive competition resulting from the flat rate business models, and as time goes on the internet application market will develop applications to attack ever-increasing parts of the telco market – first international telephony, then national telephony and messaging, then local etc. The telcos should not assume that the attack is temporary and should not have a false sense of security. In a competitive market – which network access is in many countries – this problem should be solved using the principles of supply and demand.

The access providers should rebalance their prices to reflect volume usage. If the customer wants the volume, then they will be willing to pay for it. In many cases the operators will be subject to tariff regulation for their wholesale rates - the regulator will need to take action to rebalance these regulated rates to enable the SMP operators to behave conform to the demands of the market.

Whatever happens, in the long run the OTT providers will also need a strategy to operate profitably.

A promising business model available to the operators, but which has mainly been snapped up by third parties, is the role to be played as a content delivery network (CDN). These providers offer local data storage to the OTT providers so that latency is reduced and the consumers’ joy of service increased. OTT providers pay for these services, so the traditional network operators can monetize the relationship by providing this service – and the skills required are already available as CDNs are a natural extension of the transport business.

A further group in the internet application market which is suffering from revenue loss as a result of the OTT players is that of the content producers. OTT media services provide flat rate music or video streaming: content which was previously supplied on a unit price basis. Following major legal battles concerning copyright issues, new services now seem to be emerging where the media industry is working together with the OTT providers in a way which is less destructive for the industry – offering streaming options and premium pricing for advertisement-free services. The share of illegally distributed music and video is going down.

4.2.3 Investment security

In the short term the consumer is sure to be delighted with the effects that the new players in the market are having. Prices are falling – in many cases to zero over and above the flat rate paid for the internet connection – and the range of applications on offer grows from day to day.

But there is one major flaw in the market as it is today: investments in future networks are high risk. Traditionally carriage and content went together – network operators were willing to invest in network because they knew that they could generate revenues with the provision of content, it was under this premise, and with the expectation that excess capacity would always be available, that flat rate tariff plans emerged. This is no longer true. The telcos are paid flat rates for the use of their capacity and their role is being reduced to that of a wholesaler. At the same time the prices that they are allowed to charge for their wholesale services is often regulated at a cost-oriented and rather restrictive level. The profit and thus the incentive to invest used to come from the ability to redeem payments from service providers using the network – to a certain extent including income from transit agreements – and from income earned with the network operator’s own service and content provision. This is no longer true.
In summary: the services being offered by the OTT providers – particularly OTT media and content provision – are increasing demands on capacity. Due to the predominance of flat rate tariff structures this increased traffic brings no financial benefit for the telcos. The expected market reaction would be for the telcos to change their tariff structures to reflect demand and to cover the costs necessary for new investments – but either the regulation of their tariffs is stopping them from doing this, or they are consciously delaying an improvement in their situation in the hope that the OTT services will be seen as being destructive for the market and will be banned by the regulator. Whatever the reasoning, the present situation – with increased capacity demands and no related income – is not a sustainable model for the telcos.

In the specific case of cloud services this problem is particularly acute. Cloud services need a highly resilient network and the synchronization of data to numerous devices demands significant capacity. This in turn requires investments which are generally only paid back after years. But the increasingly wholesale nature of the telco's business, the international nature of many cloud service providers (giving them access to numerous alternative network operators) and, last but not least, the upcoming demand for data portability combine to ensure that the telco has absolutely no planning certainty concerning the income to be earned if investments are made.

Unless the business models of the market players (mainly the network operators) are adapted to suit the new market structures investments in the network will ebb. This will have knock-on effects on businesses which have learnt to rely on broadband communications for their growth, and thus on the overall economy and the image of the country in question. Adaptations to the business model refer here to the rebalancing of the tariff structures – away from flat rates and network neutrality and towards traffic and/or quality of service-oriented schemes for data.

To enable the network operators to function in a competitive manner it may be necessary to change the regulatory guidelines which they face. Existing regulatory requirements must be reassessed within the framework of the new market situation to re-establish a level playing field and incentives to invest.

Although broadband access markets are generally subject to normal competitive conditions, some nations have decided that measures have to be taken if the development of broadband is to be optimized in their market.

One option is the structural separation of the markets for network provision and service provision. Australia and Singapore have both chosen this option and set up broadband companies specifically to provide nationwide broadband infrastructure. The network operators are then required to sell capacity on a wholesale basis. The rationale here is that the provision of the broadband infrastructure is not a competitive market and will not develop to the benefit of the economy if not supported by regulatory intervention. Such a major intervention into the market can therefore only be recommended if a detailed cost study reveals that a natural monopoly situation exists and such intervention is thus justified.

A further option would be the introduction or extension of existing universal service obligations to cover broadband access – potentially including a funding mechanism for the provision of broadband to be carried by all market players.

---

91 “Broadband” refers to high speed communications technologies – which speed is generally defined as a political objective, e.g. 50 Mbit/s for 75% Households (Germany), 1 Gbit/s for businesses (Bahrain).

92 The National Broadband Network in Australia is to provide 93% of homes, schools and businesses with a fiber-to-the-premises broadband connection of up to 100 Mbit/s. The other 7% are to be served with wireless and satellite connections.

93 The Next Generation NBN in Singapore has separate companies providing dark fiber network and ducts (“Opennet”) and active infrastructure (“Nucleus Connect”), while the services are provided to the users by retail service providers (RSPs).
4.2.4 Customer relationship problems

If reduced to the role of wholesale provider, the telcos will lose customer contact. If broadband capacity is seen as a commodity by the customers, brand loyalty will with time fall to zero. Competition may be purely on the basis of price and the customers will cherry pick from each service offering, behavior which will be further facilitated by consumer protection activities such as data portability regulations and market transparency provided by the internet.

On the other hand, regulatory developments away from network neutrality will enable some differentiation again – particularly in combination with requirements from the regulators that the users are well-informed of the differences in the quality of broadband connections (as in Singapore). As the role played by internet services continues to grow in society, the willingness to pay for high quality and reduced latency will develop in a greater range of customer segments.

The telco can accept its role as a commodity supplier and adjust its business model accordingly to maximize production efficiency to provide broadband connections to the mass market at minimum price, or it can search for options for differentiation in broadband provision and lobby for regulatory freedom to act as a commercial entity. In addition the telco has the alternative of entering into commercial agreements with internet application or content providers to offer, for example, value added packages to the customers with enhanced quality. Many operators have adopted a symbiotic approach with partnerships with the OTT players (e.g. Mobily in Saudi Arabia). In this case, the applications are natively installed on the device, and traffic from these applications is zero-rated when specific bundles are purchased. Although this does not fully compensate for lost SMS revenue, it offers the customers an attractive alternative which may increase loyalty.

Alternatively the operators can compete with copycat services such as the European “Rich Communications Suite” which provides IM, live video footage and files, and presence information across any mobile networks or “Joyn” which offers chat capabilities between partnering networks. Most operator responses with competing services have however had limited market success to date.

Further alternatives could be to enter into service agreements with OTT providers to provide QoS at a price – a possibility now that the concept of net neutrality has been watered down – or to use Apps as a distribution channel for telco services.

