Final report for the Dutch Ministry of Economic Affairs

The role of government in the Internet

18 April 2013

James Allen, Nico Flores

Ref: 35894-162

Contents

analysys mason

Analysys Mason Limited
Bush House, North West Wing
Aldwych
London WC2B 4PJ
UK
Tel: +44 (0)845 600 5244
Fax: +44 (0)20 7395 9001
london@analysysmason.com
www.analysysmason.com
Registered in England No. 5177472

1 Executive summary

Over the last twenty years, the Internet has gone from being a research network used mainly by academics to being a key part of countries' infrastructure. Internet availability, accessibility, privacy and other issues are now all matters of public interest, increasingly eliciting strong views from different industries, civil society and consumers. "Internet governance" looks set to become an increasingly important part of national and international governance.

In this context, in late 2012 the Dutch Ministry of Economic Affairs ("the Ministry") commissioned Analysys Mason to conduct a study into the role of government in the Internet, of which this is the final report.

The project's first objective was to develop a map of the Internet in terms of the different types of commercial player involved – that is, a map of the Internet value chain. While several aspects of the Internet (e.g. broadband networks, e-commerce, online piracy) have already been the focus of policymakers' attention in recent years, it was felt that an overall, systemic view was a necessary first step before a more substantive discussion could be had.

The second objective was to develop a framework for answering the question of the role of government. This involved considering a variety of public interests of relevance to the Internet, and the extent to which their protection (or encouragement) should be a matter for government's attention.

The third main objective was to apply our framework in detail to four specific sectors in the Internet value chain. In doing this, our aim was both to show how our general approach could be applied to specific cases, and also to explore some key issues of interest to government in some detail.

Both our general framework and case studies touch on a central issue in Internet policy: the relationship between, on the one hand, openness policies like net neutrality and interconnection, and, on the other hand, innovation and the provision of a "level playing field". Our final objective is to outline the issues that arise on this front.

1.1 The Internet value chain

Just what is the Internet? The answer to this deceptively simple question is anything but straightforward. On one level, the Internet can be seen as the collection of websites and other online services that people use, plus the networks used to reach them. But this view hides important subtleties. For example, many of the networks that carry Internet traffic are owned by operators that provide traditional telephony and TV services, both of which compete with some of the online services that the Internet makes possible – and yet, these conflicting uses coexist on the same infrastructure. In addition to being a collection of technical systems, the Internet is also a complex ecosystem of business practices.

Although end users are normally unaware of what is involved, multiple types of service provider play a role even in simple activities like viewing a web page. At a high level, the types of service provider involved can be grouped into the four following top-level **sectors**:

1. **Online services:** what the Internet gives access to and what end users care about – from popular websites to application-based services like Skype. These are typically financed by advertising or through direct payments by end users (in this report, "end users" may be businesses or individuals)
2. **Internet connectivity:** the transportation of data between online services and end users. This includes the core network and access to it via Internet service providers (ISPs), which connect end users to the rest of the Internet
3. **Access:** the provision of last-mile networks (mainly cable, DSL and mobile) linking ISPs to end users. In most cases, access to the last mile is included in the retail services offered by the ISPs, but they in turn may buy access as a wholesale service from access network operators
4. **Devices:** end users' window into the Internet, typically paid for directly by end users, but possibly with some element of subsidy from contracts (e.g. smartphones).

Additionally, we consider two traditional, pre-Internet types of service that have an important relationship to the Internet:

5. **Traditional telecoms (and TV) services:** telephony and TV offered to end users
6. **TV content:** that is, the provision of video content meant to be consumed on TV sets.

Traditional telecoms and TV operators play several important roles in the Internet value chain. First, as providers of access networks, they are key **suppliers** to the Internet ecosystem and benefit from its growth. Second, traditional operators' voice and TV services (sector 5 above) **compete** with certain "over-the-top" online communications and video services (e.g. Skype, iTunes). Third, as key **intermediaries** between end users and online services they are technically in a position to discriminate as to which online services consumers can access – although in many cases regulations and/or commercial considerations may prevent them from doing so.

The six sectors are shown in Figure 1.1 below, in which red denotes sectors that either precede the Internet and/or (in the case of ISPs) in which traditional operators play a strong role.

Figure 1.1: High-level view of the Internet value chain [Source: Analysys Mason, 2013]

Within each of the top-level sectors above (numbered 1 to 6), there are several sub-sectors (e.g. consumer-facing online services, labelled 1.1), and within each of these there are further sub-sub-sectors (e.g. social networks, which are part of 1.1). For the sake of simplicity, in this report we use the term "sector" to refer to any of these entities, regardless of hierarchical level.

1.2 The role of government

As the Internet becomes increasingly important to economic and social life, it is legitimate for government to ask when and how the public interest is at stake, and when it is, whether and how it should be protected. Specifically, below we consider the following questions:

- When is government intervention called for in order to safeguard public interests?
- What are the public interests at stake in the Internet?
- When will the market under-provide these interests?
- How can the government intervene, when appropriate?

When is government intervention called for?

Government intervention may be called for when the market, left to itself, is likely to yield outcomes (or has in the past yielded outcomes) that fall short of the standards that society sees as necessary –

that is, when the market **under-provides** on **public interests**. An example is the degree to which individuals' privacy should be observed.

Here, what "society sees as necessary" is an essentially political question, and this leads to two important observations: first, there is no a priori reason why its answer in different contexts should necessarily coincide with market outcomes (although, as we will see, sometimes this may be the case).

Second, in this report we do not attempt to answer the question of how far, and at what cost, public interests like privacy should be pursued. Rather, we merely aim to show how the public interests are involved in the Internet, how they may at times clash with market forces, some ways in which governments can intervene, and some of the key trade-offs that would be involved.

What are the public interests at stake?

Citizens, consumers, businesses and the wider society have an interest in ensuring that end users continue to benefit from the Internet's strengths while minimising their exposure to its risks and downsides. This involves, among other things, ensuring that:

- the Internet is widely **accessible** to everyone
- the Internet as a whole, and its key online services and networks in particular, can be relied upon to be **available** day to day – even if no central entity is ultimately responsible for the system's functioning
- the Internet continues to be **open** so that
  - **innovation** continues, benefiting end users and generating growth
  - **pluralism** and free expression continue to be a hallmark of the Internet
- users' **privacy** is protected, even (or especially) when online business models rely on the commercial exploitation of personal data
- users, especially minors, are **safe** from inappropriate or illegal content
- technical systems are **secure** from malicious attacks, which in turn can, e.g. disrupt availability or expose private or confidential information.

These interests are not absolute. While arguably they are all desirable in the general, abstract terms above, in practice their delivery often involves difficult, case-by-case decisions about:

- the **price** that stakeholders should be prepared to pay in pursuit of each interest; these costs may be directly financial or of a different nature (e.g. a distortion of markets)
- **trade-offs** between interests – for example, in pursuit of security, online services may require their users to authenticate themselves using "two factors" (e.g. a password and a number generated by a portable device), but this could compromise accessibility for some users.

Often there is no single valid answer to these questions; in the context of public policy decisions, the dilemmas involved are essentially political.

On the basis of discussions with the Ministry we have chosen four specific public interests as our focus in this study. These are availability, openness, privacy and security.

When will the market under-provide the public interests?

The fundamental question for government is: when are market forces alone unlikely to lead players to observe the public interests adequately – that is, to **under-provide** the public interests? To explore this question by means of an example, we consider the case of a provider of Voice-over-IP (VoIP) calling services. Arguably, it is in the provider's interest to offer a high degree of availability, since otherwise its customers might switch to the competition. Furthermore, if the provider operates in a competitive market, it will offer high availability at a price close to its own cost of providing it. In this case, we may then conclude that the public interest is enforced by the market (the "invisible hand" at work). The key enablers behind the happy outcome in this example are as follows:[1]

- **Efficient market:** a functioning market provides what customers demand, at a minimal price. This might not be the case if there is limited competition or information, or in the presence of externalities.

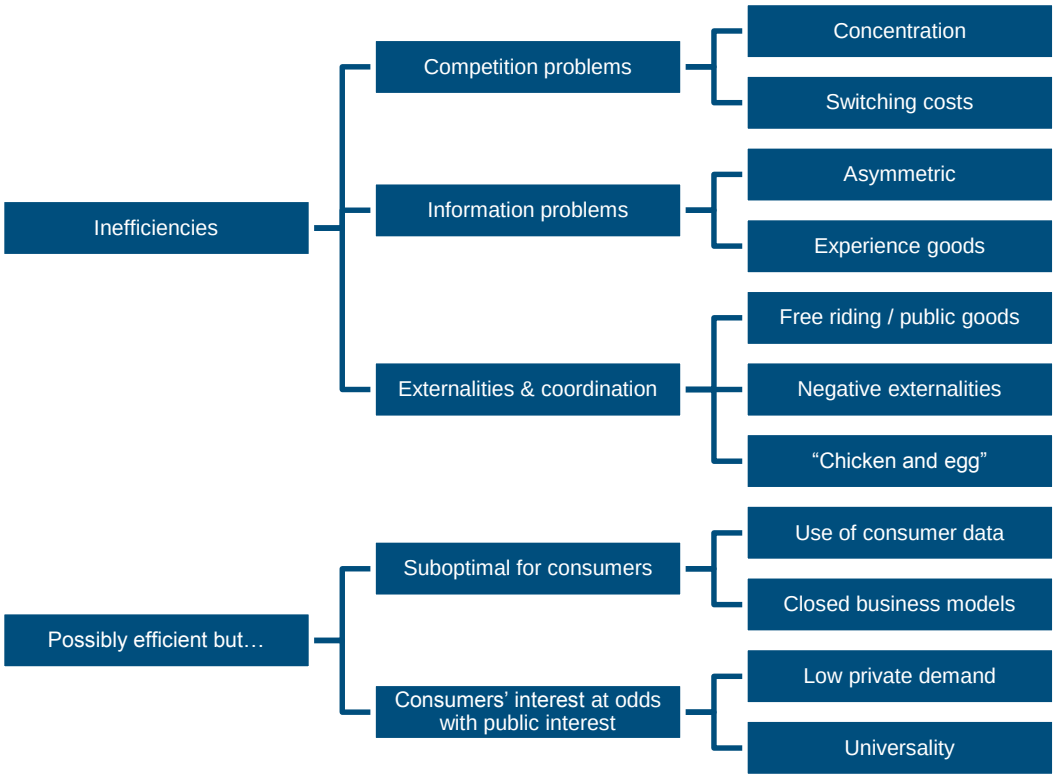
- **Efficient outcomes aligned with end users' interests:** competition centres on providing what end users demand, at low cost. This might not be the case where providers' business model involve balancing users' satisfaction with that of other customers (e.g. advertisers).

- **Alignment between efficiency and the public interest:** the market's efficient outcome (high availability) is desirable not only from the point of view of consumers, but also from that of the public interest. In other cases, it is possible that consumers' interests could fail to be aligned, or could even be at odds, with wider public interests (for example, a consumer might prefer not to pay a premium meant to subsidise universal provision of a service).

In turn, these broad drivers of under-provision can be broken down into sub-types. On the basis of analytical work, as well as drawing on the detailed case studies in this report, we can identify the following potential drivers of under-provision:

[1] In economic terms, our framework amounts to accounting for (1) inefficiencies related to market power, information or externalities; (2) outcomes that may or may not be efficient but do not maximise consumer welfare; and (3) outcomes that may be efficient, and may maximise consumer welfare, but may be sub-optimal for society or citizens (as determined through policy-making).

Figure 1.2: Typology of drivers of under-provision of the public interests [Source: Analysys Mason, 2013]



Explanations and examples for each the drivers of under-provision above are given in Figure 1.3.

How can government intervene?

Government may intervene to protect the public interest in multiple ways, including:

- effecting changes in providers' behaviour (for example, around standards) through
  - the "hard" tools of direct regulation and legislation
  - "softer" tools like co-regulation or encouraging self-regulation
  - facilitating industry dialogue
  - the state's purchasing power
- effecting marketplace changes through
  - education of end users and businesses – for example, on managing security risks
  - direct government provision or contractual arrangements with private providers for the provision of essential services (e.g. PKIoverheid, discussed below)
  - direct subsidies
- working with other governments and/or Internet governance organisations and/or industry to agree on technical standards and business practices.

The optimal approach to be used varies from case to case. Drawing on the case studies in this study, Figure 1.3 lists specific policy tools that may apply for each type of under-provision.

Figure 1.3: Drivers of under-provision and intervention options [Source: Analysys Mason, 2013]

Driver	Description	Intervention options
Concentration / limited alternatives	• Limited choice of providers may force users to tolerate bad service or features they do not like	• Lower barriers to entry – e.g. by limiting network effects through mandated interconnection/interoperability • Economic regulation (in specific, limited, circumstances) • Minimum standards
Switching costs	• Buyers may be not be able to change providers easily	• Education regarding redirection facilities, future switching costs • Mandate or encourage shared standards • Mandate data portability
Asymmetric information	• Buyers may lack visibility into providers' observance of a public interest	• Mandate disclosure on essential facts (e.g. security breach notifications, KPIs) • Require independent (forensic) auditing • Standards which allow consumer branding for high quality • Education regarding "what to look for"
Experience goods	• Buyers who have never experienced the benefits of a service may under-value it	• Education • Mandated minimum quality of service criteria • Use of government procurement to encourage adequate provision
Free riding (public goods)	• A provider may experience no negative impact from failing to observe a public interest	• Require minimum standards • Standards which allow consumer branding for high quality • Education of end users regarding responsible behaviour
Missing or insufficient liability (negative externalities)	• The cost of a provider's failure to observe a public interest may be borne mainly by third parties	• Ensure that liability is placed on parties that can cause harm • Minimum standards
Coordination difficulties: "chicken and egg"	• An activity may only be commercially attractive if most other providers join	• Use public procurement as strategic commitment to secure buy-in • Convene and coordinate stakeholders – e.g. for standard-setting • Break deadlocks by making move (e.g. adoption of new standards) mandatory • Direct provision by the State (if no commercial player)
Exploitation of end-user data	• Providers may have an interest in exploiting customer data	• Education of end users regarding what they are disclosing • Direct regulation
Closed business models	• Providers may prefer a closed business model over an open one if it is more profitable	• Mandated interconnection/interoperability • Mandated open access • "Must carry" and associated requirements • Use of government procurement in targeted ways (e.g. prefer open solutions where these are advantageous)

Driver	Description	Intervention options
Low private demand	• As private consumers, end users may give low value to the public interests	• Education • Mandated minimum quality of service criteria • Use of government procurement to encourage provision
Lack of universality	• Providers may fail to offer a service to all end users at an acceptable price	• Subsidies/universal service provisions (in limited circumstances) • Assistance with coordination mechanisms (e.g. assist rural communities to build true picture of demand)

1.3 Case studies

As part of this study, we have applied our framework above to four specific parts of the Internet value chain; these are highlighted in Figure 1.4 below (and for simplicity are called "sectors" just like the higher-level entities of which they are sub-categories). In each case we have considered the relevance of a specific public interest and assessed to what extent the market its provision can be left to market forces alone. The cases chosen are:

- security in certificate authorities (a type of authentication provider, part of sector 1.3)
- openness in connected TV (sector 4.4)
- privacy and openness in social networks (part of sector 1.1)
- availability of cloud hosting services (part of sector 2.2).

This is illustrated in Figure 1.4 below.

Figure 1.4: Overview of case studies. Numbers in circles refer to the case studies in this report [Source: Analysys Mason, 2013]

The case studies were chosen in consultation with the Ministry and reflect areas of active policy concern. Apart from the direct value that this exercise may yield to government, it is also intended as an illustration of how our framework could be used in other cases. Each case study includes:

- a brief analysis of the sector in question
- a discussion of how the public interest under study is relevant in this sector
- a discussion of the government's perspective, including
  - an application of our framework of market under-provision
  - a review of the current policy/regulatory status quo and
  - a discussion of the case for (or against), and options for, intervention.

1.3.1 Security in certificate authorities

Certificate authorities (CAs) provide solutions that enable online services to communicate securely with their users. Recent years have seen a number of successful hacker attacks on CAs themselves, undermining the guarantees they provide and leading to widespread concerns about online services' security. To a significant extent, this violation of security is likely to be due to a combination of information asymmetries preventing CAs' customers from verifying CAs' security arrangements, and CAs' liability being far lower than the system-wide losses that could be caused by a major security breach. Fortunately, legislation to address some these problems is already being drafted.