The regulator has a very limited role to play here – this is an example of competitive pressure – as experienced by companies in nearly all industries throughout the world on a daily basis.

---

94 Supported by Ideos Claro operators in South America, KT, LG U+, Metro PCS, Movistar, Orange France and Spain, SK Telecom, T-Mobile Germany, and Vodafone Germany and Spain.
4.3 National Security

The market dynamics driven by the proliferation of IP-based (incl. OTT) services and increasing IP data traffic has a three-fold impact on a nation’s cyber security:

1. The lack of visibility into internet traffic traversing different operator networks and international backbone links is a major security challenge for governments as this traffic flow can include any type of data, be it data containing legal or illegal content, applications with rightful or wrongful intent towards individuals, corporations or the government, or data generated in or outside of the country. All OTT content or traffic types referenced in the use cases are being transported in this massive information flow.

![Figure 38: User Traffic Share on Operators’ Internet Networks (Source: Telegeography)](image)

2. With an ever-increasing amount and diversity of data and the continuous evolution of the underlying ICT platforms (wider coverage, more capacity and higher technical sophistication), the efforts and costs needed to regulate content through monitoring and control measures are increasing at a faster pace than the direct costs of the threats themselves.95

3. Technical, legal and regulatory measures introduced or enforced by Government entities, while addressing national online security issues and threats can easily also cause a multitude of controversial effects or public reactions, i.e. perceived impact on user privacy, or on ISP or content provider business models and operations as well as their competitive positioning in the OTT market.

In the context of OTT content and applications, one key national security issue is obviously the natural extension of the consumer security issues described in Chapter 4.1 – for example a malware attack can, if it is big enough, endanger the function of the nation’s economy. As this issue has already been discussed the current chapter will concentrate on the two overarching national security topics: critical infrastructure security and content regulation.

4.3.1 Critical Infrastructure Security

As per definition of the US Department of Homeland Security (DHS), critical infrastructure is the backbone of a nation’s economy, security and health. It encompasses sectors such as energy, water, transportation, and communications. Critical infrastructure are the assets, systems, and networks, whether physical or virtual, so vital to a country that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

95 “The direct cost to citizens of online crime is far exceeded by the sums of money being spent on measures to counter it.” British 2012 Report on Measuring the Cost of Cyber Crime (Source: Deltica)
A presidential policy directive for critical infrastructure security and resilience for the US was released in February 2013. The directive identifies 16 critical infrastructure sectors including Emergency Services, Information Technology, Food and Agriculture, Healthcare and Public Health, Communications, and Energy.

Each sector has a designated sector-specific agency, e.g. DHS and the Department of Defense, which has institutional knowledge and specialized expertise about the assigned sector. The goal is to identify vulnerabilities to physical or cyber attacks, eliminate significant vulnerabilities, develop systems to identify and prevent attacks; alert, contain and rebuff attacks; and to rebuild essential capabilities in the aftermath of an attack.

Europe has a similar program in place, called the European Programme for Critical Infrastructure Protection (EPCIP). One pillar of this pan-European program is the Critical Infrastructure Warning Information Network (CIWIN) which is a protected public internet-based information and communication system that allows its members to exchange and discuss CIP-related information, studies and good practice across multiple sectors.

Aside of physical threats, the internet or cyber space is at the centerstage of security risk analysis and concrete measures. “We need to understand that cyber space touches everything and everyone. It is a ubiquitous feature of our lives. There is no part of our national economy, infrastructure, or social fabric that is not in some way connected to the internet backbone.”

Gaining visibility into the different internet traffic content types provides the foundation of a nation’s cyber security efforts.

**Online Surveillance**

Online surveillance is relevant for all listed use cases because it allows monitoring of any data and traffic on the internet, whether voice communications, web and media content, or transactions and services including cloud applications. It allows governments more visibility concerning online and communication activities that could pose infrastructure and general cyber security risks. However, online surveillance itself has limited benefits due to the vast amount of data that needs to be analyzed in order to extract any useful indicators. So-called big data solutions help here. New surveillance tools incorporating big data capabilities combine user data from different applications to create a complete overview of an individual’s activities and communications.

**Lawful Intercept**

Lawful Intercept (LI) is the legally approved surveillance of an individual’s telecommunications use. It is an important tool for investigating and prosecuting criminal (cyber) activities and terrorism. In terms of regulation, Lawful Intercept (LI) refers to an obligation for telecommunications service providers to grant law enforcement agencies (LEAs) access to their network/services. Most countries have passed laws that require ISPs to enable LI with duly authorized requests. Even though regulations and LI requirements vary from country to country, standardization groups like ETSI and ANSI have developed technical standards for LI.

LI allows real-time monitoring of communication flow in networks as well as the extraction and mining of such data from ISP databases for analysis purposes.

Regulations controlling the legal interception of voice communications over traditional wireline networks have been in use for several years. Many countries have amended their LI policies from this original application to the wireless domain and furthermore from circuit-switched to packet-switched or IP-based communication infrastructure.

---

Therefore LI covers traditional voice calls as well as IP-based applications like voice over IP (VoIP), email, and Instant Messaging (IM) over both wireline and wireless networks. The particular way in which an ISP enables LI depends on the existing infrastructure. If, for instance, the ISP operates an IP Multimedia Subsystem (IMS) in its core network, the LI system can be connected there as shown in Figure 39.

In order for wireline providers to enable surveillance of internet traffic there is usually the option of either active or passive intercept. Active intercept connects to available network elements like routers (typically the ones at the edge of the network) and ‘Authentication, Authorization, and Accounting’ (AAA) servers which allow the filtering of access information and content of the monitored individual’s communication. Passive surveillance relies on additional filters or probes that are connected to the operator’s network to passively intercept (listen to) all relevant data independent of the commercial services. In some cases the combination both methods provides the best results.

Intercept in mobile networks can normally be done at the Mobile Switching Centers (MSCs) for voice and at the Serving GPRS Support Nodes (SGSNs) for data.

The list below outlines the capabilities of an LI solution which are most relevant to regulatory mandates and legislative requirements:
- Comprehensive intercept capabilities (intercept all applicable communications of a certain target without any gaps in coverage)
- Reliability and integrity (precise and accurate results with the highest levels of data integrity)
- Separation of content (metadata and communication content)
- Transparent surveillance (no detection by the subscriber)
- Immediate activation and real-time responsiveness (be able to be provided immediately and deliver intercepted data in real time.)
- Sufficient capacity (to handle the scope and scale of requested surveillance activities)
- Data security and privacy (protect sensitive data during transmission and safeguard the privacy of an individual’s records and personal information)
- Decryption (deliver encrypted data in plain text format)
- Complete logging of events (record and log all LI-related activities).
In the US, three Federal statutes authorize lawful intercept. The third one, the Communications Assistance for Law Enforcement Act (CALEA), provides the statutory framework for network operator assistance in providing evidence and tactical information for Law Enforcement Agencies (LEAs).