Introduction to the certificate authority sector

CAs are trusted entities that, relying on cryptographic techniques, issue small computer files ("certificates") that allow their bearers to (i) "sign" electronic files digitally, (ii) prove to counterparts in electronic communications that they are who they claim to be (authentication), and (iii) communicate privately (encryption). There are several types of CAs and certificates. "Qualified" certificates are regulated by European and Dutch law and allow their users to sign digital documents legally, online or offline, relying on EU Directive 1999/93/EC and its implementation in Dutch law. Under its PKIoverheid scheme, the Dutch government oversees CAs responsible for qualified certificates as well as for other types of certificates used for government business. By contrast, most other types of secure communications over the Internet, including secure Web browsing (e.g. for online banking), rely on unregulated "SSL" certificates and CAs.

Security and certificate authorities

In recent years, on several occasions hackers have successfully gained control over a number of CAs, including Dutch CA Diginotar, and used this control to issue themselves illegitimate certificates allowing their bearers to (falsely) identify themselves as well-known services such as Google and Skype. Through attacks of this type, as well as others, perpetrators have been able to intercept end users' private communications and/or impersonate legitimate businesses, in turn leading to online fraud and identity theft.

The government's perspective

In terms of our framework, at first sight this situation may seem unexpected. With no clear conflicts of interest, CAs in principle have the right incentives to invest in their own security, as otherwise their customers (i.e. online services, which may rely strongly on CAs' security) would switch to the competition. However, CAs' financial exposure in cases of security breaches is far smaller than the potential system-wide losses that a security breach might lead to, which limits their incentives to invest in security (a **negative externality**). Additionally, problems of **information asymmetry** mean that CAs' customers lack visibility over CAs' security arrangements, which can have similar effects. Finally, there are **coordination challenges** involved in adopting certain secure standards that could make successful attacks less likely.

A current EU proposal on e-signature regulation (extending European directive 1999/93/EC provides for electronic signatures) seeks to address some of the underlying factors that have led to these failures. In particular, yearly audits and liability for losses arising from security breaches would be imposed on all CAs, thereby reducing information asymmetries and problems of limited liability (currently these provisions apply only to qualified certificates). Our analysis suggests that these measures should help improve security, as should the imposition of minimum terms of service for CAs. Technology may also be able to play a key role in strengthening security, in particular with new standards such as DANE. Government may be able to help this by coordinating and encouraging providers to adopt the new technologies.

Impositions applying only to European CAs could risk placing these providers at a disadvantage versus overseas counterparts. The effectiveness and viability of secure standards depends strongly on widespread implementation across the Internet. Ultimately therefore solutions are likely to call for a coordinated international approach – possibly at a global level.

1.3.2 Openness in connected TV

In this study, by connected TV platforms we mean "connected" TV sets and other devices that allow consumers to view content from online services. Providers of connected TV platforms are generally free to decide what online content providers users can access, and while traditionally this has meant that only a few services were available in each platform, recently some providers have moved towards a more "open" model in which consumers can choose content providers from "app stores". By contrast, "must carry" obligations require traditional TV platforms (e.g. cable TV) to carry public broadcasters, partly as a way of ensuring that consumers have access to a wide variety of views. The question thus arises as to the best way to ensure pluralism in connected TV – and, in particular, whether or not the imposition of "must carry" rules for connected TV may be the best way of achieving that. These and other related issues are expected to be discussed in the forthcoming EU green paper on connected TV.

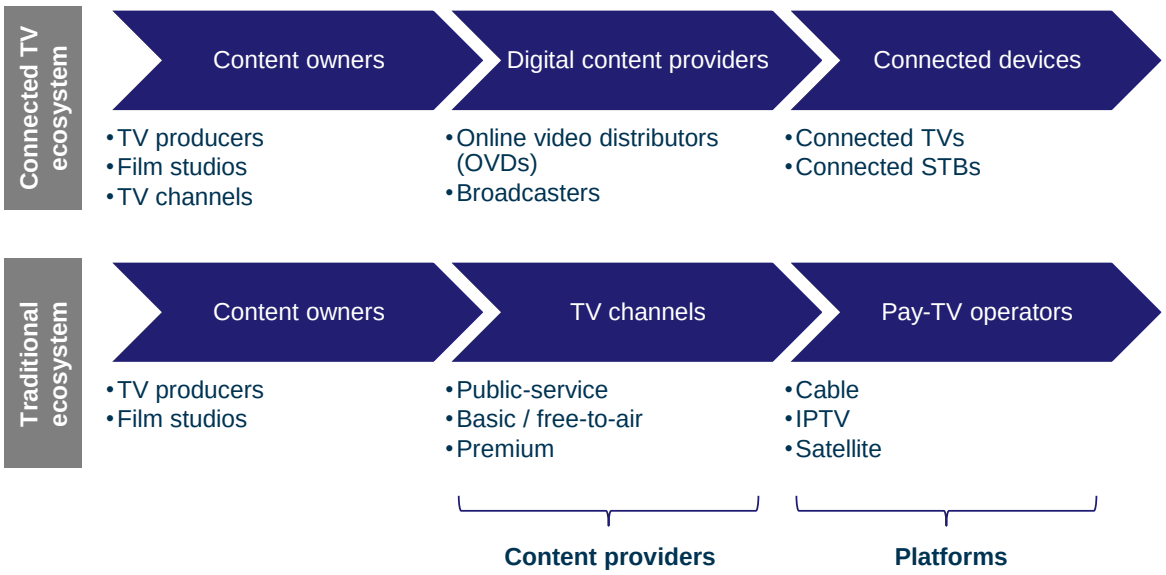
Introduction to the connected TV sector

In this case study, by "platform" we mean a service whose role it is to allow end users to access other providers located upstream in the value chain – whom we call "content providers". In the case of connected TVs, the role of platforms is played by connected devices that allow users to view video content from online services – these include "smart" TVs like Samsung's Smart TV, dedicated set-top boxes like Apple TV, and game consoles like Microsoft's Xbox. The role of content providers is played by online video services which are accessible using connected devices via the Internet ("over the top"), such as Videoland or Uitzendinggemist.nl.

In addition, we also consider the case of traditional TV distribution (or pay TV), so that we can draw a parallel between traditional and new ways of distributing TV content. In the case of traditional TV, the platforms are the traditional operators, e.g. cable companies or telecoms incumbents offering IPTV services, – and the role of content providers is played by TV channels.

This is illustrated in Figure 1.5Figure 1.4 below.

Figure 1.5: The connected TV and traditional TV ecosystems [Source: Analysys Mason, 2013]



Openness in connected TV

By an "open platform", we mean a platform whose provider exercises limited or no discretion as to which content providers can be accessed by end users. Neither connected nor traditional TV platforms are fully open in this sense, and in both cases this can partly be attributed to historical, technical limitations:

- in the case of early connected TVs, a lack of interoperability standards and other limitations used to mean that only a few content providers could be carried by a platform
- in the case of traditional TV, bandwidth limitations traditionally meant that there was only room for a limited number of channels.

However, as technology evolves these limitations are being overcome. Thus, with the advent of "app stores" platform providers are evolving towards a more open model in which all content providers are welcome (with exceptions); and with increasing capacity, traditional TV operators can carry hundreds of channels. Although a removal of the technical basis of discrimination does not imply that an open regime will necessarily follow, early signs are encouraging.

In both cases, it is worth distinguishing between carriage (that is, whether a content provider is available at all) and prominence (how easy it is to find a content provider). In the case of connected TV, this mainly means deciding which content providers are listed in the all-important "start screen" that users see when they switch on their devices. In the case of traditional TV, prominence is largely a matter of the slots to which TV channels are assigned in the Electronic Programme Guide (EPG). Even if platforms become fully open in terms of carriage, by its nature prominence will always remain a scarce asset that cannot be given equally to all content providers; as a result, it is likely to continue to play a key role in platforms' relationships with content providers.

The government's perspective

In terms of our framework, the concern here is that platform providers' business models may not always be aligned with ensuring consumers' access to all content providers, thereby potentially limiting pluralism and innovation in online services. For example, platform owners may also be in the business of providing content (vertical integration), and may have an interest in preventing access to other content providers. Legally, providers of connected TV platforms have full discretion as to which content providers they carry and how prominently they are featured. By contrast, under "must carry" rules traditional TV platforms are obliged to carry public broadcasters' channels.[2] Thus the two TV ecosystems are clearly different.[3]

This situation gives rise to two questions. First, should openness conditions be imposed on connected TV platforms? This would be a case of extending the openness rationale of net neutrality, with its basis on considerations of innovation, free expression and pluralism, to connected TV – going from the ISP-centric "network neutrality" to a concept of "net neutrality" applicable at multiple points in the value chain..[4] We note that the market may already be evolving in this direction naturally; if so, government's intervention might best be directed at removing the obstacles in this– for example, by supporting coordination around key standards.

Second, should the regimes for connected and traditional TV be harmonised, either by "levelling up" and introducing "must carry" requirements on connected TV, or "levelling down" and removing

2 "Must carry" channels include the national/regional/local Dutch PBS channels and the three channels of the public Belgian broadcaster.

3 Although general competition law always applies.

4 We note that a similar question has recently been raised in France by the Conseil National du Numérique, and at the European level by BEREC. See *Rapport relatif à l'avis net neutralité No. 2013-1 du 1er mars 2013,* available at http://www.cnnumerique.fr/wp-content/uploads/2013/03/130311-rapport-net-neutralite-VFINALE.pdf and *Overview of BEREC's approach to net neutrality,* (especially p 4) available at http://berec.europa.eu/files/document_register_store/2012/12/BoR_(12)_140_Overview+of+BEREC+approach+to+NN_2012.11.27.pdf.

requirements on traditional TV? "Must carry" rules aim to ensure universal access to public service (and selected other) broadcasters. In turn, the rationale for this is partly to ensure consumers' exposure to a wide range of views – that is, pluralism again. It is partly a result of traditional platforms' capacity limitations that this has traditionally been a responsibility of public broadcasters (in the programmes that they show), rather than of platform providers (in the content providers that they carry).

Thus, in the case of connected TV perhaps the right question is not whether "must carry" should be introduced but rather how pluralism can be secured in this context, and specifically whether openness in general is a more adequate means towards this end (and, as noted above, as technology develops, universal carriage of all content providers may well become commonplace in any case).

As for removing or reducing "must carry" obligations from traditional platforms ("levelling down"), the case for this depends on whether it is believed that widespread viewing of public service broadcasting on traditional platforms remains essential for the overall delivery of policy objectives such as plurality, social cohesion and civic engagement. These questions are beyond the scope of this study.

Perhaps a more pertinent policy tool than "must-carry" is EPG prominence. Without high visibility, public service content may go unnoticed, and if only content providers of certain types (e.g. entertainment and sport) or persuasions are given prominence, plurality would suffer. Although no such rules apply in the Netherlands,[5] the nature of traditional platforms (i.e. a linear "dial" of channels in the EPG) means that public broadcasters are not difficult to find. By contrast, in connected TV platforms a public broadcaster might only be located through a search engine (if at all). Introducing requirements on prominence in the Netherlands, for both traditional and connected TV platforms, might not only effectively harmonise the situation for all platforms, but also ensure the findability of public service content on new platforms. Exactly what requirements these should be, and what types of content should be covered, would be a key question for further study.

Again, all of these options require international collaboration – not least because the applicability of current EU directives to the case of connected TV is unclear at best. We note that the upcoming EU green paper on connected TV is expected to address many of the issues discussed here.

1.3.3 Privacy and openness in social networks

In the context of communication networks such as VoIP platforms or online social networks, by "openness" we mean interconnection – that is, users' ability to interact with users of competing platforms. A lack of openness not only limits the benefits for users in a direct way but also, through network effects, may lead to "winner takes all" situations in which a platform becomes dominant, which in turn may potentially allow it to – for example – impose abusive privacy terms on its users. These concerns have been voiced extensively in connection to major social networks, and regulations are being drafted to address the main concerns.

5 Currently, both the UK and Germany mandate prominence of public service content on the EPGs of traditional TV platforms.

Introduction to the social network sector

Social networking is a highly concentrated space. Although the last decade has seen numerous social networks try to succeed, in each national market the space has generally tended to concentrate around one or two leaders. In. general, this is the result of strong positive network externalities, which means that the value of joining a network increases with the number of contacts that a prospective member already has inside the network. Importantly for this case study, most social network platforms are in the business of collecting and processing a wealth of information about their users, which they can also use for targeted advertising and other purposes.

Openness and privacy in social networks

This dual situation (market concentration and platforms' interest in personal information) gives rise to concerns about the potential for abuse of market power, and in particular about platforms' possible incentives and power to maintain low privacy standards. The record suggests that these concerns may not be entirely misplaced, with incidents in recent years of social networks unilaterally changing privacy policies, eventually triggering lawsuits and government interventions in the USA.

The government's perspective

In terms of our framework, the main likely causes of under-provision of privacy are that:

- users seem to have limited motivation to engage with privacy options (**low private demand**)
- major social networks have high **market power** as a result of network effects
- **switching** platforms is difficult if users' personal data and content is not "portable" across providers
- users may have no visibility on uses to which their data is put (**asymmetric information**)
- social networks' **business models** are based on the exploitation of end-user data.

The Data Protection Regulation currently being considered by the European Parliament seeks to address many of these issues. Key provisions under discussion concern service providers' ability to use customers' data for unauthorised purposes and to unilaterally change terms and conditions; and consumers' ability to erase their records from online providers' databases and to transfer their data across providers, thereby facilitating switching.

Forced interconnection between social networks is not currently part of the proposals. In our view, while this might potentially be effective in reducing market power, it would be a drastic measure, with potentially adverse effects on innovation (as we discuss below) and whose justification is not clear at this stage.

Given the global nature of the players involved, at a minimum an EU-level approach is needed, since this allows enforcement for players with EU subsidiaries. Nonetheless, we note that emerging and/or specialised social networks may have no EU offices and are likely to pose jurisdictional and enforceability challenges.

1.3.4 Availability of cloud hosting

In our final case study, we consider the issue of (problems with) availability in cloud hosting services – that is, the underlying infrastructure behind many online services. Unlike the situation in other case studies, here we see no compelling evidence or arguments suggesting that the market is likely to under-provide availability at an adequate price. This is not to say that there are no potential concerns. Two key concerns are the possibility of systemic failure stemming from complex interdependencies among providers. Intervention options include education of small businesses on ways of maximising resilience in case of cloud outages.

We stress that our analysis is only concerned with failures by cloud providers to provide availability to clients that are themselves online services. Questions of privacy or the availability of services targeting end users are outside the scope of this case study.

Introduction to cloud infrastructure providers

In this case study, by "cloud computing" we understand the provision of IT resources as services. By "as services" we mean that resources can be provisioned and discarded with little or no notice, typically automatically. Our focus in this case study is the use of outsourced cloud services as the infrastructure behind online services targeted at end users. For our purposes, cloud computing offerings can be segmented along two dimensions of customer need: value-add and geographical sensitivity:

- **Value add** – the "stack": cloud computing services can be categorised according to the level of functionality (or "abstraction") offered, ranging from basic resources such as servers and storage ("Infrastructure as a Service" or "IaaS") to more elaborate building blocks for online services such as database services ("Platform as a Service", or "PaaS"), to end user-ready online software ("Software as a Service" or "SaaS").

- **Geographical sensitivity**: thanks to the Internet, cloud service provision is to a large extent a global market. When customers are indifferent as to where their data is stored or processed, they can source resources from anywhere in the world. However, in practice they are not always indifferent as to location. Factors that may prevent customers from sourcing providers globally include compliance with law or contracts, connectivity, confidentiality, unique technical requirements and cultural factors.

In terms of these dimensions, the following six high-level categories can be identified.