In March 2004, the US Department of Justice, FBI and Drug Enforcement Administration filed a petition which included expansion of CALEA provisions to allow surveillance of all internet traffic, including VoIP. CALEA was updated and now applies to facilities-based broadband internet access providers and providers of interconnected VoIP services, meaning VoIP providers that offer services permitting users to receive calls from, and place calls to, the Public Switched Telephone Network (PSTN). These providers are obliged to install LI equipment in their networks. Pure peer-to-peer VoIP providers are excluded, as are OTT email, cloud services and IM providers.

Governments and LEAs have a continuous challenge conducting lawful surveillance in a privacy-protective way. The fast and constantly changing ways individuals choose to communicate is one core root of the problem: landline phones, mobile phones, mobile apps, instant messaging, pagers, Skype, Facebook, Twitter, Google, multiplayer video games, peer-to-peer services, etc. Surveillance laws are playing catchup with the latest technological innovations. Legally collecting part of this information, e.g. stored emails from Google or other online providers, has long been possible in the US, enabled through the 1986 Electronic Communications Privacy Act (ECPA). But lawful real-time extraction of email traffic is not allowed, which creates practical challenges when quick and comprehensive authorized intercepts have to be executed across several communications platforms.

Extracting such communication information through deep packet inspection probes in ISP networks is technically impossible since most of the voice/data communications and also stored information (i.e. cloud storage) is encrypted.

Due to these issues the FBI is now talking about the “Internet going dark” which means that the US government will soon fall technologically so far behind that it will be unable to lawfully intercept communications over OTT communications forms such as Skype, a variety of text, photo, and video messaging services, online file transfer, or videoconferencing via Facebook and other social media sites.

For this main reason the FBI is currently pushing for CALEA II. This is basically the move from wire tapping to web tapping and would: (1) expand CALEA policies to all internet-based communication services, including VoIP, social networking services and cloud storage providers - who would need to deploy technology enabling real-time, or near-real time, intercept of communications; (2) prevent these providers from providing encryption features for their clients’ secure communication and storage needs; and (3) mandate online providers to build “backdoors” into communications software for LI due to the encryption and peer-to-peer communication nature of a lot of these services.

Discussions on the validity of the FBI’s CALEA II requests are currently taking place.

To support CALEA, and also to overcome its current limitations, significant budgets have been allocated to agencies like the FBI, the Information Awareness Office (ISA), and the National Security Agency (NSA) to develop and utilize systems for online surveillance. NarusInsight, a product from California-based Narus, Inc. (a Boeing subsidiary) plays a central role in the FBI’s CALEA and extended surveillance activities. It is a sophisticated, fast and scalable DPI system, able to support monitoring of large, complex IP networks. It can be configured to analyze a particular activity or IP service such as lawful intercept or for example Skype detection and blocking. It is able to track users’ web browsing and IM activities, monitor VoIP traffic, and capture and reconstruct webmail. Besides the US, the national telecommunications authorities of both Pakistan and Saudi Arabia are Narus customers.
Russia and several countries in the region have either passed or are considering legislation that further expands their surveillance powers. Russia’s System for Operative Investigative Activities (SORM and SORM-2) laws enable comprehensive monitoring of any communication, electronic or traditional without warrant. SORM-2 allows monitoring of the internet in addition to telephone communications through special devices installed on ISP servers. Russia’s latest regulation draft requires ISPs and mobile operators to install equipment that allows the recording and storage of any network data for at least 12 hours. Furthermore providers are now obliged to store user’s identity information in all data exchanges (i.e. e-mail/IP addresses, IM IDs, physical locations of people using Skype or Google Hangouts).

In the context of OTT applications and content, all data is transported over the internet using wireline or wireless access networks, computers or smartphones. Internet traffic is routed through access routers, core networks and backbone with many interconnection points for the exchange of traffic between countries. This infrastructure provides many access points for surveillance and respective DPI systems.

One form of surveillance with increasing popularity is the creation of social network maps based on data from social networking sites (Facebook, MySpace, Twitter) in combination with traffic analysis information from phone call records provided via LI activities. Using big data software for mining extensive sets of data, these maps are created and dissected to analyse personal interests, friendships & affiliations, wants, beliefs, thoughts, and activities.

Many government agencies are investing heavily in this, partly triggered by the assumption that the main threat to a nation comes from decentralized, leaderless, geographically distributed groups of terrorists, extremists, and dissidents. Big Data and social network analysis also interest the corporate world, which hopes to gain more insight into customer behavior and trends to optimize their marketing and sales efforts. New open and commercial protocols and software solutions are therefore being developed, benefiting both government and corporate sectors.

Social network analysis is probably the area that will see the most traction in the coming years, supported by software developers, large software firms and, last but not least, the general public who are sharing an increasing amount of data online by engaging in social networking activities, using online media and communications offerings and making commercial transactions.

From a technical point of view the area of online surveillance, including LI, is therefore quite advanced. Nevertheless, DPI systems are currently challenged by the trend that web sessions are being encrypted to make them more hacker-safe. A continuous increase in the amount of encrypted traffic is to be expected as service after service adds this security feature.

This means that, without appropriate legislation (for example what the FBI in the US is trying to achieve with CALEA II) and the cooperation of the respective service provider (i.e. Google), it will not be possible to look into the actual packet content of the monitored traffic flow. This needs to be taken into account when making decisions about LI legislation or reaching out to the internet provider community. Current proposals like CALEA II also create tremendous controversy because the enforcement of LI capabilities can introduce substantial security threats - collaboration should be established with the internet community to come up with a mutually beneficial approach that still guarantees maximum data and privacy protection instead of creating additional security issues.

---

The internet is vital to most national economies and the daily lives of their citizens. Therefore it is important for the GCC countries to position themselves as general supporters of the dynamic internet content, communication and service landscape.

In order to minimize cybersecurity threats, the general public should be involved in the management of these threats. For instance, in the USA models are being established as public-private partnerships to educate businesses, public institutions and individuals and to provide sources and tools for optimized preparation and reaction to these threats. The US National Cyber Security Alliance (NCSA) has been formed to “educate and therefore empower a digital society to use the internet safely and securely at home, work, and school, protecting the technology individual’s use, the networks they connect to, and our shared digital assets”. NCSA’s focus is on encouraging a culture of cybersecurity. As a communication vehicle NCSA created a “Stay Safe Online” initiative, building on the statement that protecting the internet is a shared responsibility.

Another perspective is the UK’s positioning in the cyber security domain. The country has clearly realized that “with greater openness, interconnection and dependency comes greater vulnerability.” The UK government is now pursuing new ways to protect businesses and make the nation more resilient to cyber-attacks and crime. UK’s “National Security Strategy” categorised cyber attacks as a Tier One threat to its national security, alongside international terrorism. The Cyber Security Strategy defines how the UK will support economic prosperity and protect its national security by building a more trusted and resilient digital environment.