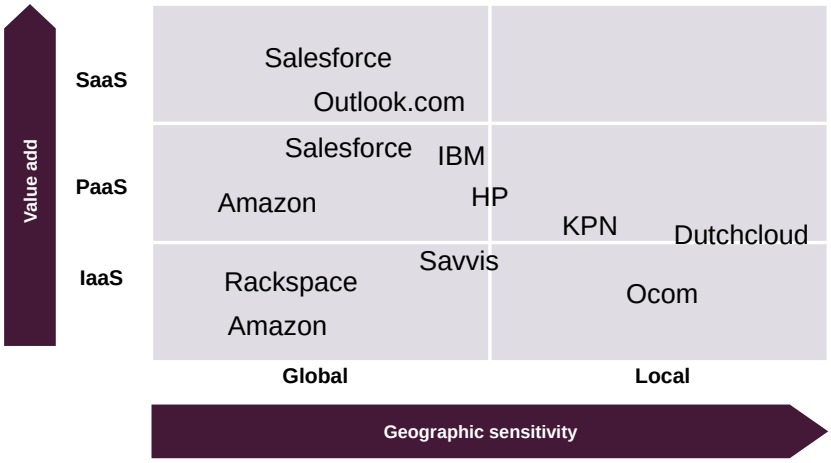


Figure 1.6: Segmentation of the cloud services space (firms' positioning is indicative; some firms are present in more areas than indicated)[Source: Analysys Mason, 2013]

Availability in cloud hosting

By a lack of cloud availability, we mean a loss of service in a cloud service supplied to an online service provider, so that the online service's availability to end users is disrupted, and/or the service owner cannot control its own service. An outage by a major provider can have significant consequences and can affect millions of end users.

Recent research[6] by cloud firm Rightscale found that in 2012 there were only 27 "notable" cases worldwide, of which only about a third (around 10) involved services in the SaaS or IaaS categories, and 21% were due to natural disasters; the average downtime was around eight hours.

The government's perspective

A preliminary application of our framework to the case of cloud providers suggests several potential issues for consideration; however, on closer inspection not all of these concerns seem justified. Thus:

- **Limited alternatives**: market concentration around low-cost players could mean that buyers are unable to negotiate adequate availability guarantees. However, although the market is relatively concentrated at the low-price commodity end, it also contains a variety of providers that offer higher levels of reliability – at a higher price.
- **Switching costs**: if switching costs are high, customers may be forced to accept poor service quality. However, while lock-in is certainly seen as a concern by industry participants, we note that both technical developments (e.g. Openstack) and new business models (e.g. Rightscale) aim to help customers decrease their reliance on single providers.
- **Lack of liability**: a lack of proportionate liability might lead providers to under-invest in availability. However, while it is certainly the case that some entry-level providers only offer very limited liability in case of outages, this does not necessarily mean that higher liability contracts are over-priced.

6 See http://blog.rightscale.com/2013/02/27/lessons-learned-from-recent-cloud-outages/

- **Experience goods**: the nature of availability means that, because outages are relatively rare, customers may be undervalue technologies designed to maximise availability, and thereby fail to make the necessary investments. Given the increasingly interconnected nature of cloud services, this may entail systemic risks.

The above suggests that availability is unlikely to be under-provided at least in the sense of the market meeting demand efficiently. However, the question of **systemic risks** remains. Also, there are questions of access to cloud computing for small online businesses: even if availability is not priced inefficiently, this may still mean that small online start-ups cannot afford the levels of availability that they require. While this in itself is not enough to qualify as under-provision in our sense, if ensuring that such businesses succeed is a policy aim, then government could consider intervening.

As part of its Digital Agenda, the EC has recently published a cloud strategy document[7] outlining potential areas of intervention. Relevant points include concerns about vendor lock-in, the corresponding need for cross-vendor standards and certification, and cloud customers' difficulties in negotiating contracts, especially in the case of small firms purchasing services from large providers which may offer "take it or leave it" contracts.

Besides introducing formal regulation, government may be able to help mitigate the concerns listed above by:

- **educating** cloud customers – especially small firms – about techniques for ensuring continued availability even when a cloud provider becomes unavailable. While larger firms are gaining expertise in these techniques, smaller firms may find this more challenging
- working with industry to help produce and implement **open standards** (e.g. Openstack) that allow customers to achieve resilience by not relying on a single cloud provider.

Regulatory and standards-based options call for EU-level approaches; standards-related work may also call for global-level coordination. On the other hand, education-based options can be pursued at a national level.

We stress that our analysis is only preliminary, and that our failure to find conclusive grounds for intervention does not necessarily imply that intervention is unwarranted. We suggest that in coming years policymakers continue to monitor the key issues mentioned here – in particular, degrees of market concentration and the "tail risk" of systemic outages.

1.4 Openness, innovation and a level playing field

In our discussion so far "openness" has been presented in two guises: as non-discrimination in the case of connected TV platforms, and as interconnection in the cases of social networks. What both concepts have in common is the idea that providers of open services do not refuse to carry, connect to,

[7] European Commission: "Unleashing the Potential of Cloud Computing in Europe". Available at http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

or otherwise **interoperate** with other service providers when this is of value to end users, and do so on a non-discriminatory basis.

Although so far openness has been presented as one among many different public interests, in many ways its role is more important than that. Arguably, openness in the form of non-discrimination (or "net neutrality") is one of the Internet's defining characteristics. However, openness is by no means present everywhere in the Internet, and arguably where it is present it also carries some costs.

Thus, although openness in networks (that is, net neutrality) may well be key to the high degree of innovation and competition seen in online services, arguably this has also meant a ISP sector with limited scope for service differentiation among providers, and has led to concerns – which may or may not be ultimately justified – about the intensity of competition and the viability of future infrastructure investments.

In turn, this raises the issue of regulatory asymmetries between online services and traditional telecoms services. While telecoms providers are subject to openness requirements not only in terms of network neutrality but also in terms of interconnection, no parallel requirements apply to either connected TV platforms or to social networks, and the same can be said of other cases. Should these asymmetries be addressed, thereby effecting a level playing field? As suggested by the case of connected TV, the answer likely depends on the extent to which these fields are comparable as well as the ultimate policy goals involved. In general, some key considerations that policymakers should bear in mind include the following:

- The profits that closed business models can generate may be key drivers of investment and **innovation** in online sectors.[8] Any potential short-term, static benefits of mandated openness should be weighed against the potential dynamic, long term effects on future investments in online sectors.

- The likelihood of any resulting market power being **durable** should be assessed carefully. For example, Myspace was a dominant social network only a few years ago, only to be relegated to relative obscurity by Facebook. The same could happen in the next few years. "Schumpeterian innovation" may be a natural antidote to online players' market power.

- The potential **harm** to the public interest that can be caused by a lack of openness varies from one case to the next. For example, the public interest is relatively unharmed by an online game that does not interoperate with other games.

None of this should be taken to imply that asymmetric regulations are always desirable, or that openness requirements should only be applied to network operators. Rather, we suggest that openness policies may entail a certain degree of industrial policy, encouraging innovation in some sectors while possibly restricting it in others.

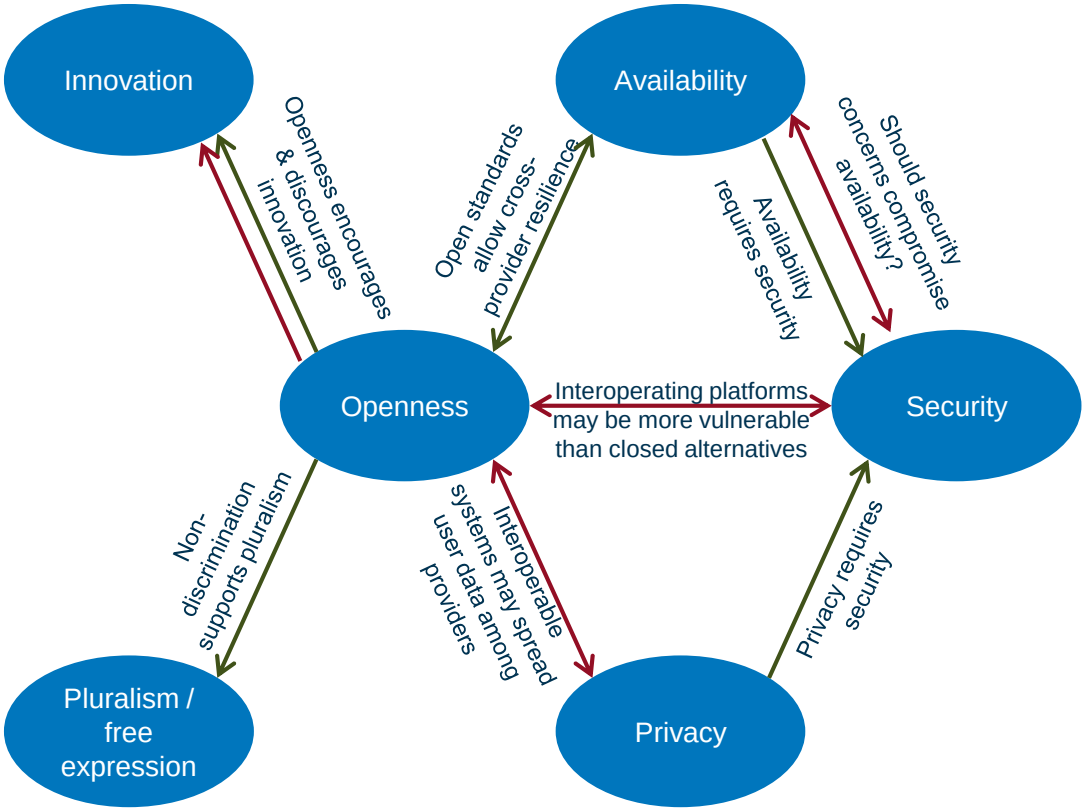
[8] For a recent, informative discussion on this topic in the context of social networks, see Justin Fox, "The New Monopolists" in *The Atlantic*, January 2013, available at http://www.theatlantic.com/magazine/archive/2013/01/the-webs-new-monopolists/309197/.

1.5 Conclusions

Our aims in this study were to provide a picture of the Internet value chain, show how the public interests relate to different types of player, and on the basis of this produce a framework for government intervention when market provision is unlikely to meet the public's needs. We have also explored how this applies to four case studies, both as a way of exploring certain key issues and of showing how our framework can be applied.

As we discussed earlier, the various public interests involved in the Internet include difficult trade-offs that are inherently political decisions. The main relationships between public interests are shown in Figure 1.7 in which red arrows denote tensions and green arrows denote dependencies:

Figure 1.7: Key relationships between public interests [Source: Analysys Mason, 2013]



Over the next decade, as the Internet's importance to society grows even beyond current levels, the complex set of relationships between public interests is set to become increasingly important to policymakers. There are no easy solutions, and with industries pitted against each other the arguments on each side of the main trade-offs are likely to be articulated in increasingly sophisticated ways. Policymakers will need to master the issues and be prepared for a series of potentially difficult, case-by-case decisions. We hope that this report will provide a useful start in this area.

2 Introduction

2.1 Context

Over the last twenty years, the Internet has grown into a central part of countries' infrastructure. Its impact across the economy – from media to retail to e-government to telecommuting – has been transformative to the point that life before the Internet now seems hard to imagine. Perhaps the single sector that has changed most is telecommunications, for which the Internet has simultaneously been an important new business and a serious disruptor of established models.

The Internet's impact goes beyond the economy. Email, blogging, social networks and free-at-the-margin global voice communications mean that both social and political life has also changed in important ways. As a result, the Internet matters to consumers and citizens, and issues of Internet policy and governance are no longer a specialist interest. From ACTA to net neutrality to calls for universal access in election manifestos, increasingly the Internet is a matter of public interest. For governments, this calls for a systematic assessment of the Internet from the point of view of the public interest.

2.2 Project objectives

In late 2012, the Dutch Ministry of Economic Affairs ("the Ministry") commissioned Analysys Mason to conduct a two-phase study into the role of government in the Internet. The project's main objectives were to:

- understand the Internet value chain, including types of players, strategic aspects and trends
- develop a framework for answering the question of the government's role in the Internet, specifically by
  - identifying the main public interests at stake in the Internet
  - assessing to what extent players across the value chain have the ability and incentives to affect the public interests positively or negatively
- apply this framework to four detailed case studies, each focusing on a specific part of the Internet value chain in its relation to a specific public interest
- analyse implications of the above for innovation and competition.

This document is our final report for this study.

2.3 Synopsis

Our approach has been structured as follows:

First, it is important to map out what the Internet is—and what it is not. To do this, we have developed a value chain analysis of the main types of player involved in the Internet value chain. This is an essential task before any systematic discussion can take place. We provide a high-level view in Section 3 and further details in Annex B.

With this in hand, we then turn to the question of the role of government in the Internet – our focus in Section 4. We begin addressing this question in Section 4.2 by considering some key public interests – availability, openness, privacy and security – whose relevance to the Internet we then examine in detail by assessing the relevance of each sector in the Internet value chain to each of the public interests. Next, in Section 4.3, we turn to the question of when government intervention may be called for. After developing a general framework to answer this question, we go through each of the public interests in turn and ask what could lead value chain players to act in a way that is not conducive to the public interests – that is, to "under-provide" the public interests. In Annex C, we apply this analysis at a high level to each sector in the Internet value chain. As a final step in our high-level analysis, in Section 4.4 we provide a set of policy tools of relevance for the different types of market under-provision.

In Section 5, we then apply our general thinking in detail to four case studies, each of which deals with a specific sector in the value chain from the point of view of a specific public interest. We review each sector in detail, consider its relationship to the public interest, assess the current policy/regulatory position, and consider where changes may be appropriate.

Although in most of this report openness is presented as one among many different public interests, in many ways its role is more important than that. Arguably, openness in the form of net neutrality is one of the Internet's defining characteristics. It has key impacts on online services (which may themselves not be open), traditional services (which are disrupted by the Internet), and ISPs (whose services may become a commodity). In turn this raises questions about the relationship between openness, innovation and competition between online and traditional services. These are discussed in Section 6.

Finally, in Section 7 we offer concluding remarks on some key issues discussed in this report and their implications for government.

2.4 Acknowledgements

Analysys Mason would like to thank staff members at the Ministry for valuable feedback contributed during this study. We also thank Nico van Eijk, of the Institute of Information Law at the University of Amsterdam, for expert advice on relevant aspects of Dutch and European public policy.

3 The Internet value chain

Just what is the Internet? The answer to this deceptively simple question is anything but straightforward. On one level, the Internet can be seen as the collection of websites and other online services that people use, plus the networks used to reach them. But this view hides important subtleties. For example, many of the networks that carry Internet traffic are owned by operators that provide traditional telephony and TV services, both of which compete with some of the online services that the Internet makes possible – and yet, these conflicting uses coexist on the same infrastructure. In addition to being a collection of technical systems, the Internet is also a complex ecosystem of business practices.

As part of this project, we developed a view of the Internet value chain comprising both traditional telecoms firms and new Internet players. Our analysis is documented in the present section, starting with a general overview of the Internet value chain, and then focusing on the top-level sectors and adjacent sectors within the value chain. The analysis developed here plays a central role in the rest of this report. Further information regarding the Internet value chain is provided in Annex B.

3.1 Overview of the Internet value chain

3.1.1 Sectors directly involved in the Internet

Figure 3.1 below shows a high-level view of the Internet value chain in which players have been organised into four **top-level sectors**.[9] These are:

- **Sector 1: Online services** – what the Internet gives access to and what end users care about – from popular websites to application-based services like Skype. These are typically financed by advertising or through direct payments by end users (in this report, "end users" may be businesses or individuals).
- **Sector 2: Internet connectivity** – the transportation of data between online services and end users. This includes the core network and access to it via Internet service providers (ISPs), which connect end users to the rest of the Internet.
- **Sector 3: Access**[10] – the provision of last-mile networks (mainly cable, DSL and mobile) linking ISPs to end users. In most cases, access to the last mile is included in the retail services offered by the ISPs, but they in turn may buy access as a wholesale service from access network operators.
- **Sector 4: Devices** – end users' window into the Internet, typically paid for directly by end users, but possibly with some element of subsidy from contracts (e.g. smartphones).

9 Strictly speaking, the entities in our value chain represent groupings of products and services. Although we refer to firms as if they belonged to one of our sectors, this should be understood as referring to firms in their capacity as providers of a product/service of a given type. Firms often span several sectors and/or offer products or services from multiple sectors as an integrated package.

10 We have chosen to list access connectivity separately from Internet connectivity in order to highlight the fact that access networks are used not only for accessing the Internet but also for providing traditional telecoms services (voice and TV), as discussed below.

Figure 3.1: High-level view of the Internet value chain [Source: Analysys Mason, 2013]

Within each of the top-level sectors above (numbered 1 to 4), there are several sub-sectors (e.g. consumer facing online services, labelled 1.1), and within each of these there are further sub-sub-sectors (e.g. social networks, which are part of 1.1). For the sake of simplicity, in this report we use the term "sector" to refer to any of these entities, regardless of hierarchical level.

3.1.2 Adjacent sectors

Our picture would not be complete if it did not also include *adjacent sectors* that are competing with or converging with the Internet. For the purposes of our study, the two main ones are:

- **Sector 5: Traditional telecoms services** – telephony and TV, offered as services to retail and business customers.
- **Sector 6: TV content** – that is, the provision of video content meant to be consumed on TV sets. This is a key input both for traditional operators' TV services and for digital content online services.

Finally, two other essential external stakeholders must be mentioned:

- **End users**, including:
  - private persons using the Internet – that is, retail consumers

— businesses that use the Internet to access services, e.g. when they rely on the Internet to access email or online software, to order supplies, or to outsource their IT[11]

- **The wider economy**, including all the businesses that use the Internet to sell, promote or distribute goods – from supermarkets to record labels to utilities.

The importance of end users and the wider economy cannot be underestimated. They are the ultimate beneficiaries of the Internet, and the justification for any public intervention. This study has been prepared from the perspective that end users' interests are paramount.

The six sectors are shown in Figure 3.2 below, in which red denotes sectors that either precede the Internet or (in the case of ISPs) in which traditional operators play a strong role.

Figure 3.2: High-level view of the Internet value chain [Source: Analysys Mason, 2013]

3.1.3 International aspects

The sectors in the Internet value chain exhibit varying degrees of globalisation, but broadly fall into two groups:

11 At the same time, businesses may also use the Internet as online service providers – for example by providing a website for their customers.

- Given their physical nature, access networks (sector 3, possibly with the exception of satellite access) are inherently local and are fully within the remit of national regulators. Traditional telecoms services (sector 5) have historically been provided by the same firms that own last-mile networks and are also subject to national regulations. ISPs (sector 2.1) offer facilities-based retail services and are also covered by telecoms regulations.

- By contrast, online services, consumer devices and most aspects of Internet connectivity are provided by global players. Although different types of services are subject to various types of sector-specific regulations (for example, online video providers cannot provide illegal content), the Internet as a whole does not fall under a single regulatory body either at a national or EU level, and many subsectors are only subject to general law (e.g. on competition). Online services accessed by Dutch users may be based outside the EU.

The second group of services may pose important challenges for policymakers when providers are based overseas. We return to this point below.

3.2 Sectors directly involved in the Internet

In this section, we describe the value chain only up to the second level of detail (for example, we discuss consumer facing online services, but not social networks). A further level of detail is provided in the diagrams included in Annex B, where the key players are also listed. We begin with those sectors that are directly involved in the Internet.

3.2.1 Online services

Online services are the Internet's reason for existing; they are what 'Internet access' gives access to. They provide value to consumers, businesses, citizens and the State, with profound impacts for all of them. We refer to firms offering online services as online service providers; their offerings can be subdivided into three sectors:

- consumer-facing online services – from social networks to digital content services
- business-facing online services – from software-as-a-service providers like Salesforce.com to the millions of websites that firms of all sizes provide for their customers ("self-provided")
- enabling services – behind-the-scenes services that makes all other services work, from online payment services to advertising networks.

Online services are mainly provided by businesses launched specifically for the Internet – from online giants like Google, Amazon and Salesforce.com to thousands of small, innovative start-ups. Firms from traditional telecoms and IT sectors have also entered this space, with varying degrees of success.

3.2.2 Internet connectivity

Internet connectivity is the set of networks, servers and related infrastructure that allow end users to reach online services – the Internet's "plumbing". It comprises:

- ISPs (on which more below)
- co-location and cloud hosting services, which provide infrastructure for online service providers;
- core connectivity providers, including
  - transit providers, which connect ISPs to the rest of the Internet
  - content delivery networks (CDNs), which connect online service providers to ISPs through expedited networks
  - Internet exchange points (IXPs), which allow ISPs to connect to each other, CDNs and other providers.
- certain key central enabling services that orchestrate the Internet's overall functioning (e.g. DNS), themselves governed through a variety of multi-stakeholder arrangements.

The ISP sector merits special mention. Its product, Internet access, is a retail public electronic communications service. It should not be confused with the "last-mile" access services and networks on which it relies (our sector 3, discussed below). Although the two services are often provided by the same firm, the ISP may rent access networks from another player (e.g. under regulated terms in some cases, such as LLU; for example, Tele2 relies on last-mile networks owned by KPN).[12]

Like the access networks they rely on, ISP services are typically provided by traditional telecoms operators. Operators are also present in all other sectors of Internet connectivity (and particularly in the Internet transit sector), but global Internet-native firms like Level 3 and Akamai play at least as large a role in this sector.

3.2.3 Access

Access refers to the provision of last-mile networks (mainly cable, DSL and cellular) linking ISPs to end users. Access is the domain of traditional telecoms players. These are typically vertically integrated so that the owners of access networks also provide ISP services as a retail product. Access networks:

- connect to end-user devices
- generally cover specific geographical areas (except satellite)
- require high capex to build and have strong economies of density, which often leads to limited competition and regulation
- may be leased wholesale to third-party ISPs, which then sell Internet connectivity and last-mile access as a single service.

3.2.4 Devices

Internet-connected devices are end users' window into the Internet – they range from the general-purpose to the service-specific. Their providers are mainly traditional consumer electronics and computer manufacturers; however, new online players have started making forays into this space e.g.

[12] Even when ISPs and last-mile providers are not the same, this is normally hidden from end users who only deal with the ISP. Last-mile access is normally sold to ISPs as a wholesale product.

Amazon's Kindle. Conversely, some electronics manufacturers like Apple have become important in the online space.

3.3 Adjacent sectors

3.3.1 Traditional telecoms services

Traditional telecoms and TV operators play several important roles in the Internet value chain. First, as providers of access networks, they are key **suppliers** to the Internet ecosystem and benefit from its growth. Second, traditional operators' voice and TV services (sector 5 above) **compete** with certain "over the top" online communications and video services (e.g. Skype, iTunes). Third, as key **intermediaries** between end users and online services they are technically in a position to discriminate as to which online services consumers can access – although in many cases regulations and/or commercial considerations may prevent them from doing so.

3.3.2 TV content

By 'TV content', we refer to the provision of video content meant to be consumed on TV sets. This includes TV channels' linear signals (both basic and premium) and individual TV programmes as well as films.

TV content has traditionally played a key role in the telecoms value chain as a key input for operators' cable-TV and multi-play services. However, increasingly TV content providers are either licensing their content to online distributors (part of the "digital content" sector in sector 1.1) or launching their own online services directly. As they do this, they open a new distribution channel that competes with operators' preferred model – even though they rely on the same last-mile infrastructure, owned by the same operators.

4 The role of government

As the Internet becomes an increasingly important part of countries' infrastructure, it is legitimate for government to ask when and how the public interest is at stake, and when it is, whether and how it should be protected.

Specifically, below we consider the following questions:

- When is government intervention called for in order to safeguard public interests in the Internet?
- What are the public interests at stake in the Internet?
- When will the market under-provide these interests?
- How can the government intervene, when appropriate?

4.1 When is government intervention called for?

The Internet has largely grown organically, with only minimal government intervention. It is partly a testament to what the market can achieve, and a warning as to what unnecessary regulations could prevent. However, governments have always played a crucial, behind-the-scenes role throughout the Internet's history – from its origin as a US government-funded network, to governments' ongoing involvement in key parts of the infrastructure such as domain name assignment and digital certificates.

As the Internet's importance to the economy and society grows, its functioning, how it is managed, and who can access it all become matters of public – and hence the government's – interest. Often, things work well under the private sector and no intervention is needed. But sometimes the market may fail to deliver what society requires from the Internet, and at those points intervention may be appropriate. The key question is thus: when are market forces alone unlikely to lead players to observe the public interest to the standards that society sees as necessary – that is, to **under-provide** the public interests?

Here, what "society sees as necessary" is an essentially political question, and this leads to two important observations: First, there is no a priori reason why its answer in different contexts should necessarily coincide with market outcomes (although, as we will see, sometimes this may be the case).

Second, in this report we do not attempt to answer the question of how far, and at what cost, public interests like privacy should be pursued. Rather, we merely aim to show how the public interests are involved in the Internet, how they may at times clash with market forces, some ways in which governments can intervene, and some of the key trade-offs that would be involved.

4.2 The public interests

Citizens, consumers, businesses and the wider society have an interest in ensuring that end users continue to benefit from the Internet's strengths while minimising their exposure to its risks and downsides. In turn, this involves, among other things, ensuring that:

- the Internet is widely **accessible** to everyone
- the Internet as a whole, and its key online services and networks in particular, can be relied upon to be **available** day to day – even if no central entity is ultimately responsible for the system's functioning
- the Internet continues to be **open** so that
  - **innovation** in online services continues, benefiting end users and generating growth
  - **pluralism** and free expression continue to be a hallmark of the Internet
- users' **privacy** is protected, even (or especially) when online business models rely on the commercial exploitation of personal data
- users, especially minors, are **safe** from inappropriate or illegal content
- technical systems are **secure** from malicious attacks, which in turn can, e.g., disrupt availability or expose private or confidential information.

These interests are not absolute. While arguably they are all desirable in general, abstract terms, in practice their delivery often involves difficult, case-by-case decisions about:

- the **price** that stakeholders should be prepared to pay in pursuit of each interest; these costs may be directly financial or of a different nature (e.g. a distortion of markets)
- **trade-offs** between interests – for example, in pursuit of security, online services may require their users to authenticate themselves using "two factors" (e.g. a password and a number generated by a portable device), but this could compromise accessibility for some users.

Often there is no single valid answer to these questions; in the context of public policy decisions, the dilemmas involved are essentially political. The extent to which each interest should be pursued, and which one should be prioritised, is likely to be a matter of debate in years to come. Our aim here is only to provide a map for this debate.

On the basis of discussions with the Ministry, we have chosen four specific public interests as our focus in this study. These are: availability, openness, privacy and security. In this section, we discuss each of these in some detail. We consider the government's role in their protection or enhancement in the next section.

4.2.1 Availability

Availability refers to the uninterrupted, correct and effective functioning of systems. A lack of availability can affect consumers' private and social life, as well as the wider economy. We can distinguish three key variants of availability:

- availability of specific, valued online **services**

- availability of the **networks** that allow use of valued services for specific groups of users or services – for example, an ISP becoming unavailable (disrupting its subscribers' connectivity) or a CDN becoming unavailable (disrupting the websites that rely on its services)
- **systemic** availability of the overall Dutch Internet, or aspects thereof – for example, the DNS servers for the .nl domain, leading to widespread disruption across all Dutch websites.

Clearly, the potential harm to the public increases from one type of unavailability to the next. For instance, if an entertainment website were to go down, the extent of the harm would be that certain consumers could not enjoy, say, online music for a day. If an individual ISP were unavailable, its customers might have alternative options (such as an Internet café). By contrast, if the domain-name-system (DNS) servers for the .nl domain were to become unavailable, much of the Dutch Internet would be affected, with far-reaching implications for social life and businesses well beyond the Internet value chain.

Figure 4.1 shows a high-level analysis of the Internet value chain in terms of the public interest's sensitivity to potential service unavailability in the different sectors. Note that even in the case of a single online service, the harm to society or the economy can be considerable. For example, when gmail is unavailable, not only are personal communications disrupted for millions of users, but economic activity suffers given the infrastructural role that email plays in the modern economy (note that the same argument does not apply to anything like the same extent for an online entertainment service).

Figure 4.1: Availability: relevant sectors [Source: Analysys Mason, 2013]

Note also that the high level of technical interdependency of online systems (e.g. with specialist firms providing authentication, content distribution, payments, etc.) means that systemic unavailability can be caused by online services that may not be normally thought of as infrastructure (e.g. payment processing services), and not only by major network or infrastructure providers. Many of these players often play a "behind-the-scenes" role that may be invisible to end users and even to smaller online service providers.

We discuss availability in more detail in the context of cloud providers in Section 5.4.

4.2.2 Openness

Openness is a central but ill-defined concept in Internet policy. Different stakeholders use it with different meanings in different contexts – from open source software, to software implementing open standards, to systems interoperating through standard APIs, to non-discrimination by ISPs (net neutrality), to incumbents being required to rent their networks to end users, to platforms. These many uses bear a certain family resemblance but have many crucial differences. In order to proceed with our analysis a more precise definition is needed.

Defining openness and open platforms

In general terms, in this report "openness" refers to the notion that players in the Internet value chain should not unduly prevent end users from reaching other services or users. More precisely, our discussion of openness will centre around two kinds of player:

- **aggregation platforms:** services whose role is to allow end users to access another provider (a **content provider**) that is located upstream in the value chain e.g. an online service. Key examples include ISPs (allowing users to reach online services), connected TVs (allowing users to access online video providers) and web browsers (allowing users to access websites)
- **inter-communications platforms:** players whose role is to allow end users to interact with each other. Key examples include instant messaging applications (e.g. Whatsapp), voice communications (e.g. Skype), social networks (e.g. Facebook, LinkedIn, etc.) and even ISPs themselves.

We say that a platform is **open** when it **interoperates** with other relevant services and its owner cannot arbitrarily decide with which other services it should or should not interoperate. In familiar terms, this means that:

- open aggregation platforms do not discriminate as to the content providers their users can access, and
- open inter-communications platforms allow their users to communicate with users of competing platforms.

Key examples of open aggregation platforms are ISPs under net neutrality, and a key example of an open inter-communication platform is the traditional phone system. Figure 4.2 shows our analysis of the sectors in which openness is most relevant.

Figure 4.2: Openness: relevant sectors [Source: Analysys Mason, 2013]

Key considerations

Discrimination in a platform may be prevented by regulation, contractual obligations (e.g. terms of service), convention or technology. Non-discrimination does *not* mean that no money can change hands between providers (it can, provided that payments are based on objective criteria such as a rate card), or that open platforms must necessarily interoperate with *all* relevant third parties (interoperation may be limited for instance by capacity constraints or compatibility[13]). However, whether an open platform interoperates with a third party cannot be a matter of free negotiations. Two general observations are relevant here:

- Openness is not a binary, "black and white" question. For example, an app store's policy concerning third party apps may be broadly non-discriminatory for all types of app except for those that fall in certain narrow categories.

- A competitive sector may yield openness as a collective outcome even if none of its participants is "open" in our sense. For example, Internet transit providers (see 3.2.2 above) have no obligation to interconnect with each other, and yet competitive pressures mean that failures to interconnect

13 Note that although technical standards facilitate openness, their adoption is often not sufficient.

are rare, and even when these happen users are often unaffected, thanks to ISPs' ability to source services from multiple transit providers simultaneously.

Why openness is a public interest

Openness is a public interest mainly by virtue of its relationship to two other interests listed at the beginning of this section: pluralism/free expression, and innovation. The different variants of openness (open access and interconnection) relate to these interests in different ways; additionally, interconnection also has other economic benefits. The relationships, as well as other key aspects of the two types of openness, are set out below:

Figure 4.3: The public interest case for openness [Source: Analysys Mason, 2013]

	Open access	Interconnection
Paradigmatic case	Net neutrality	PSTN interconnection
Type of platform	Aggregation platforms	Inter-communication platforms
Link to pluralism and free expression	Open access platforms can allow access to a wide variety of voices to be heard	Improved personal/social communications
Link to innovation[14]	Upstream players can access the platform's end users, which in turn may lead to investment and innovation in those sectors	Interconnection may be essential for entry by new platforms
Wider economic benefits	N/a	Positive network externalities are obtained (by users and the wider economy) when communications platforms interconnect

Using terminology from traditional telecommunications, we call aggregation platforms that are open "**open access platforms**", and we say that communications platforms that are open "**interconnect**".

We discuss open access in more detail in the context of connected devices in Section 5.2, and interconnection in the context of social networks in Section 5.3.

4.2.3 Privacy

The principle at stake here is that service providers should not collect or handle personal data except as agreed by users and in accordance with the law. This involves:[15]

- data collection – the process of recording and tracking consumers' activities or data
- storing and processing – the process of aggregating, segmenting and analysing the data collected, so that it can be used for various purposes

14 We recognise that openness can also have adverse unintended consequences in sectors where it is imposed. We discuss this in Section 6.