Concrete steps the UK has taken or is taking are:

- setting up a National Cyber Crime Unit
- providing cyber security advice to businesses
- building a Cyber Information Sharing Partnership with businesses to allow the government and industry to exchange information on cyber threats in a trusted environment
- creating a joint Cyber Growth Partnership with technology industry representatives, to support the growth of the UK cyber security industry and increase exports
- introducing a single reporting system for people to report financially motivated cyber crime through Action Fraud (the UK’s national 24/7 fraud and internet crime reporting centre) since the central recording of fraud incidents enables the shared analysis of intelligence gathered about crimes, resulting in more targeted enforcement action.
As a general guideline with respect to implementing or expanding lawful online surveillance and intercept practices, and in the light of the privacy, technical and economic challenges, measures taken should:

- address only problems which currently exist or can be reasonably anticipated in the near future, instead of significantly expanding online surveillance / lawful intercept beyond its original intent or mandate
- minimize, to the greatest extent possible, resulting damage to innovation and positive economic effects
- preserve the free flow of ideas and information over the internet
- provide strong protection for privacy and civil liberties
- act in the best interests of all citizens by imposing only those regulations necessary to accomplish important public policy goals such as the protection of public safety, national security and privacy concerns

4.3.2 Content Regulation

This issue covers any sort of widespread content monitoring or restriction as mandated, either explicitly or otherwise, by government or regulatory bodies. It concerns access to illegal content as well as material deemed undesirable for the general public. The global perspectives on this matter are quite diverse, driven by different social values, economic incentives, and political objectives. There is a broad array of reasons to regulate or censor internet content, including the protection of minors, human rights, social values, preventing violence, or to stop illegal online activities such as the distribution of copyrighted material, or gambling.

Aside from commercial tools, a wide variety of technical methods can be used to limit access to online content, e.g. IP address blocking, URL filtering, DNS filtering and redirection, packet filtering and, more drastically, network disconnection.

From a technical point of view content access can be controlled at different levels:

- Internet Backbone: government-directed, nationwide use of content filtering and blocking technologies (often done at the international gateway or interconnection points);
- ISP: government-mandated filtering using methods such as search-result removals, take-downs, or technical blocking;
- Institution: mandated or encouraged filtering, technical blocking or self-censoship in institutional networks (companies, schools, government, public hot spots);
- Individual: home or individual device-level filtering and blocking.

Content regulation is relevant to all internet-based activities that deal with content in the form of communications data and media (video, pictures, music, text).

Blocking and Filtering

Any type of online content can be blocked or filtered based simply on relatively static or dynamic blacklists created as a result of a real-time examination of the internet information being exchanged.

China, Iran and Saudi Arabia are among the countries with the most extensive blocking and filtering mechanisms, especially with regards to restricting access to web destinations. Saudi Arabia's censorship is focused on pornography, alcohol and drug use, gambling, terrorism, sites that provide the means to bypass the filter systems and sites that call for political reform or are critical of the current social landscape. Filtering policies and blocking/unblocking decisions are made by a permanent committee headed by the Ministry of the Interior. The CITC is responsible for the internet filtering service and provides a daily database of blocked sites to service providers, who provide the technical filtering solutions and must block all sites banned by the CITC. Filtering in Saudi Arabia takes place at the country-level servers of the three data service providers which are placed between the state-owned internet backbone and servers in the rest of the world. All user requests that arrive via Saudi ISPs travel through these servers, where they can be filtered and possibly blocked.
In Egypt, the government does not widely censor internet websites, except those that are a threat to national security – and these are tracked, blocked or closed down. Egypt also has a fair amount of self-censorship, for instance by editors of official news websites, but some Egyptian ISPs also offer optional filters to block specified subjects or offer internet services with content controls.

Legal Enforcement

Several governments are passing new laws which criminalize certain types of political, religious, or social speech. For instance in 2013 a ban was applied to Jordanian news websites which had not been registered and licensed by the government. The blocking order contained a list of over 300 websites. Under the new law for enforced registration of websites, online news sites are held accountable for comments posted by their readers. Furthermore the sites are required to archive all comments for at least six months.

In some cases particular prominent sites like youtube, facebook and twitter are being targeted, enforcing censorship of select content in the form of blocking or disabling access to individual pages or profiles. This is mainly driven by local trends - where a combination of social media platforms is used by various groups to manage protests or sit-ins: facebook is often used to specify the date, time and place of a protest or event, while video footage of the event is uploaded on youtube and then disseminated via twitter.

Holding ISPs, site hosts, webmasters, etc. legally liable for the content published by individuals through their services and internet sites, as in the aforementioned Jordan example, has the effect of proactive censorship enforced by the respective intermediary.

In one extreme case, intermediary liability in China has triggered several private companies to apply pressure on entire divisions to force them to monitor the content of social media sites, online forums, and search engines and to delete content regarded as undesirable. In some cases failure to remove content has resulted in the arrest of corporate executives.

In Europe the liability lies with the host instead of the ISP, as specified in the EU Directive on Electronic Commerce: “ISPs have no liability when the service provided is a mere transmission or access to a communication network, to the extent that the ISP cannot select or modify the content of the transmission, or select the receiver of the transmission. There is no liability on the ISP when the service is an automatic, intermediate or temporary storage of data
Policy and Regulatory Framework for Governing Internet Applications

Study

(caching) so long as the provider does not modify the information, complies with conditions on access, and acts promptly to remove or disable access to the information when required. Furthermore, the ISP is not liable when the service offered consists merely of the storage of information, provided that the ISP does not have knowledge of illegal activities or information, or upon being aware, acts promptly to remove or disable access to the information.” Instead of holding the internet service or content intermediary liable, many governments target the content source (i.e. authors and publishers) directly. They are then held liable for the content posted on websites, blogs or social networks. Egypt is an example where bloggers are being prosecuted for online activities like “offending the state institutions, incitement to hatred of Islam, destabilizing public security, and inciting others to demonstrate and strike via the Internet.”

This approach is sometimes considered less disruptive toward the ISP or content hosts who are relieved of having to deal with these issues, but it requires more effort on the law enforcement side as it is a much more distributed approach (i.e. targeting many content authors instead of one website or ISP). A benefit of this model is that it encourages online users to apply more self-censorship.

With respect to protecting intellectual property online, the United States has been quite active over the last couple of years. The Recording Industry Association of America (RIAA) and the Motion Picture Association of America (MPAA) have successfully pursued legal actions against suspected infringers. Prominent cases are Napster, PirateBay, Defense Distributor, and MegaUpload. Now the RIAA, MPAA and a few other associations have partnered with five major US ISPs to form the “Center for Copyright Information” with the aim of implementing a system to remove copyright infringing materials from the web. The organization’s so-called “Six-Strikes” plan was launched at the beginning of 2013. The ISPs circle in on peer-to-peer systems and traffic, monitoring their networks for activity that may involve copyrighted material. After five or six suspected instances, the ISPs may take action such as blocking a user’s access to some of the most frequently visited websites until they have completed a copyright education course, slowing down the connection speeds of repeated pirates, or temporarily interrupting the individual’s ability to browse the internet. So far the emphasis has been on educating the public and a number of different ISP-enforced restrictions on access for suspected violators.

In December 2012, Russia and the USA agreed on an action plan to jointly improve protection of Intellectual Property Rights. Key priorities are combating copyright piracy over the internet, enhancing IPR enforcement, and coordinating legislation.