15 See Solove, Daniel J., A Taxonomy of Privacy. University of Pennsylvania Law Review, Vol. 154, No. 3, p. 477, January 2006; GWU Law School Public Law Research Paper No. 129. Available at SSRN: http://ssrn.com/abstract=667622.

- information dissemination – the process of delivering the processed information to other people or allowing access to consumers' personal information
- keeping the data secure – preventing unauthorised parties from obtaining personal data, possibly for malicious purposes (e.g. fraud).

As shown in Figure 4.4, some value chain players for whom privacy considerations are particularly relevant include:

- providers of social networks and online communications (e.g. email)
- players with visibility over users' online behaviour across service providers e.g. advertising networks and ISPs
- providers of connected devices (or software running in those devices) that can track users' physical locations as they go about their lives.

Figure 4.4: Privacy: relevant sectors [Source: Analysys Mason, 2013]

Key current privacy challenges involve efforts to gain knowledge about individuals by aggregating publicly available data from a wide range of sources; the increased accessibility of previously obscure information ("the death of privacy through obscurity"); and consistent observation or eavesdropping (surveillance).

We discuss privacy issues in detail in the context of online social networks in Section 5.3.

4.2.4 Security

By cyber security, we mean preventing the misuse of systems or networks by unauthorised parties. For end users (whether businesses or consumers), a breach of cyber security can mean:

- a data **breach**, in turn leading to unforeseen loss of **privacy**, identity theft or other forms of **impersonation** (in turn leading to **fraud** or other types of harm)
- illicit **interception** of private communications (potential loss of privacy for two or more parties)
- **loss, damage or decreased availability** of affected systems or data
- **misuse of affected resources** (e.g. computers, mobile devices, cloud accounts, networks) for illicit purposes (e.g. hosting illegal content, launching further cyber attacks, etc.)
- **monetary losses** (theft, loss of customers/business, loss of intellectual property)
- **loss of trust** e.g. for online service providers (other than as business users of the Internet), a security breach can lead to customers deserting or using online services less.

Figure 4.5 shows value chain players of particular relevance to security.

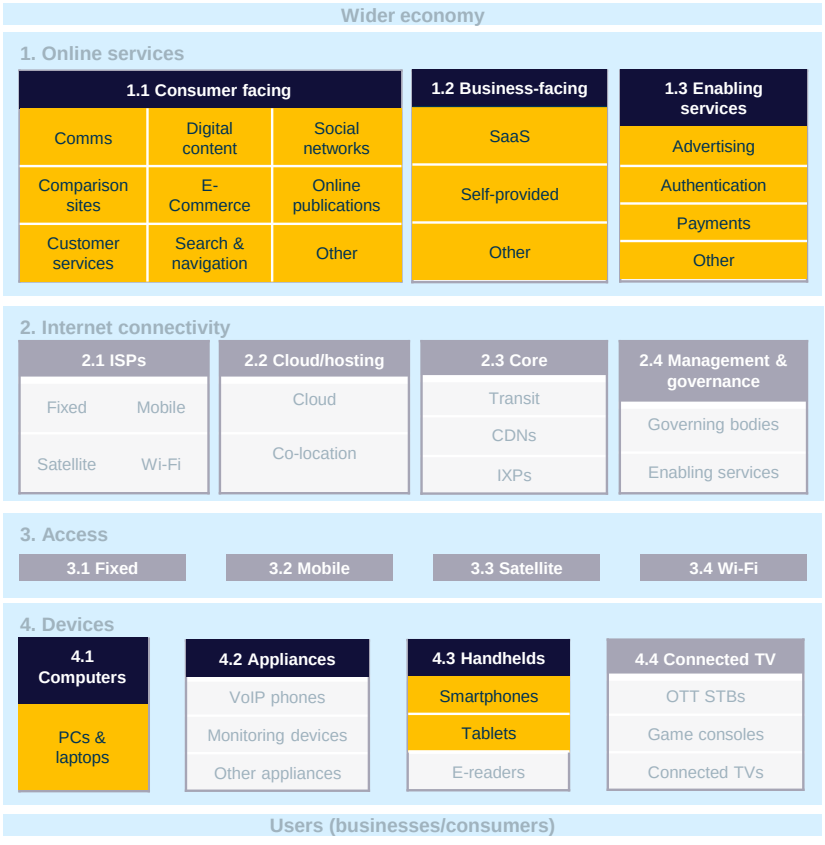


Figure 4.5: Security: relevant sectors [Source: Analysys Mason, 2013]

These include:

- Authentication services, which if compromised can lead to the interception of private communications, and widespread impersonation of both end users and online services ("phishing") by unauthorised parties.

- All online services, from which attackers can obtain data about users (which in turn can be used for instance to commit fraud or steal sensitive commercial information).

- End-user devices like PCs, smartphones and tablets, which may be vulnerable to malicious attacks, especially when end users fail to take protective measures (e.g. anti-virus).

To study cyber security in practice, we consider the particular case of certificate authorities (CAs) in Section 5.2.

4.3 When will the market under-provide?

Earlier we said that government intervention in the Internet may be called for when market participants fail to provide what society requires from the Internet. In this section, we develop a framework for identifying situations in which this is likely to be the case.

To start exploring this, consider the case of a provider of (interconnecting) VoIP calling services. Arguably, it is in the provider's interest to offer a high degree of availability, since otherwise its customers might switch to the competition. Furthermore, if the provider operates in a competitive market, it may offer high availability at a price close to its own cost of providing it. In this case, we may then conclude that the public interest is enforced by the market (the "invisible hand" at work).

Three key enablers behind this fictional, happy outcome are:[16]

- **Efficient market:** a functioning market provides what customers demand, at a minimal price. This might not be the case if there is limited competition or information, or in the presence of externalities.

- **Efficient outcomes aligned with end users' interests:** competition centres on providing what end users demand, at low cost.

- **Alignment between efficiency and the public interest:** the market's efficient outcome (high availability) is desirable not only from the point of view of consumers, but also from that of the public interest of ensuring high availability of communication services. In other cases, it is possible that consumers' interests could fail to be aligned, or could even be at odds, with wider public interests (for example, a consumer might prefer not to pay a premium meant to subsidise universal provision of a service).

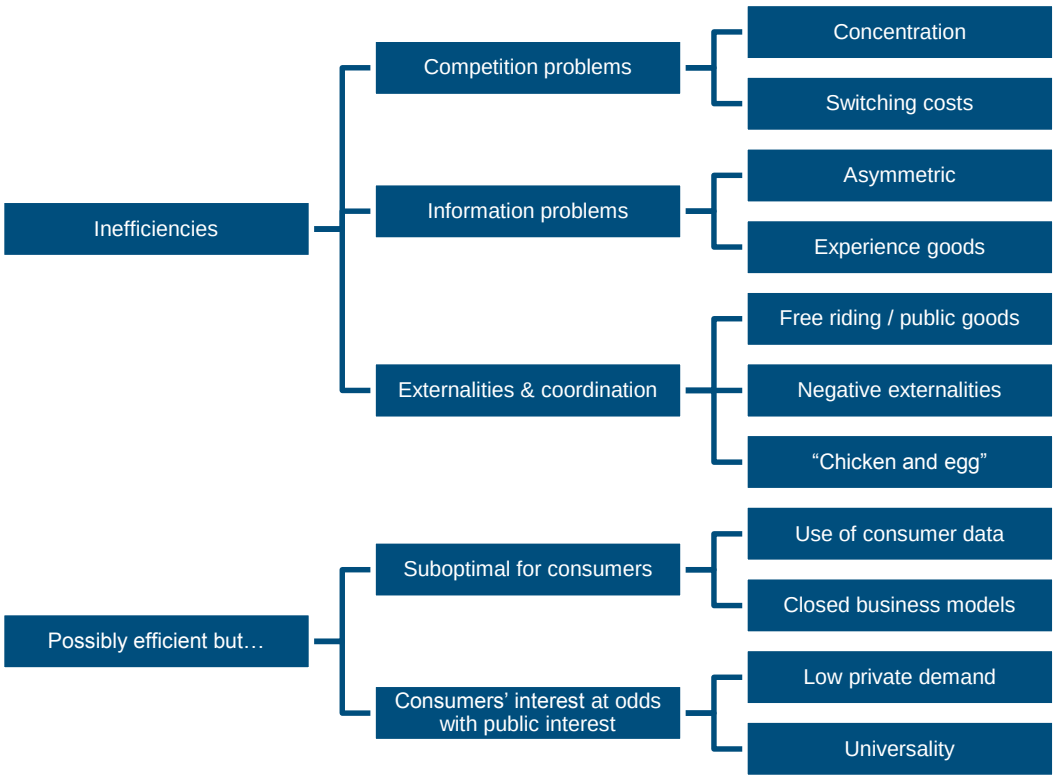
[16] In economic terms, our framework amounts to accounting for (1) efficient outcomes that maximise consumer welfare but may be sub-optimal for society or citizens (as determined through policy-making); (2) inefficiencies related to market power, information or externalities; and (3) outcomes that may or may not be efficient but do not maximise consumer welfare.

However, in practice any of these conditions may fail to hold. Thus the following **drivers of under-provision** may be present:

- **Inefficiencies:** provision may be inefficient if there is limited competition or information, or in the presence of externalities.
- **Efficient outcomes that are sub-optimal for consumers:** outcomes may not simply be a matter of negotiation between demand by end users and supply by providers if providers' business model involve balancing users' satisfaction with that of other customers (e.g. advertisers).
- **Misalignment between consumers' and public interests:** it is possible that consumers' interests could fail to be aligned, or could even be at odds, with wider public interests. For example, a consumer might prefer not to pay a premium meant to subsidise universal provision of a service.

In turn, the three broad drivers of under-provision above can be broken down into sub-types. On the basis of analytical work, as well as drawing on the detailed case studies in this report, we can identify the following types.

Figure 4.6: Typology of drivers of under-provision of the public interests [Source: Analysys Mason, 2013]



The eleven drivers of under-provision above are described in more detail in Figure 4.7:

Figure 4.7: Drivers of market under-provision [Source: Analysys Mason, 2013]

Group	Driver	Description	Example
Inefficiencies	Concentration/limited alternatives	Limited choice of providers may force users to tolerate bad service or features they do not like	Users of dominant social networks could potentially be forced to accept unfavourable terms of service
	Switching costs	Buyers may be not be able to change providers easily	Switching ISPs may be difficult or costly, especially in the case of triple-play bundles
	Asymmetric information	Buyers may lack visibility into providers' observance of a public interest	Buyers of online services may lack visibility over providers' security arrangements
	Experience goods	Buyers who have never experienced the benefits of a service may under-value it	Users who have never been victims of hackers may under-estimate the importance of antivirus or backup software
	Free riding (public goods)	A provider may experience no negative impact from failing to observe a public interest	"If all my contacts have antivirus software, I am largely protected from email viruses at no cost to me"
	Missing or insufficient liability (negative externalities)	The cost of a provider's failure to observe a public interest may be borne mainly by third parties	Providers of web browser software have limited/no direct liability for security faults
	Coordination difficulties: "chicken and egg"	An activity may only be commercially attractive if most other providers join	Using IPv6; Implementing new security standards for digital certificates
Efficiency not optimal for consumers	Exploitation of end-user data	Providers may have an interest in exploiting customer data	Two-sided markets such as advertising-funded services
	Closed business models	Providers may prefer a closed business model over an open one if it is more profitable	Non-open communications platforms (Skype, IM); vertically integrated connected TV platforms
Mismatch between consumer and public interests	Low private demand	As private consumers, end users may give low value to the public interests	Consumers may see privacy loss from social networks as tolerable in view of benefits gained
	Lack of universality	Providers may fail to offer a service to all end users at an acceptable price	ISPs may fail to offer some forms of Internet access at acceptable prices to users in certain (high cost) areas

It is worth clarifying the role that costs of provision play in our analysis. From a certain perspective, it could be argued that a public interest (e.g. high availability) may be under-provided simply because it is expensive to deliver (e.g. high availability may require redundant infrastructure). In our framework, this could be a case of individuals as consumers caring relatively little for something that society as a whole cares about more strongly (our "low private demand" category). For example, suppose it became public policy that high-quality anti-virus software should be provided cheaply enough that

nearly every consumer would use it. Even with effective competition, it could be that the costs of providing such a service would make this policy goal unreachable through market forces alone. In this case, government might consider intervening through a subsidy.

It should also be noted that the drivers above are not mutually exclusive and can reinforce each other. For example, a provider's adoption of a closed business model may lead (through network effects) to it gaining significant market power, thereby limiting competition. In turn, a provider with limited competition may have no incentive to offer contracts under which it assumes liability for the possible ill-effects of under-provision in some areas (e.g. security).

Below for each of the four main public interests introduced in Section 4.2, we discuss the drivers of market under-provision (as listed in Figure 4.7) that are most relevant to each.

4.3.1 Availability

In general, the provision of availability is a straightforward transaction between the provider and buyer of services, with no inherent misalignment between the parties' interests *or* between public and private interests. This means that consumer demand for reliable services, aided by competition, should go a long way towards providers delivering acceptable availability, and that under-provision is likely to be mainly due to market inefficiencies, or public policy demanding higher standards or lower prices than the market can provide.

An application of our framework suggests that the main potential drivers of under-provision of availability are as outlined below.

Figure 4.8: Our framework as applied to availability [Source: Analysys Mason, 2013]

Driver of market under-provision	Relevance to availability
Limited alternatives	• Limited alternatives for supply might lead to the ability to act not in accordance with the wishes of end users
Switching costs	• High switching costs create barriers to entry for competitors, and might lead to the ability to act not in accordance with the wishes of end users
Experience goods	• Customers may underestimate the importance of availability (and be unwilling to pay a premium) until a dramatic incident causes substantial harm

We noted above that customers' switching costs may have a bearing on service providers' level of availability provision. To understand this better, it is worth distinguishing between:

- Customers being able to switch providers from time to time, incurring a non-negligible but manageable switching cost, typically responding to *patterns* of unreliability over a period; and
- Customers (or intermediaries) being able to fall back on an alternative provider *immediately*, as soon as an initial provider becomes unavailable. For example, if a DNS provider becomes unavailable, users may resort to alternative providers seamlessly; and with national roaming agreements, customers of a mobile network that becomes unavailable may be unaffected.

We call the first case **switching** in the economic sense, and the second **cross-provider redundancy**. Customers' ability to switch imposes discipline on the market and leads to better service, but has no bearing on the potential harm that a lack of availability may cause. By contrast, cross-provider redundancy can greatly mitigate or even eliminate the harm caused by an outage; once achieved, cross-provider redundancy also means that customers can have low or negligible switching costs.

Cross-provider redundancy is facilitated when different providers use common standards, when users can "multi home" across providers (that is, be customers of multiple providers simultaneously), and when providers allow data to be carried from one to another seamlessly ("data portability"). All of these conditions also facilitate switching in the traditional sense.

4.3.2 Openness

The main cause of providers failing to observe openness principles is that doing so often goes against their business models. There are two main variants worth noting:

- Providers of aggregation platforms (see 4.2.2) may have an interest in preserving or exploring a closed model over an open access one. For example, a platform may have established (or may hope to establish) a **two-sided business model** with revenues not only from consumers but also from content providers who would pay for carriage.

- Providers of communications platforms (e.g. social networks, instant messaging and VoIP) may likewise find a closed model more attractive, especially if they hope that network effects[17] may lead to **winner-takes-all dynamics**, eventually leading to market domination.

In either case, lack of choice or high switching costs may prevent users from "voting with their feet" in favour of open platforms. Alternatively, consumers may be relatively indifferent as to a platform's lack of openness (for example, a connected TV platform that provides key entertainment content), even if as citizens they favour openness.

These considerations are summarised in Figure 4.9 below in terms of our typology illustrated in Figure 4.6.

Figure 4.9: Our framework as applied to openness [Source: Analysys Mason, 2013]

Driver of market under-provision	Relevance to aggregation platforms	Relevance to Inter-communication platforms
Concentration	Lack of meaningful choice can be a key reason for users accepting a closed network. Conversely, closed communications platforms or access platforms may grow exponentially because of network effects, eventually eliminating the competition.	
Switching costs	High switching costs (e.g. a subscription contract or equipment costs) may dissuade users from switching. Additionally, lack of data portability can further increase switching costs	

[17] More specifically, the value of the platform for end users may increase as more users join. Past a certain size, it no longer makes sense to join another network.

Driver of market under-provision	Relevance to aggregation platforms	Relevance to Inter-communication platforms
Closed business models	Providers may have incentives to turn open access platforms into walled gardens if two-sided revenues are achievable	Providers may find a closed model more attractive, especially if they hope that network effects may lead to winner-takes-all dynamics, eventually leading to market domination
Low private demand	As private consumers, end users may not pay attention to whether a platform is open, provided that it delivers enough benefits (e.g. quality content available, friends online). Also, a closed network can sometimes function better than an open one[18]	

4.3.3 Privacy

Providers may fail to deliver adequate privacy for a number of reasons, including limited demand for privacy, market power (when it applies) and asymmetric information. However, we expect the main cause of privacy under-provision to be a business-model misalignment, whereby certain providers may prioritise the exploitation of consumer data. The combination of these factors is likely to be particularly problematic.

In terms of our typology, the main drivers of under-provision are:

Figure 4.10: Our framework as applied to privacy [Source: Analysys Mason, 2013]

Driver of market under-provision	Relevance to privacy
Limited alternatives (concentration)	Not inherently linked to privacy, but, when there is high concentration, buyers may have no option but to accept onerous privacy terms. Changes in privacy or copyright terms of major online services such as Facebook and Instagram have caused significant media coverage
Switching costs	Difficulty in switching providers may make it more difficult for a user to reject a provider's unilateral changes to its privacy policy
Asymmetric information	End users may find it difficult to assess how well a provider respects privacy
Experience goods	Privacy may be under-appreciated until too late: users may be indifferent to privacy concerns until one day they see their information being used in a way they did not anticipate – by which time it may be too late
Exploitation of consumer data	Service providers may have a second type of customer other than consumers – e.g. advertisers – who may either want access to consumers' data, or who may expect the service provider to process consumers data on their behalf (e.g. so as to target advertisements)
Low private demand	Users may not value privacy very highly at the point of purchase as compared to other interests such as price – e.g. many online services are "free" in exchange for personal information

[18] For example, its different aspects (e.g. device and online service) may be better integrated if they are produced by the same provider rather than if two providers' products interoperate. Also, a closed platform may be able to innovate faster than if interoperability standards have to be coordinated across providers (which may be needed for open platforms).

In addition to the above, it should be noted that all the causes of **security** breaches (discussed below) can also lead to data breaches and privacy loss – so that, for example, service providers' lack of security may also be, indirectly, a cause of privacy issues.

4.3.4 Security

In general, we do not believe that the interests of value chain participants in any of the sectors studied in this report are inherently in conflict with the provision of cyber security.

Rather, in terms of the types of market under-provision explored in Figure 4.7, we see cyber-security lapses as being mainly the result of problems associated to externalities (both positive and negative), users' relatively low valuation of security (until too late) and asymmetric information. This is set out in Figure 4.11 below.

Figure 4.11: Our framework as applied to security [Source: Analysys Mason, 2013]

Driver of market under-provision	Relevance to security
Asymmetric information	Difficulties assessing the quality of a service's security can lead to buyers purchasing the cheapest lowest-quality service ("market for lemons")
Experience goods	Users or service providers may only value security once an attack causes substantial damage
Free riding (public goods/positive externalities)	In some cases, parties may have limited incentives to invest if they can "free ride" on others' investment (e.g. just as immunisation against infection by real viruses allows free riding, one can be protected against certain cyber threats by others' actions)
Missing or insufficient liability (negative externalities)	Parties suffering losses (e.g. end users) may be several steps removed in the value chain from the party that failed to apply adequate security. Market power, transaction costs, lack of intermediary liability or lack of information may all conspire to prevent the loss from being realised by the party whose action or inaction allowed the breach This lack of internalisation may remove service providers' incentives to invest in security
Coordination difficulties	Certain security solutions (e.g. secure standards) only work if multiple/all parties adopt them, making early adoption unprofitable
Low private demand	Users may not value security very highly at the point of purchase as compared to other interests such as price or the continued availability of certain services. This in turn may lead customers to (for example) ignore warnings or install software in order to complete some desired task. It can also lead to service providers choosing to keep providing services even after they know of major security breaches (because while withdrawing a service may address security concerns, it may also mean the unavailability of a critical system)

4.4 How can the government intervene?

We conclude this section with a brief outline of intervention policies that may be considered by government to address the various drivers of market under-provision.

4.4.1 A toolbox for intervention

Government may intervene to protect the public interest in multiple ways, including:

- effecting changes in providers' behaviour (for example, around standards) through
  - the "hard" tools of direct regulation and legislation
  - "softer" tools like co-regulation or encouraging self-regulation
  - facilitating industry dialogue
  - using the State's purchasing power
- effecting marketplace changes through
  - education of end users and businesses – for example, on managing security risks
  - direct government provision or contractual arrangements with private providers for the provision of essential services (e.g. PKIoverheid, discussed below)
  - direct subsidies
- working with other governments and/or Internet governance organisations and/or industry to agree on technical standards and business practices

The optimal approach to be used varies from case to case. Drawing from our case studies in Section 5, Figure 4.12 lists specific policy tools that may apply for each of the eleven drivers of market under-provision in our typology.

Figure 4.12: Drivers of market under-provision and corresponding intervention options [Source: Analysys Mason, 2013]

Group	Driver	Intervention options
Inefficiencies	Concentration/ limited alternatives	• Lower barriers to entry – e.g. by limiting network effects through mandated interconnection/interoperability • Economic regulation (in specific, limited, circumstances) • Minimum standards
	Switching costs	• Education regarding redirection facilities, future switching costs • Mandate shared standards • Mandate data portability
	Asymmetric information	• Mandate disclosure on essential facts (e.g. security breach notifications, KPIs) • Require independent (forensic) auditing • Standards which allow consumer branding for high quality • Education regarding "what to look for"
	Experience goods	• Education • Mandated minimum quality of service criteria • Use of government procurement to encourage adequate provision
	Free riding (public goods)	• Require minimum standards • Standards which allow consumer branding for high quality • Education of end users regarding responsible behaviour
	Missing or insufficient liability (negative externalities)	• Ensure that liability is placed on parties that can cause harm • Minimum standards

Group	Driver	Intervention options
	Coordination difficulties: "chicken and egg"	• Use public procurement as strategic commitment to secure buy-in • Convene and coordinate stakeholders – e.g. for standard-setting • Break deadlocks by making move (e.g. adoption of new standards) mandatory • Direct provision by the State (if no commercial player)
Efficiency not optimal for consumers	Exploitation of end-user data	• Education of end users regarding what they are disclosing • Direct regulation
	Closed business models	• Mandated interconnection/interoperability • Mandated open access • "Must carry" and associated requirements • Use of government procurement in targeted ways (e.g. prefer open solutions where these are advantageous)
Mismatch between consumer and public interests	Low private demand	• Education • Mandated minimum quality of service criteria • Use of government procurement to encourage provision
	Lack of universality	• Subsidies/universal service provisions (in limited circumstances) • Assistance with coordination mechanisms (e.g. assist rural communities to build true picture of demand)

4.4.2 International considerations

The Internet is intrinsically global, and the power of the Dutch government to enforce or encourage change may be limited in respect of services with no physical ties to, or offices in, the Netherlands or the European Union.

For activities that fall under the scope of an EU directive, then EU law can be applied and enforced, more in particular if the providers have a presence in the EU. However, for firms without EU offices and/or activities not covered by EU directives or regulations, jurisdictional and/or enforcement challenges may arise. For example, if a provider without EU presence fails to respect users' privacy in accordance with EU regulations, then EU or Dutch Law may still be applicable in the sense that the provider may be subject to lawsuits in the Netherlands; however, Dutch courts' jurisdiction may not be recognized by authorities in the country where the firm is based and enforcing the court decisions will be difficult. In these cases, coordinated approaches by multiple governments at EU or higher levels may be needed.

International coordination is also relevant beyond the context of legislation and regulation. Issues like standard adoption and Internet governance (for example, on adoptions of technologies like IPv6, DNSSEC or DANE) are managed through multi-stakeholder institutions (e.g. ICANN), in which governments can play a key role at multiple levels – from formal channels to coordinating with other governments to working with industry informally towards shared solutions.

5 Case studies

As part of this study, we have applied our framework above to four specific sectors of the Internet value chain, each from the perspective of a different public interest. These were chosen in consultation with the Ministry and reflect areas of active policy concern. Apart from the direct value that this exercise may yield to government, these case studies are also intended as an illustration of how our framework could be used in other cases. The cases chosen are:

- Case study 1: security in certificate authorities
- Case study 2: openness in connected TV
- Case study 3: privacy and openness in social networks
- Case study 4: availability of cloud hosting services.

This is summarised in Figure 5.1 below:

Figure 5.1: Overview of case studies [Source: Analysys Mason, 2013]

Each case study comprises:

- a brief analysis of the sector in question (e.g. certificate authorities)
- a discussion of how the public interest under study is relevant in this sector (e.g. security in the case of certificate authorities), including
  - an explanation of what the provision of the public interest means in practical terms
  - a discussion of the negative impact that under-provision of the interest would have
  - a discussion of the degree to which providers currently provide the public interest
- a discussion of the government's perspective, including
  - a review of the current policy/regulatory status quo and
  - a discussion of the case for (or against), and options for, intervention, drawing on our framework developed in Section 4.

Beyond this general outline, our case studies differ in their detailed structure so as to best address each case's unique characteristics. We stress that our case studies focus on the combinations of sectors and public interests in question only, and do not provide a wider discussion of how the various public interests apply to each sector. Also, we only cover the sectors highlighted above; for a high-level view of likely areas of under-provision across the value chain, readers are referred to Annex C.

5.1 Case study 1: Security in certificate authorities

Certificate authorities (CAs) provide solutions that enable online services to communicate securely with their users. Recent years have seen a number of successful hacker attacks on CAs themselves, undermining the guarantees they provide and leading to widespread concerns about online services' security. To a significant extent, this is likely to be due to a combination of information asymmetries preventing CAs' customers from verifying CAs' security arrangements, and CAs' liability being far lower than the system-wide losses that could be caused by a major security breach. Fortunately, legislation to address some of these problems is already being drafted.

5.1.1 Introducing certificate authorities

Before we can discuss the economic activities and characteristics of players in this sector, it is necessary to briefly review the relevant technologies at a high level.

Technology essentials

Digital certificates and associated technologies allow their users to carry out one or more of the following activities:

- **Authentication** – the ability for one party to prove to another that it is who it claims to be. For example, a bank's website needs to prove to its customers that it is not an impostor's website. Although authentication can also refer to end users proving to online services that they are who they claim to be (e.g. by providing a password), in this case study our focus is on the authentication of the online services themselves.

- **Digital signing** – the ability to "mark" a digital file (such as an email or a PDF document) in such a way that it can be proven that only a specific person could have created the mark, and that the file's contents have not been modified since then (integrity).

- **Encrypting communications** – ensuring that the contents of a digital file, or a communication channel, can only be deciphered by its intended recipients.

Under a **public key infrastructure** (PKI) scheme, an entity (e.g. a bank's website) wishing to engage in any of these activities must first obtain a digital **certificate** from a trusted third party, a **certificate authority (CA)**.[19] The technology is such that anybody communicating with the certificate holder can establish with mathematical certainty that it is communicating with an entity that the CA certifies as being the party named in the certificate (e.g. abnamro.com) and not an impostor. If, in turn, end users trust the CA, then they know that they are communicating with the entity named in the certificate.

The key point to be taken from this is that CAs play a central role in facilitating all PKI functions – authentication, signing and secure communications. If CAs become compromised, all of these can be subverted, leading to significant harm to consumers and lack of trust in the Internet – with associated costs for the economy.

Overview of market provision

So far our discussion of PKI schemes has been quite general, and refers to a certain family of set-ups rather than a specific technology or implementation. In particular, certain PKI schemes exist more or less independently of the Internet, while others are specific to it.

In this case study, we focus on the PKI schemes behind three specific types of certificates:

- **Unregulated SSL[20] certificates** – these are used by nearly all websites that offer secure, encrypted browsing to end users (e.g. banking websites, Gmail). SSL is also used in many other types of secure Internet connection, including email and VPN connections. We discuss unregulated SSL certificates in more detail below.

- **Qualified certificates** – these are supervised by OPTA, based on the implementation of EU Directive 1999/93/EC in the Dutch Telecommunications Act. They are issued only to natural persons (who may be representatives of organisations), and can be used only for digitally signing documents with legal force. Qualified certificates can be used without the Internet – for example, a company can digitally sign a PDF document, save it on a CD-ROM and send it by post.

19 We note that not all PKI schemes rely on certificate authorities; however, CA-based schemes are used for website security and the "qualified" certificates discussed in this case study.

20 SSL stands for Secure Sockets Layer, a protocol used to provide secure encrypted communications over the Internet. Although SSL has been superseded by a new version of the protocol called TLS, or Transport Layer Security, in this document we use the acronym SSL in keeping with much of the relevant literature. When applied to the encryption of web browsing activities, SSL (or TLS) is used to encrypt the web transmission protocol, HTTP (hypertext transfer protocol), resulting in the secure browsing protocol HTTPS.

- **PKIoverheid** – the Dutch government's own scheme, supporting authentication, digital signing and encrypted communications, intended for use in communications within government as well as between government and businesses or citizens. PKIoverheid is managed by Logius, which itself belongs to the Ministry of the Interior. Certificates issued by PKIoverheid include qualified certificates.

The key aspects of each type of certificate are summarised below.

Figure 5.2: Key characteristics of each type of certificate [Source: Analysys Mason, 2013]

Aspect	Unregulated SSL	Qualified	PKIoverheid
Purposes	• Secure Internet communications (Web, email, VPN, others)	• Digital signatures only	• Digital signatures • Authentication • Secure Internet communications
Recipients	• Mainly websites • Other firms	• Natural persons	• Natural persons • Websites • Other firms
Regulation	• None	• OPTA, under EU Directive 1999/93/EC and Dutch law	• None
Relevant agencies	• None	• OPTA (supervision of CAs)	• Logius on behalf of Ministry of the Interior (which has oversight)
Private involvement	• Over 600 estimated "root" CAs worldwide • no formal governance	• 4 commercial : KPN; Diginotar (withdrawn) ; ESG; QuoVadis; Digidentity • Plus 3 government units (Ministries of Defence, Infrastructure and Environment and CIBG)	

Two sub- sectors

The provision of PKIoverheid and qualified services overlaps significantly; in practice, qualified certificates are provided by, and only by, the entities that issue PKIoverheid certificates, and the two are managed jointly. As a result, for practical purposes the commercial provision of both types of certificate can be treated as representing a single activity – the provision of "State-supervised certificates". In what follows, we discuss separately the provision of unregulated SSL certificates and State-supervised certificates.

► *Provision of unregulated SSL certificates*

The provision of unregulated SSL certificates is a purely commercial activity. The sector lacks a supervisory body (although there are attempts at self-regulation, e.g. through the CA/Browser Forum discussed below) or central operational management, and it is essentially global.

The reasons for this lie partly in the SSL's technical architecture. Web browsers come pre-configured with a set of trusted CAs whose certificates can be trusted i.e. the browser's **root CAs**. When an

end user attempts to access a secure website, his/her browser first asks the website for an SSL certificate to confirm the site's identity. If the certificate is from a trusted root CA (and passes certain other tests, a point we will return to), the certificate is considered valid and the website is accepted as authentic. However, if the certificate is from an unknown CA, the browser will then seek to establish whether this CA is itself trusted by one of the root CAs that it already trusts; if this is the case, again the certificate is trusted, and the new CA is considered a trusted, **intermediate CA**. This process can be iterated multiple times, with multiple CAs each vouchsafing for the next. The end result is a **chain of trust**.

In terms of money flows, certificate recipients pay CAs for the issuance of certificates. Deep chains of trust result in deep supply chains, with money flowing from a website owner to its CA, and then from one CA to the next, all the way to a root CA. The outcome of this architecture is a large sector with an estimated total 650 CAs worldwide, a small group of "top tier" CAs that are used as roots by the main Web servers, and a large number of smaller CAs of secondary status. Barriers to entry are relatively low, as new entrants only need to be certified by a few existing CAs which may themselves be far removed in the supply chain from the root CAs. Crucially, nothing at the technology level prevents any CA (even those far removed from the root level) from issuing certificates covering any website.