In Saudi Arabia, The Ministry of Culture and Information (MoCI) has started the implementation of a number of major anti-piracy measures in a move intended to establish the Kingdom as a regional leader in such efforts. Protection is granted to artists whose works are expressed in writing, sound, drawing, photography, motion pictures or computer software.

Infrastructure or Service Shutdown

Many governments have “kill switch” authority, which means that they have the authority to mandate a suspension of private communications networks, typically for reasons of national security or natural disaster. This has also been used to maintain public control during certain critical events or times. This can be quite localized - limited to select towns or regions - but can go as far as cutting off the entire country. Egypt, Syria and Venezuela are examples where either the government or the ISP has taken such action.

In January 2011 Egypt shut down close to 90% of Egyptian internet by withdrawing more than 3,500 routes from the ISPs’ networks. In fact, the government’s order was that all forms of mass communication including internet access, mobile networks, and SMS be blocked. The internet was basically shut off for five days. This drastic measure has had severe repercussions on the country’s economic situation. The Organization for Economic Cooperation and Development (OECD) estimates that the blackout cost Egypt’s economy about $90 million, or $18 million per day, comprising 3% to 4% of the country’s economic output. They further stated that Egypt will find it “much more
difficult in the future to attract foreign companies and assure them that the networks will remain reliable. In order to ease the financial impact on the affected telecom providers, the government is now making large compensation payments for the loss of revenue in the period of internet downtime.

A more targeted approach is to block dedicated services like text messaging. India and China for example have both disabled this service during protests and rioting.

Additionally, instead of shutting down services or infrastructures it is also possible to throttle connection speeds, making it more difficult or inconvenient for individuals to share videos or access certain content.

**Content Filtering Tools**

A variety of sophisticated filtering solutions are commercially available to identify undesirable or illegal content. Popular vendors/products are McAfee’s SmartFilter, Websense and NetSweeper. Besides by the Kingdom of Bahrain, SmartFilter is also used by Kuwait, Saudi Arabia, Sudan, Tunisia, the UAE, Iran, and Oman, as well as the United States and the UK. Netsweeper is used in Qatar, the UAE, Pakistan and Yemen. Myanmar and Yemen have used filtering software from Websense.

It is worth mentioning that there are several key vendors of content filtering and blocking solutions whose business intentions are considered by many independent observers as in violation of human rights. They have been dubbed “Corporate Enemies of the Internet”: 98 Amesys (France), Blue Coat Systems (U.S.), Gamma (UK and Germany), Hacking Team (Italy), and Trovicor (Germany). Using these companies’ products can have a negative impact on a country’s political and social image.

The creation of a transparent and cooperative environment for law enforcement, and common or aligned objectives so that the public and ISPs work together to fight cyber crime and illegal content on the internet is the way forward.

Establishing an internet code of conduct as a guideline for internet content and service provider behavior is a lightweight regulatory option. Content providers and ISPs hosting content should be obliged to remove illegal content upon identification or notification. The code of conduct should contain proper notification requirements for ISPs,99 content providers and users to facilitate compliance with legal obligations and also for liability reasons. Enforcement of the code of conduct should be performed by self-regulatory agencies, which have defined legal privileges but are subject to consent from public authorities.

---


In summary the promotion of self-regulation is most recommended.\textsuperscript{100, 101, 102} The framework should be sensitive to public information and communication needs, economic and political objectives, while maintaining a robust communication environment. Active user involvement is critical for effective self-regulation and this requires appropriate community consultation. Governments should educate the public (communities, schools, etc.), provide information and raise awareness among users of self-regulatory options such as filtering and blocking content and also of how to file complaints about illegal internet content. The provision of rating and filtering technology for internet content to users enables them to assume responsibility for the control of harmful content. To further support self-regulation, users must be able to intuitively respond to internet content that they find of concern. Intermediate and independent organizations should be put in place to handle and evaluate such reporting, and to trigger remedy measures if required. The framework provided by Q-Cert in Qatar could be taken as a basis for development here.

The provision of transparent and dynamic blacklisting of web content that falls into pre-defined filter categories (for instance illegal or national security threatening content) is a further tool to prevent the distribution of illegal or unsuitable content. The blacklists can be centralized and made available to ISPs who should then be held accountable for executing the content filtering and blocking measures (without holding them responsible for the previous transport of such illegal content before they knew of its existence.)

\textsuperscript{102} FTC and self-regulatory frameworks regarding online behavioral advertising http://www.insidecounsel.com/2013/10/18/technology-ftc-and-self-regulatory-frameworks-rega
5. Conclusions and Recommendations

5.1 Conclusions

The international dynamics of the internet will not be halted by national regulations. A major enabler of the net’s development has indeed been the lack of regulation that it has faced to date. The regulator’s objectives must be to catalyse additional opportunities offered by the internet to the benefit of the consumer and to support competition. While avoiding the trap of regarding the internet as a threat, a further regulatory task must be to facilitate the reduction or minimization of internet-driven risks in the areas of security and data protection – both from the consumers’ and from the nation’s point of view.

One negative effect of the internet revolution is the loss of data control. The likelihood of accidental or intentional disclosure of personal or classified information continues to increase. The research has revealed that there are increasing risks affecting users’ online data, but that regulators worldwide are working on measures to improve the consumers’ protection from these risks. The output of this activity can be used by the GCC to develop its own data protection legislation.

In terms of malicious attacks on the internet, beyond the introduction of cybercrime laws the most important measure is to increase consumer awareness of the risks and to encourage the suppliers of services to self-regulate and prevent the dispersion of malware, spam or similar.

The proliferation of IP-based telecommunication networks has facilitated the decoupling of application and network layers and enabled OTT providers to deliver their content and applications directly to end users. Structural change always leads to the need for new business models, for a letting go of old practices and the welcoming of new opportunities. The tendency to accuse the OTT providers of being “free riders” in the transport market is not entirely accurate. The operators are paid for the transport of the data – albeit a flat rate from the user.

OTT providers are compounding the telcos’ commercial problems by using this flat rate tarifed capacity to provide services (often free of charge) in direct competition to the telcos’ services, thus eroding some of their most important revenue sources (e.g. international telephony and sms services).

While the competition provided by the OTT application providers does lead to disruption, a functional market should be able to adapt to the new situation.

If competition was working, the telcos would change their tariff plans in line with market demand. As this is not happening, competition is apparently dysfunctional. The research shows that this is a situation found throughout the world and for which there is not yet a patent solution – although the root cause apparently lies in the combination of flat rate tariffs based on business plan assumptions that no longer hold true in combination with apparently non-sustainable competition from OTT players and regulatory obligations which make it impossible for the telcos to react freely to the commercial changes demanded of them. It must be a central regulatory task to analyse this dysfunctionality thoroughly and to introduce measures to eradicate the problem.

Competitive principles should also ensure that broadband infrastructure will be built and operated where demanded and to the commercially feasible extent. The commercially feasible extent may however not be the extent needed to satisfy political goals. International examples show that in this case the provision of the broadband infrastructure may be organized as a state-run business, or further infrastructure may be subsidized either through direct government intervention or through obligations placed on operators.