Different CAs charge different fees for issuing certificates. Additionally, certificates are further segmented in terms of a quality flag contained in the certificates: the flag Extended Validation (EV) denotes a certificate for which the issuing authority conducted relatively thorough checking about the recipient's identity (e.g. through physical communications or face-to-face meetings), while Domain Validation (DV) only involves online verification via email.

Key Dutch CAs include DutchGrid and Gemnet, while prominent foreign competitors include Verisign (Symantec), GlobalSign, GoDaddy and Comodo.

► *Provision of State-supervised certificates*

PKIoverheid, including its qualified certificates, is ultimately supervised by the State, although most of its day-to-day operations are outsourced to private firms, which have to satisfy strict criteria and are periodically audited. The services delivered by PKIoverheid include the provision of qualified certificates for digital signatures, and all provision of qualified certificates is managed under the PKIoverheid scheme. PKIoverheid is managed and controlled by Logius, which belongs to the Dutch Ministry of the Interior and Kingdom Relations. The Ministry of Defence, Ministry of Health and Ministry of Infrastructure and Environment each control a qualified certificate service provider in specific domains. Additionally, the scheme includes four commercial certificate service providers: Digidentity, ESG, KPN and QuoVadis. These four companies are also included by OPTA in its Trusted List and can provide other qualified certificates.

OPTA supervises the provision of qualified certificates to ensure that they meet the requirements of the Dutch Telecommunications Act implementing EU Directive 1999/93/EC on electronic signatures. EU Directive 1999/93/EC includes provisions for liability and security practices. The Dutch Telecommunications Act and the relevant decree and regulation also specify strict security requirements and auditing obligations (discussed below).

5.1.2 Security in certificate authorities

What a lack of security can mean

► *Illegitimate certificates*

Security breaches or malfunctions at certificate authorities may allow third parties to issue illegitimate or "fake" certificates – that is, certificates that bear cryptographic evidence of having been signed by a legitimate CA, asserting that its holder is a given entity e.g. Google or a bank, even though the CA's legitimate controllers did not intend to issue the certificate. The types of attack that malicious third parties in possession of such illegitimate certificates can launch include:

- **Man-in-the-middle** (MITM) attacks whereby a perpetrator "sits between" an end user and a targeted website, relaying messages back and forth between the two while being able to decrypt and intercept communications.
- **Spoofing and phishing** attacks in which perpetrators direct end users to a fake version of the website they intended to use (e.g. a bank's website), where they are prompted to disclose confidential information such as passwords or financial information, leading to, for instance, identity theft or credit card fraud.

When performed with the aid of illegitimate certificates, the attacks above are uniquely effective in that it is extremely difficult (if at all possible) for end users – or their software – to detect them. Web browsers would display the "padlock" icon normally shown for encrypted communications, and may even show the additional visual clues (e.g. a green address bar) normally reserved for websites whose certificates have undergone additional vetting by CAs (see our discussion on "Extended Validation" below).

Importantly, in addition to an illegitimate certificate, both types of attack above also require the perpetrator to physically control (part of) the link in the network between the end user, to subvert the domain name system (DNS), or to subvert the victim's machine using malware.

Because of the difficulty involved in obtaining an illegitimate certificate (plus the additional requirements listed above), some experts believe that fake-certificate attacks are mainly a surveillance tool launched by State entities able to intercept international traffic, rather than ordinary fraud-driven cybercriminals.

► *Certificates lacking due diligence and look-alike domain names*

Some CAs keen to sell certificates may offer certificates with only minimal due diligence (e.g. simply requiring an email address to be verified) and no background checks. This can potentially allow a malicious third party to obtain a valid certificate covering a domain name such as one corresponding to an online bank e.g. online.abank.nl. A variant of this attack involves perpetrators purchasing a certificate for a domain that does not have a legitimate owner but *looks* as if it might be legitimately associated with a given entity e.g. abank.login.com.

In both cases, the failure is at least largely centred on certificate authorities failing to conduct adequate due diligence on parties that claim to be the legitimate owners of a given domain name. Below we will see how two industry initiatives aim to tackle this.

How a lack of security can harm the public interest

For affected users, in the first instance the direct consequence of any of the types of attack above is typically a loss of privacy, either through the interception of private communications or through perpetrators posing as a trusted party to whom users may disclose private information. In turn, this can undermine trust in the Internet and thereby slow down the development of the Internet economy.

Current observance of the public interest

► *The Diginotar incident*[21]

Diginotar BV was a Dutch company which ran a number of certificate authorities, including SSL CAs treated as "root" by major Web browsers and CAs for qualified and PKIoverheid certificates. In June 2011, an attacker gained control of the servers hosting its SSL CAs and over a period of more than a month issued 531 illegitimate certificates for domain names including google.com and skype.com. Over 300 000 users are estimated to have used an illegitimate certificate, and it is estimated that some 99% of these were located in Iran. This has led to speculation that this may have been a MITM attack relying on control over Iranian networks, launched by the Iranian State seeking to monitor its own citizens' communications.

Traces of hacker activity were also discovered in the servers responsible for qualified and PKIoverheid certificates. It is not known whether the hacker also issued illegitimate certificates of these types. The possibility remains that the confidentiality of an unknown number of official transactions (e.g. tax submissions by individuals) may have been compromised.

Notably, although DigiNotar knew that its systems had been hacked as early as mid-July 2011, it kept this information from the public for almost two months. It was only in late August that Govcert.nl (discussed below) received a report from a German sister organisation that something was probably wrong. The incident led to the Dutch government taking over Diginotar's operation and the company declaring bankruptcy.[22] Also of note, as a provider of qualified certificates, Diginotar was subject to yearly audits by an independent auditor against ETSI standard TS101456.

In the weeks following the discovery of the incident, the Dutch government faced a dilemma. It could have Diginotar's servers issue revocations of all the certificates Diginotar had issued in the period

21 Unless otherwise noted, this section is based on two public reports of the incident: Fox-IT's interim report of September 5 2011, available at http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2011/09/05/diginotar-public-report-version-1.html; and ENISA's report *Operation Black Tulip* available at http://www.enisa.europa.eu/media/news-items/operation-black-tulip.

22 Arnbak, Axel and Van Eijk, Nico, *Certificate Authority Collapse: Regulating Systemic Vulnerabilities in the HTTPS Value Chain* (August 15, 2012). 2012 TRPC. Available at SSRN: http://ssrn.com/abstract=2031409 or http://dx.doi.org/10.2139/ssrn.2031409.

during which it was under attack; however, had it done so, potentially thousands of users and businesses who may not have been affected by the hacker would have had their activities disrupted as the certificates underpinning their digital transactions would have stopped working.

The government's decision to adopt a gradual phasing-out of Diginotar's certificates reflects a difficult trade-off between two public interests: protecting privacy and ensuring the availability of key services. It is worth noting that a rapid revocation of all potentially fraudulent certificates might have amounted to a government-imposed denial of service which would have major impacts on trade and individuals and companies dealings with government and each other (tax revenues, land transactions, e-commerce, etc.), thereby potentially maximising the original attack's harm on society and the economy.

► *Other cases*

Security problems with certificate authorities are frequent. Other notable incidents include the following:

- Recently, Turkish root CA TURKTRUST mistakenly issued two subsidiary CA certificates (that is, certificates allowing their bearers to act as a subsidiary CA), when it intended to simply issue two ordinary SSL certificates. The certificates were issued in August 2012 and were only discovered in late December 2012.[23] Microsoft reported attacks involving these certificates, noting that they "could be used to spoof content, perform phishing attacks, or perform man-in-the-middle attacks".[24]

- In June 2012, Microsoft issued a security advisory[25] concerning illegitimate certificates issued in its own name and used by the W32.Flamer virus.[26]

- In November 2011, following a security breach, KPN/Getronics suspended the issuing of certificates by its CA.[27]

- The larger US-based CA Comodo[28] was breached in 2011, leading to the issuance of illegitimate certificates.

- Verisign's systems were hacked in 2010. Whether its CA was compromised is not known.[29]

---

23 Krebs on Security: 'Turkish Registrar Enabled Phishers to Spoof Google', Jan 03 2012, available at http://krebsonsecurity.com/2013/01/turkish-registrar-enabled-phishers-to-spoof-google/

24 Microsoft security advisory 2798897, available at http://technet.microsoft.com/en-us/security/advisory/2798897

25 Microsoft security advisory 2718704, available at http://technet.microsoft.com/en-us/security/advisory/2718704

26 Infosec Island: 'W32.Flamer Used Spoofed Microsoft Digital Certificates' http://www.infosecisland.com/blogview/21534-W32Flamer-Used-Spoofed-Microsoft-Digital-Certificates.html

27 See http://www.kpn.com/corporate/overkpn/Newsroom/nieuwsbericht/KPN-stopt-uit-voorzorg-uitgifte-nieuwe-veiligheidscertificaten.htm

28 See http://blogs.comodo.com/it-security/data-security/the-recent-ra-compromise/

29 See http://www.pcmag.com/article2/0,2817,2399773,00.asp

5.1.3 The government's perspective

Policy/regulatory position

► *Status quo*

European directive 1999/93/EC provides for electronic signatures to have the same legal force as physical ones, provided that the certificates on which they are based, and their providers (the CAs), meet certain requirements. The directive is implemented in Chapter 18 of the Netherlands's Telecommunications Law; parties wishing to become certificate service providers for qualified certificates can choose between registering directly with OPTA (which will then exercise direct oversight), and using the mechanism of article 18.16, which mandates periodic inspections by an approved independent organisation (this is the path chosen by all existing CAs). Importantly, the directive and its implementation:

- apply to providers of qualified digital signature certificates in general, whether or not these are used or transmitted over the Internet, and
- do not cover certificates used for encrypted SSL Internet communications.

The laws do not explicitly cover the government's options for intervention in case of CSP failure.

► *Under discussion: EU proposal on e-signature regulation*

In January 2012, the European Commission introduced a draft regulation on electronic identification and trust services for electronic transactions in the internal market, which is meant to extend the previous directives. For the purposes of this case study, two key aspects of the proposed regulation are that, under it, all "trust service providers", **including providers of ordinary SSL certificates**, would be **liable** for damages resulting from security breaches and would be required to issue security breach notifications when their security is compromised.

Certain limitations of the proposed regulation are worth noting. Yearly audits would be required only for CSPs issuing qualified certificates; audits would be non-forensic and ex-post; and no approval would be required before activities start. Also, the proposed regulations do not provide an explicit authority for governments to intervene in emergencies involving failing CSPs; and Web browsers (a key part of the ecosystem) are not covered.

The case for intervention

To be sure, the main reason why intervention ought to be considered is practical, not theoretical: the repeated security breaches seen concerning digital certificates are a clear call to action. More specifically, there are two problems at stake: (a) the fact that current regulations concerning security of qualified certificates seem to be insufficient, and (b) the fact that ordinary SSL certificates play an increasingly important role in both economic and social life (from online banking to personal email). The proposed EU regulation aims to deal with both of these points: by imposing yearly audits for qualified certificate providers, and by imposing liability on all certificate providers.

For a more general consideration of the case (and options) for intervention, we turn to our general framework outlined in Section 4.3.4. Its application to the specific case of CAs is summarised in Figure 5.3, and discussed in more detail below.

Figure 5.3: Our general framework as applied to security in the specific case of certificate authorities [Source: Analysys Mason, 2013]

Driver of under-provision	Specific case of certificate authorities
Need for coordination and free riding	• Emerging technical **standards** like DANE (see below) require widespread take-up before their adoption by individual players makes sense ("bootstrap problem")
Lack of liability and indirect liability	• CAs are currently not automatically **liable** for third parties' losses[30] • Firms with websites, but which are not themselves Web-based businesses, often outsource Web issues to third parties (e.g. **Web agencies**), which may be required to buy SSL certificates as part of their contracts, but which have no stake in possible security breaches (unless specified by the contract) and hence may buy the cheapest certificate available • Web browsers play a key role – for example in deciding which CAs are to be granted root status – but have limited downside in case of security breaches
Information asymmetries	• **Website owners** cannot easily judge the level of security of their contracted CAs. As a result, they may opt for the cheapest competitors, leading providers to compete on price while sacrificing security • **End users** are often unable to judge security situations (because of technical complexity)
Low private demand	• Users may tend to prioritise service **availability** over security
Experience goods	• End users may be unlikely to pay attention to security issues until they suffer an attack – by which time it is too late

Potential policy approaches to addressing the issues above include:

► *Addressing the need for coordination: DANE, TACK and other technical standards*

New technical standards offer the possibility of tackling security issues at their source. In particular:

- The DNS-based Authentication of Named Entities (DANE) is a set of protocols that, when implemented, will allow each domain owner (e.g. Google, as the owner of google.com) to publish its own list of trusted CAs – thereby eliminating the weakness in SSL certificates whereby any CA can issue certificates applying to any domain.

- Two emerging standards (Trust Assertions for Certificate Keys, or TACK;[31] and Google's Public Key Pinning[32]) seek to achieve a similar effect. However, in their current forms they suffer from limited scalability or security.

30 Although current regulations do not provide a default liability regime, this does not preclude limited liability provisions from being included in contracts; additionally, CAs are subject to general tort law.

31 See http://arstechnica.com/security/2012/05/ssl-fix-flags-forged-certificates-before-theyre-accepted-by-browsers/

32 See http://ssl.entrust.net/blog/?p=615

While both types of solution can help, the first has the potential to address the problem of illegitimate certificates in a more structural way. However, unlike the second type, the investments needed by stakeholders for DANE to be effective only make sense (from stakeholders' financial perspective) once enough other stakeholders have made similar investments.[33]

Government may be able to help break this "bootstrap problem" not through technology-specific regulation (which may be problematic in the context of fast-changing technology), but by facilitating coordination between large browser providers, websites and Internet infrastructure players, and/or by using its market power as a major technology purchaser. To be clear, we are not recommending that Government favour DANE over TACK, or even that it make a decision as which standard should be adopted. Such interventions – although sometimes necessary – often risk favouring the wrong technology and/or limiting innovation. A "light touch" approach could see the government working with industry to facilitate or speed up the standard-setting and implementation processes.

Finally, we note that even without new standards small technical interventions might go a long way towards improving security. For example, today web browsers do not always check with the relevant CA whether a certificate received from a website has been revoked. Changing this would be a relatively straightforward task for web browser developers; however, it may require significant infrastructure investments by CAs so as to handle the resulting workload.

► *Addressing liability issues*

As noted above, proposed European regulations would impose liability for damages on SSL certificate authorities. While this would address a fundamental weakness in the value chain, there are concerns about the possible unintended consequences of imposing unlimited liability on trust service providers; it is feared that such a requirement could lead to extreme market concentration around a few large players,[34] or even the exit of European providers.

We note that the proposed EU regulation does not consider extending liability to Web browsers, despite their crucial role in security (namely, given that it is they who determine which CAs are to be trusted, how/when trust is to be revoked, etc.). In future, policymakers may wish to consider whether regulation should also include this sector of the value chain.

► *Dealing with information asymmetries*

The fact that website owners have limited visibility over CAs' security arrangements can lead to a "market-for-lemons" situation in which CAs invest only minimally in quality and website owners

[33] For example, companies can only deploy DANE once DNSSEC is in place in their relevant domains, which in turn may only make sense to DNS providers once demand is clear. For a discussion of the economic "bootstrap problem" behind DNSSEC, see "DNSSEC deployment study" a report by InterConnect Communications for Ofcom, available at http://stakeholders.ofcom.org.uk/binaries/Internet/domain-name-security.pdf, p 21.

[34] We note that, in this case, the consequences of a single provider being hacked would be even more severe than today (and the targets will become even more attractive).

purchase the cheapest certificates available. Through the CA Browser Forum,[35] the industry has attempted to address this problem through the introduction of quality differentiation in certificates, so that price-conscious buyers can purchase low-security certificates while other buyers can purchase more expensive certificates subject to international quality standards.

However, the evidence of continued problems suggests that there may be a limit to what self-regulation alone can do. While self-regulation requires compliance to ETSI standards, formal regulation could require that this compliance be audited regularly by an independent party (this is the case today for providers of qualified certificates only).[36]

We also note that providers of qualified certificates, as well as telecoms firms that provide any type of certificate, are currently required to issue security breach notifications when their systems are compromised. However, this does not cover providers of normal SSL certificates (except when they are telecoms firms). We note that there are discussions at the EU level aimed at addressing this.