As a result of the detailed assessment of the regulatory treatment of internet application markets throughout the world it can be concluded that the GCC region is already advanced. For example, in most countries there is
significant competition in the ISP market and guidelines concerning the treatment of VoIP have been developed. The decision to limit action against OTT providers to those actively flaunting the Kingdom of Bahrain’s regulations is a clear indication that the regulators in the region are aware of the need to balance the costs and benefits of control.103

The area of cybersecurity is a new area for regulators and offers an opportunity for GCC regulators to establish themselves as thought leaders. The study has revealed that the creation of a transparent and cooperative environment for law enforcement, and common or aligned objectives to enable the public and ISPs to work together to fight cyber crime and illegal content on the internet is the only way forward.

5.2 Recommendations

Regulatory Policy

5.2.1 Assessment of broadband104 market, development/adaptation of policy

A major motivation for governments to investigate the need to intervene in the internet application market is the surprising realization that the rollout of nationwide broadband – often a political objective - has not occurred “naturally”. It is recognized that a country’s businesses and residents must have access to broadband in order to take full advantage of the benefits offered by the internet and its services and applications, and it was expected that its provision would be driven by the network operators’ recognition of the need to supply more transport capacity in order to sell more applications and services. This market mechanism has not worked to the extent hoped for by governments. If the rollout of broadband is to be facilitated, the reasons behind this malfunction must first be identified and quantified. The following steps are recommended.

Assess the market for broadband:

- Implement research to assess the economic demand for broadband, including differentiation for different qualities of service. Such research must combine existing data concerning use of broadband and consumer/business research to assess how much users would be willing to pay for capacity and quality and their elasticity of demand with increasing or decreasing tariffs.
- Based on this research an initial plan for network extension can be drafted and a cost estimate made.
- The feasibility of the network extension can then be calculated.

Three outcomes are possible:

- The extension of the broadband network is feasible and in line with the policy objectives of the government.
- A partial extension of the broadband network is feasible, but the extent of the rollout which is commercially feasible is not in line with the policy objectives of the government,
- The extension of the broadband network is not feasible.

In the second and third cases the government is obliged to make a policy decision as to whether and how the broadband rollout is to be supported with regulatory measures:

- The establishment of a national broadband network which is not obliged to operate on a purely profit basis;
- The obligation of a network operator to expand the broadband network but with financial support either from the government (subsidization) or from a sort of universal fund funded by all players in the market;
- A change in policy decision away from the extension of the broadband network beyond economic demand.
- A further option often chosen in Europe is the setting of coverage obligations for SMP licence holders (particularly for LTE) – this option is not recommended as it puts the burden of fulfilling political objectives on a limited user group rather than on the general public as a whole.

---

104 “Broadband” refers to high speed communications technologies – which speed is generally defined as a political objective, e.g. 50 Mbit/s for 75% Households (Germany), 1 Gbit/s for businesses (Bahrain).
In the first case a functional market should lead to the installation of broadband and, where this has not happened to the extent hoped for, market structures must be examined in more detail to identify the root cause. Here there are two main potential causes – either regulatory barriers are preventing the correct functioning of the market, or the competitive pressure on the operator is not strong enough to force a commercial reaction.

An analysis of each of these potential causes is recommended.

5.2.2 Implement review of regulation faced by network operators to ensure that these reflect the changed market situation. Rebalance obligations as found to be appropriate.

The research clearly shows that the entry of OTT providers into the market has changed the network operators’ competitive situation dramatically. In a functional market all market players would adapt their business models accordingly and a new equilibrium would be found. As this is apparently not happening in the current case there must be market imperfections. This may be because regulatory obligations (e.g. tariff regulations) placed on the operators are impeding their attempts to respond appropriately to the competitive challenges they are facing. For this reason it is recommended that the regulatory obligations faced by the operators are reviewed in detail and appropriate adaptations made according to the results revealed.

The following tasks must be implemented:

- Initial check that the SMP status of the operator is still maintained and that the specific ex-ante regulation is thus still justified. This check involves a market study in line with general regulatory practice and may result in the removal of specific regulated services from tariff obligations.
- Detailed analysis of the SMP operators’ costs and cost structure taking the shift in business from services to transport into account.
- If so required, allocate the costs of the required broadband expansion to the operator in line with government objectives – so that these are also reflected in any new tariff regulations.
- Review existing regulated tariffs to take new cost structure and expected market developments into account.
- Review of other regulatory obligations/decisions\textsuperscript{105} to reflect changes in the market situation.
- Public consultation and hearing on planned changes.
- Finalization and implementation of changes.

As a result of this work, regulatory imbalances preventing the network operators from reacting to competitive challenges should be removed. Please note that this rebalancing exercise is a recommendation developed specifically as a result of this study – it has not yet been implemented in other markets and can therefore not be benchmarked.

5.2.3 Determine whether the provision of specific (free) OTT services represent destructive competition and is detrimental to the development of the market.

A further hypothesis concerning the root cause of the market’s malfunction is that the OTT providers’ competitive behavior is unfair. The basis for this hypothesis is that the competition created by the OTT providers is not sustainable, as indicated by the fact that they are often loss-making and their financing is based on extremely high stock market valuations rather than on solid business cases. In the medium to long term their business cases will have to be adapted to be profitable, but if their short term behavior forces other providers into cut throat (negative margin) price competition the detrimental effects on the market may not be reversible. This hypothesis must be tested and if proved reflected in changes made to rebalance the regulatory obligations of the telcos in comparison to those of the OTT providers.

\textsuperscript{105} Here a case in point is the recent verdict of a civil court case in Germany which has prevented Deutsche Telekom from redefining its transport tariff in line with market developments.
In the short term encouraging alternative business models for the OTT providers – such as joining forces with local ISPs to provide services (as is propagated in UAE) – could reduce negative impact as well as providing legislative control over the OTT service provision through the ISPs. This would of course require the extension of the ISPs’ licences to include voice provision.

However, it is strongly recommended that licence-free OTT application providers continue to be tolerated in the market. The destructive nature of their competition will be reduced as shareholder pressure forces them to charge for services in order to make a profit. A ban would destroy competition and limit innovation – in a functional market it should absolutely not be necessary.

5.2.4 Determine whether a lack of competitive pressure is preventing the market from functioning.

A further reason for the lack of investment in broadband may simply be that the operator is not subject to enough competition to be forced to react. Despite a strong natural tendency to protect the incumbent telecommunications operators, regulators should resist the temptation to do so. The regulatory task is the facilitation of fair competition – not tipping the scales in favour of a particular player. It is recommended that, once regulatory limitations have been removed, an assessment of competition in the transport market is implemented. The following steps are necessary:

- Identify market players in the transport market for broadband services (these will now include mobile broadband operators).
- Assess degree of competition.
- In case of limited competition develop framework to open up the market. Here the option of structural separation may be particularly relevant – in both Australia and Singapore this method has been chosen to improve the functioning of the market and facilitate the spread of broadband.
- Develop implementation plan.

5.2.5 Define a framework for net neutrality regulations to enable commercial service offers and cost-oriented market pricing while protecting the consumers’ interests.

Although international trends show that network neutrality is becoming less strict, it is recommended that the GCC countries develop basic neutrality guidelines to protect consumers’ interests. This is particularly relevant as the trend towards differentiated/tiered service offers could, without a framework, lead to some internet traffic being neglected completely. It is recommended that the net neutrality guidelines issued in Singapore are used as the basis for discussion:

1) Operators are not allowed to block legal content;
2) They must always comply with competition and interconnection rules;
3) They must disclose information to the end-users about their network management practices and typical internet broadband download speeds;
4) They must meet minimum QoS standards as defined in their licences; and
5) They are allowed to provide niche or differentiated services.
5.2.6 Update license conditions of existing operators and service providers to reflect the findings of this study concerning net neutrality and growing data protection and security requirements.

Developments in the internet application market – particularly in terms of security and data protection – render some licences and authorizations outdated as they do not account for needs which have only arisen in the recent past. This situation must be rectified. The appropriate tool for doing this will vary from country to country – in some cases it may be the subject of a directive, in other cases licence conditions may need adaptation. The areas requiring attention are:

- **Decryption obligations.** The surveillance of OTT communications is only possible as long as the traffic is not encrypted. As the trend is towards encryption, a requirement for the decryption of encrypted data if so required by Law Enforcement Agencies should be added to license holders’ legal intercept obligations.

- **Business Continuity Management System (BCMS).** The impact of security issues on corporations can be reduced through obligations to the holders of licences to introduce business continuity measures.

- **Content regulation (self-regulation).** Add obligation to ISP terms of operation for them to adhere to a Code of Conduct for content regulation (self-regulation), alternatively or in addition to requiring blocking of the blacklist content providers.

- **Net neutrality regulations.** As defined as a result of 5.2.5.

For all these areas draft amendments are to be produced and subjected to public consultation before they can be implemented as requirements.

5.2.7 Establish coordination procedures between financial service regulation, data privacy and protection regulation, broadcasting/publishing regulation (PPP Law) and communications regulation to ensure that measures are consistent and coherent.

It is recommended that a government committee is set up to coordinate all activities concerning the management and regulation of the internet. The central role that the internet is already playing in both business and private life can be expected to become even more important in the future. In some countries (Germany for example), there are even calls for an “Internet Ministry” to be established. This creation of new bureaucracy is not recommended, but coordination of existing bodies is absolutely vital.
5.2.8 Combine broadcasting, communications (and publishing) regulation.

It is suggested that the convergence of these markets makes the convergence of their regulation logical. As the barriers between the markets are blurring this would help ensure consistent treatment of market players. To verify this hypothesis the feasibility of such convergence should be assessed in a first step and, if proved, a single regulatory body set up. The feasibility study should include:

- A quantified assessment of the benefits/synergies of combining the authorities and councils responsible for broadcasting, communications (and publishing) into one regulatory unit. Broadcasting and communications are already an integrated area in some jurisdictions.
- Assessment of the costs of such a convergence.
- Determination of the plan’s feasibility and securing of political approval.
- Implementation if appropriate.

5.2.9 Draft and ratify cybercrime legislation which is coordinated throughout the GCC.

The research shows that global internet players will not abandon their business models or service portfolio just because a single country tries to regulate them or the services that they provide. It can be concluded that an individual country will generally not have the power to force the global players’ hands: joining forces with other regulators will increase the impact that an individual regulator may have. We therefore recommend that the GCC regulators should coordinate their cybercrime and data protection activities. Additional alignment with regulations being introduced in the EU may further increase impact.

The examination of existing cybercrime laws and drafts indicates deficiencies in the areas of encryption requirements, copyright/IPR infringements and piracy. These deficiencies should be eliminated before the process to pass the law/its amendment is triggered (public consultation, editing, passing and ratification). In those countries still lacking cybercrime legislation, this situation should be rectified as soon as possible. Combined cybercrime and data protection legislation is to be found in several jurisdictions. Such a combination is commendable as long as the two aspects enjoy equal emphasis and the law is comprehensive.

5.2.10 Draft and implement new/updated data protection law in line with the leading edge work being implemented in the EU.

Most existing data protection legislation was developed prior to big data, DPI and Facebook etc. and thus does not address all relevant issues. The new data protection guidelines agreed by the European Parliament and now being discussed in the Member States are leading edge here. The guidelines concentrate on consumer rights by creating a comprehensive framework to put the individual’s personal data back into their possession and control (including the right to decide whether tracking/profiling is allowed, the right to check data saved about oneself – and to correct it -, the right to demand deletion of data, guidelines concerning the national/international storage of data, and a framework for data portability). It is recommended that the GCC members join forces to use these guidelines as the basis for a GCC-wide data protection legislation.

5.2.11 Develop GCC-wide procedures to facilitate content regulation.

Although content regulation has to date not been an area allocated to telecom regulators, the convergence of the markets (see 5.2.7/5.2.8) and the technical expertise required to implement such regulation make it relevant. It is recommended that the feasibility of centralizing content regulation in the GCC region is tested:

- Each member country’s objectives concerning content regulation should be determined and compared to assess whether there is consensus;
- In this case the measures to be taken should be defined;
- The benefits and costs of implementation should be assessed, along with a financing model for the measures agreed;
• If agreement is reached on the joint implementation of content regulation this should be implemented.
• If at any of the previous stages it should become clear that regional centralization is not possible, the maximum possible degree of coordination should be aimed for – again the costs and benefits of this coordination should be quantified before implementation.

Measures recommended in the area of content regulation are:
• A (centralized) database of blacklisted content providers – covering all categories of unsuitable/illegal content, copyright/IPR flouting, and malware distributors - for daily distribution to ISPs within the framework of their content blocking obligations (see recommendation 5.2.6).
• A (centralized) hotline for individuals to contact concerning content complaints and linked to the blacklist database.
• Consumer demand for a blocking tool to be provided to end-users to enable them to self-regulate their content provision should be quantified and the tool elaborated if demand is there.

5.2.12 Develop strategy for consistent and continuous user information concerning the risks and benefits of the internet

This study has made clear that the most promising method of reducing security issues or cybercrime is to improve customer awareness. It is recommended that the GCC members develop a joint strategy for the provision of consistent and continuous user information and education. In this way economies of scale can be enjoyed – for example, even if training materials have to be adapted to suit regional requirements the one-off development of the content will reduce the costs to be carried by each regulator. Bahrain is already active in the area of consumer information. Measures recommended are:
• Set up an online information centre for users covering:
  - Information about the government/GCC’s internet policy;
  - Consumer information concerning current internet risks and methods for avoiding them;
  - Access to the content regulation blacklist and to the hotline for reporting doubtful content;
  - Access to the cybercrime center (see recommendation 5.2.13);
  - Online tutorials in data protection and security (for adults and children);
• In addition school project material should be developed to align training in the use of the internet with children’s first exposure to the medium. Here an “internet driving licence” is recommended along with supporting training materials for teachers.
• Public awareness campaign (TV, billboards)

5.2.13 Investigate the feasibility of establishing a regional cybercrime center for GCC.

It is recommended that the GCC sets up a regional cybercrime center. This should be closely connected to the information services in recommendation 5.2.12. The center’s main tasks should certainly include:
• provide advice to users and individual governments concerning cybercrime;
• provide an early warning system for cyber attacks;
• enable the centralized registration of cybercrime activity (enabling better early warning);
• provide a forum for exchange of cybercrime prevention related ideas;
• initiate and/or organise the development of further cybercrime prevention measures as and when necessary.

In addition it is suggested that such a center could position itself as a skill center in business continuity management (BCM). As increasing risks from online business make BCM more relevant, the provision of advice and support here could become a central pillar of the center’s activity.
The feasibility and exact mandate of such a center must first be assessed and agreed upon. The steps to be taken are:

- A working group should identify and compile the member countries’ objectives concerning the prevention of cybercrime to assess whether there is general consensus on the need/benefit of a centralized cybercrime center;
- The tasks to be carried out by the cybercrime center should be defined. It is suggested that the experience of Q-Cert in Qatar should be used as the basis for discussion;
- The benefits and costs of implementation should be assessed, along with a financing model;
- Based on the results of the feasibility study the members should be in a position to negotiate and issue a mandate for the creation of such a center.
- If at any of the previous stages it should become clear that regional centralization is not possible, the maximum possible degree of coordination should be aimed for as this is expected to lead to significant economies of scale.

5.2.14 Encourage development of the local CDN market with the objective of establishing a data center hub for the region.

There are both commercial and regulatory reasons for encouraging the development of the local CDN market in the GCC region:

- The CDN market is a natural extension of the transport market. As the telcos are being pushed out of the applications market and by default are forced to concentrate on the transport business, it makes commercial sense for them to investigate the opportunities provided by the CDN market – this is a method by which they can monetize the relationship with OTT players.\textsuperscript{106}
- By encouraging OTT providers to replicate their content at a CDN in the region its regulation may be facilitated – the condensed data at one or a limited number of locations is easier to control from a security point of view than individual data streams originating outside the region and destined for users within it.
- The combination of CDN services with an internet exchange infrastructure could facilitate the continued development of internet business in the region and reduce dependency on global internet providers.

Of course, the decision by an operator to provide CDN services is a commercial decision to be made on the basis of feasibility and a business case. It is not under the auspices of the regulator. The benefits could however be pointed out and operator action encouraged.

\textsuperscript{106} This was used in Germany by DTAG as a method of getting OTT players to pay for transport.
5.3 Roadmap

On the following page a roadmap for the implementation of the above recommendations is given. Although the roadmap shows the order in which the various recommendations should be implemented this is not set in stone and may be changed quite easily as a number of areas of activity are completely independent of each other.

<table>
<thead>
<tr>
<th>Month</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
<th>17</th>
<th>18</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Assess broadband market</td>
<td>Market assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Review Operator Regulation</td>
<td>Review, analysis and drafting of plans</td>
<td>Consultation</td>
<td>Finalization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Assess OTT competition</td>
<td>Analysis and assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Check competition in transport market</td>
<td>Market assessment</td>
<td>Further action follows if market is found to be non-competitive</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Develop Net Neutrality guidelines</td>
<td>Draft</td>
<td>Consultation</td>
<td>Final</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Update license conditions of operators and service providers</td>
<td>Draft</td>
<td>Consultation</td>
<td>Final</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Set up coordination committee for all internet-related activities</td>
<td>Setup</td>
<td>Regular committee activities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Combine media and IT regulation</td>
<td>Draft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Cybercrime legislation</td>
<td>Negotiate and Draft</td>
<td>Consultation</td>
<td>Finalize</td>
<td>Press legislation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Data protection law.</td>
<td>Negotiate and Finalize</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Content regulation</td>
<td>Feasibility</td>
<td>Negotiation on framework</td>
<td>Implementation follows if GCC members in agreement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Public Information Strategy</td>
<td>Strategy</td>
<td>Implementation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Regional cybercrime center</td>
<td>Feasibility</td>
<td>Negotiation on framework</td>
<td>Implementation follows if GCC members in agreement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>CDN Market</td>
<td>Research market</td>
<td>Further work depends on options identified in research</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
6. The Authors

**Detecon**
Shirley Baldry, Shirley.Baldry@detecon.com
Dr. Markus Steingröver, Markus.Steingroever@detecon.com
Rachad Abdallah, Rachad.Abdallah@detecon.com
Lars Bodenheimer, Lars.Bodenheimer@detecon.com
Joseph Noronha, Joseph.Noronha@detecon.com
Leo Niedermann, Leo.Niedermann@detecon.com
Dragos Titica, Dragos.Titica@detecon.com

Detecon International GmbH
Sternengasse 14-16
50676 Köln
Tel + 49 2219161-0

**TRA Bahrain**
Mohamed Bubashait – General Director, Mohd.Bubashait@tra.org.bh
Mohamed Tayeb Mahmood – Technical & Operations Director, mtayeb@tra.org.bh
Faisal Aljalahma - Finance and Human Resources Director, faljalahma@tra.org.bh
Shadi Alwaswasi - Finance Manager, salwaswasi@tra.org.bh
Ahmed Alabsi – Legal Affairs Manager, aalabsi@tra.org.bh
Jean Pierre Scerri – Legal Advisor, jpierre@tra.org.bh

P.O. Box 10353, Kingdom of Bahrain
Tel +973 1752 0000
Fax + 973 1753 2125
7. The Company

Detecon International GmbH
We make ICT strategies work
Detecon is a consulting company which unites classic management consulting with a high level of technology expertise.

Our company’s history is proof of this: Detecon International is the product of the merger of the management and IT consulting company Diebold, founded in 1954, and the telecommunications consultancy Detecon, founded in 1977. Our services focus on consulting and implementation solutions which are derived from the use of information and communications technology (ICT). All around the globe, clients from virtually all industries profit from our holistic know-how in questions of strategy and organizational design and in the use of state-of-the-art technologies. Detecon’s know-how bundles the knowledge from the successful conclusion of management and ICT projects in more than 160 countries. We are represented globally by subsidiaries, affiliates, and project offices. Detecon is a subsidiary of T-Systems International, the business customer brand of Deutsche Telekom. In our capacity as consultants, we are able to benefit from the infrastructure of a global player spanning our planet.

Know-how and hands-on expertise
The rapid development of information and telecommunications technologies has an increasingly significant influence on the strategies of companies as well as on the processes within an organization. The subsequent complex adaptations affect business models and corporate structures, not only technological applications.

Our services for ICT management encompass classic strategy and organization consulting as well as the planning and implementation of highly complex, technological ICT architectures and applications. We are independent of manufacturers and obligated solely to our client’s success.

Detecon International GmbH
Sternengasse 14 - 16
50676 Cologne
Phone: +49 221 9161 0
E-Mail: info@detecon.com
Internet: www.detecon.com