Finally, we note that public provision may also be a tool worth exploring. The government could consider "setting a high bar" for the private sector by providing non-qualified SSL certificates for general use through PKIoverheid. The implicit quality assurance involved would likely incentivise other providers to develop their own ways of demonstrating their security credentials (e.g. by publishing independent audits) in order to compete.

► *Addressing under-demand for security*

Asymmetric information can result in buyers of CA services "giving up" on trying to ascertain quality and simply buying the cheapest available products. This problem is compounded by:

- experience goods: stakeholders' failure to value security accurately until it is too late.
- low private demand: stakeholders not valuing security highly enough as compared to policy goals (the latter of which may be based on a consideration of systemic harm). This may be because security concerns come into conflict with the need to maximise availability.

It may be possible for government to partly address the first problem by promoting understanding of key technical issues among both businesses and consumers (e.g. through education and information dissemination). However, more broadly, if policy calls for higher levels of security across all stakeholders, stronger measures may be necessary. These may include the imposition of minimum quality of service criteria that could be mandated in the terms and conditions of CA services. While this is already the case for qualified certificates, it is not for ordinary SSL certificates, and we note that its extension beyond qualified certificates is not part of current EU discussions.

35 The CA/Browser Forum is an industry body formed by the world's leading SSL CAs and Web browser developers in 2005. Its key achievements to date include the introduction of Extended Validation (EV) certificates and the requirement on its members to meet standards set by either the American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA) or the European Telecommunications Standards Institute (ETSI).

36 Notably, Diginotar had regularly passed yearly audits conducted by an independent auditor (self-regulation calls for compliance with ETSI standards but not for yearly independent audits; In Diginotar's case the latter were required because of its involvement in qualified certificates.

► *Summary*

Our analysis from the preceding sections is summarised in Figure 5.4 below:

Figure 5.4: Certificate authorities: issues, current position and possible interventions [Source: Analysys Mason, 2013]

Driver of under-provision	Status quo	Possibilities
Need for coordination and free riding	• DNSSEC already in place for .nl domain with 4m+ registrations[37]	• Facilitate standard-setting and standard-implementation processes (DANE, DNSSEC, TACK) • Require minimum functionality (e.g. certificate revocation checks)
Lack of liability and indirect liability	• Liability applies only to providers of qualified certificates	• Extend liability to all CAs (part of proposed EU regulations) • Extend to other relevant value chain participants e.g. web browsers (not currently contemplated)
Information asymmetries	• Self-regulation DV/EV certificates • Qualified certificate providers and telecoms operators are required to issue security breach notifications • Mandated independent audits for qualified certificate providers	• Mandated security breach notification for providers of non-qualified certificates • Independent audits for non-qualified CAs • PKIoverheid provision
Low private demand and experience goods	• Minimum quality-of-service criteria apply to qualified certificates	• Minimum quality-of-service criteria could be expanded to all CAs • Education

National/international dimension

Finally, we note that issues of territoriality play a key role when assessing policy options. To an extent, the cross-border nature of the technologies behind CAs limit the effectiveness of what a national approach can achieve, especially in the case of SSL certificates. For example:

- any requirements imposed only on EU-based CAs might put European CAs at a disadvantage versus non-EU competitors
- in order to impose regulation on Web browsers, issues such as jurisdiction would need to be assessed.

However, these limitations are far from absolute. For example, the first problem could be partially mitigated by mandating that EU-based online services only use CAs complying with EU regulations; and on the second, we note that most major browser providers (e.g. Microsoft, Google and Apple) have EU subsidiaries.

37 See Ofcom, *ibid*, p 29.

Nonetheless, although there is much that can be done at a European level, the limits should be acknowledged. The Internet is a global network, and even if many important online services have European subsidiaries, they could easily leave, and there will always be countless others that will also be popular with European users. In our view, ultimately a solution is likely to call for a global approach – with a coordinated European level approach playing a key role (a point that has been noted by ENISA).

5.2 Case study 2: Open access and connected devices

In this study, by connected TV platforms we mean "connected" TV sets and other devices that allow consumers to view content from online providers on their TV sets. Providers of connected TV platforms are generally free to decide what online content providers users can access, and while traditionally this has meant that only a few services were available in each platform, recently some providers have moved towards a more "open" model in which consumers can choose content providers from "app stores". By contrast, "must carry" obligations require traditional TV platforms (e.g. cable TV) to carry public broadcasters, partly as a way of ensuring that consumers have access to a wide variety of views. The question thus arises as to the best way to ensure pluralism in connected TV – and, particular, whether or not the imposition of "must carry" rules for connected TV may be the best way of achieving that. These and other related issues are expected to be discussed in the forthcoming EU green paper on connected TV.

5.2.1 Introducing connected TV

In this case study, our focus is on the value chain of connected TV. By this we mean TV sets and other consumer electronics that can obtain video content over the Internet from online service providers. Specifically, we consider the following value chain sectors:[38]

- **Providers of connected devices**, including connected TVs (e.g. Philips Net TV, Samsung Smart TV, etc.), dedicated set-top boxes (e.g. Apple TV, Roku) and game consoles (Xbox, Nintendo, Playstation, etc.).

- **Online video providers**, accessible using connected devices via the Internet ("over the top"). Key examples include "online video distributors" (OVDs[39]) like Videoland or iTunes (which license content from a broad range of content owners), and major broadcasters (such as public broadcaster Uitzendinggemist.nl, which is available on Philips Net TV).

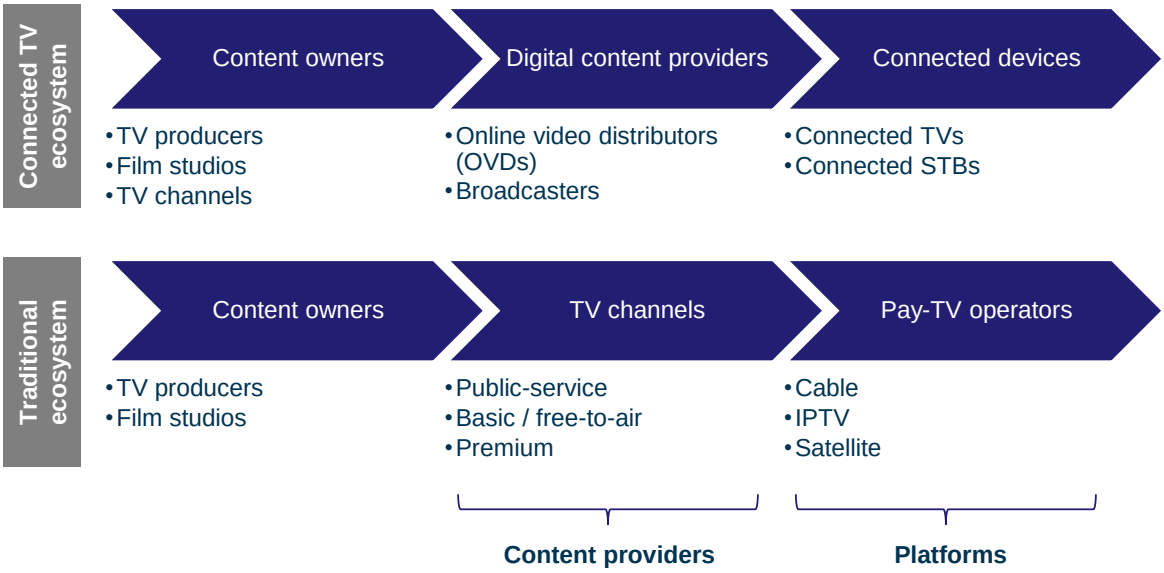
In terms of the terminology introduced in Section 4.2.2, connected devices are "aggregation platforms" (or simply **platforms**), and online video providers are **content providers.**

[38] Some key players are vertically integrated across two of the steps above. Thus, Apple's Apple TV, for instance, connects to Apple's iTunes, and some broadcasters have their own catch-up services.

[39] The OVD sector was analysed (and given its acronym) by the US Federal Communications Commission (FCC) in its research related to the merger of Comcast and NBC Universal.

In addition, in order to draw a parallel between traditional and new ways of distributing TV content, we also consider the case of traditional TV distribution. In the traditional ecosystem, the platforms are the traditional TV operators (e.g. cable companies, or telecoms incumbents offering IPTV services) and the role of content providers is played by TV channels. The two ecosystems under study are illustrated below.

Figure 5.5: The connected TV and traditional TV ecosystems [Source: Analysys Mason, 2013]



5.2.2 Openness in connected TV

In Sections 4.2.2 and 4.3.2, we introduced the concept of open access as the notion that platforms should allow end users to access other players upstream in the value chain ("content providers"), without discrimination. Key examples are ISPs carrying traffic for any and all online services, and web browsers allowing users to access any website. Before we apply them to the case of connected TV, it will be helpful to refine these concepts further.

The concept of open access

It will help to distinguish between:

- **commercial non-discrimination**: the notion that a platform's owners should exercise no discretion in deciding which content providers a platform should carry; and
- **technical non-discrimination**: the notion that all content providers should be treated equally at a technical, physical level.

We say that a platform is **open** when it does not discriminate commercially – that is, when it offers the same terms to all its current and potential content providers. This means that owners of open platforms cannot use their discretion when deciding which content providers their users will be able to access. It also means that if an open platform requires payments from content providers, these should be based on objective, transparent criteria.

It is important to note that technical constraints often make discrimination at a technical level unavoidable; for example, certain platforms only have room for a limited number of content providers, or rely on navigation systems (for example, a TV channel numbering scheme) that unavoidably accord different statuses to different providers. But whether these technical limitations are dealt with in a way that is commercially non-discriminatory, or open, is a separate question – and often one of interpretation.

It should also be observed that, in general, a platform cannot carry a content provider that does not wish to be carried (even in the Internet, some websites only allow access from certain ISPs). For instance, this could be because the content provider expects payment and there is disagreement regarding compensation (a common occurrence in the case of traditional TV platforms), or because of an existing exclusive contract. We call this **reverse discrimination** (because they are case of discrimination by content providers rather than platforms) and it is not our focus here.[40]

Commercial discrimination should not be taken as necessarily negative. Parties' ability to refuse to interoperate is essential to their ability to negotiate their own arrangements, which in turn may be vital to the creation of new business models. In particular, when platforms can capture revenues from content providers, we speak of **two-sided platforms**, reflecting their dual revenue streams. In practice, closed platforms may mix multiple models, paying some content providers for the right to carry their content while at the same time charging other content providers for the right to be distributed.

What openness means in this context

In both of the ecosystems under study, a platform can discriminate in (at least) two ways: (i) in its choice of content providers, and (ii) in the prominence it gives to different providers in end users' navigation (e.g. menus, app stores or channel placement).

Each kind of discrimination has a technical and a commercial dimension, and in both ecosystems platform providers must discriminate technically on matters of both carriage and prominence.

- In the case of traditional TV, capacity constraints mean that a set number of TV channels can be carried, and channel numbering schemes by their nature give more prominence to some channels over others.

- Perhaps more surprisingly, a similar situation can also be observed in the connected-TV ecosystem, where typically each content provider requires special software to be written for each platform. Except for platforms with relatively unrestricted "app stores" like Google TV, this software must then be approved and possibly installed on the devices by the platform owners.

Thus, choices of carriage and/or prominence are unavoidable. Whether a platform is open depends on how these choices are made.

40 In cases of TV content providers deemed to have market power in certain content markets, this has prompted regulators or competition authorities to intervene by imposing "wholesale must offer" obligations on content providers to offer their content to all platforms on non-discriminatory terms. In the Internet space, there are a few cases of content providers restricting their content to selected ISPs – the practice has been called "reverse net neutrality".

Current observance of the public interest

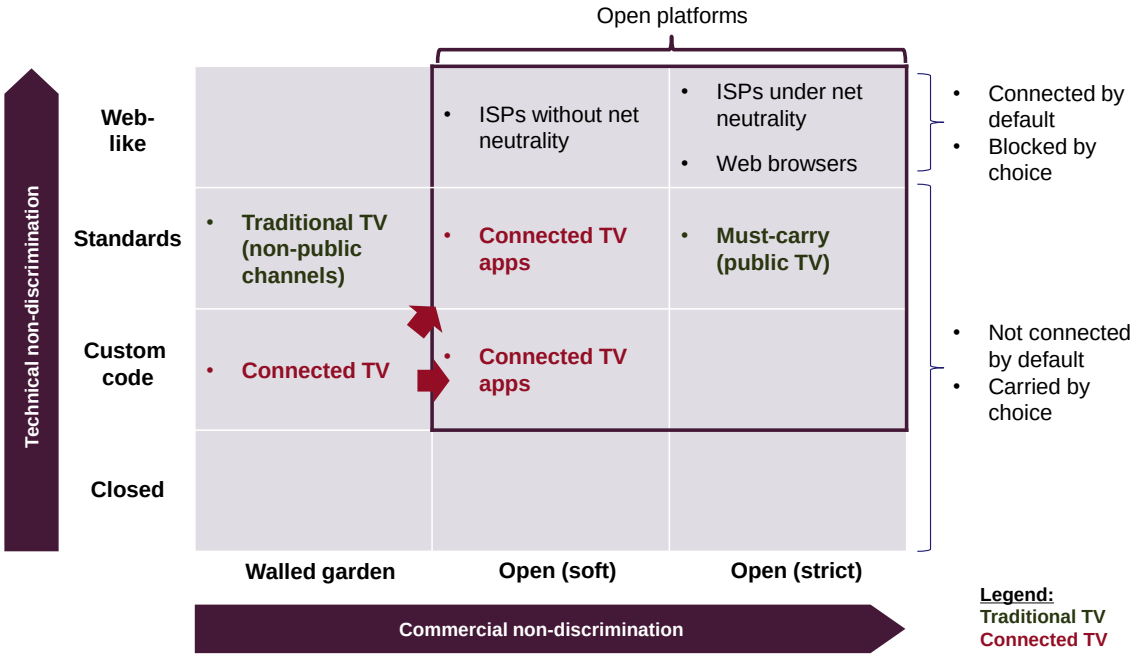
With the notable exception of net neutrality, in practice full openness is relatively rare, and where it is present it is a matter of degree. Platforms span a wide spectrum from openness to closedness, which can be defined along two dimensions:

- The degree with which commercial non-discrimination is enforced can vary. We distinguish between:
  - platforms with **strict** non-discrimination: if regulations mandate the use of a rate card, or of zero payments
  - platforms with **soft** non-discrimination: if non-discrimination is self-imposed and subject to exceptions, a matter of convention, or if legal requirements only call for "good faith" negotiations
  - **walled gardens**: whereby platform owners can carry whom they choose.

- In terms of technology, we can distinguish between various degrees of "technical openness":
  - **web-like:** platforms for which the default is to interoperate with all content providers, without requiring any agreement or intervention between the two parties. Cases of a web-like platform not connecting to a content provider is due to deliberate **blocking** by one of the two parties rather than a failure to deliberately interconnect
  - **standards-based:** technologies which make interoperation between the parties simple to implement, but which nonetheless still require the explicit enablement of a link between platforms and content providers
  - **custom code:** platforms requiring ad-hoc software to be written for each content provider's presence
  - **closed:** platforms whose only content provider is the platform owner itself (i.e. vertical integration).

Multiple combinations of commercial and technical non-discrimination can be observed in practice. This is summarised in Figure 5.6 and discussed below.

Figure 5.6: Variants of openness in platforms [Source: Analysys Mason, 2013]



The following cases can be identified:

► *Connected TV*

For connected TV, platform providers have traditionally chosen which content providers to carry on the basis of private bilateral deals i.e. a closed "walled garden" approach. Technologically, each platform is different, which means that applications have to be developed on a one-off basis. Thus, connected-TV platforms have traditionally been in the cell labelled "1" in Figure 5.6.

However, and importantly for us, this is changing in two ways. First, some major players (e.g. Samsung, Google TV) are moving to an "app store" model whereby content providers are encouraged to submit applications on a first-come first-served basis. Second, technical standards are beginning to emerge (e.g. HbbTV, OIPF, MHP, ITU and the Smart TV Alliance) which aim to standardise app development technologies so that developers can "build once, run everywhere".

It is too early to tell how far these efforts will go. Even with "app stores", without a formal undertaking or established practices on non-discrimination it is not clear to what extent platforms will retain a gatekeeper role. As to technologies, it is not clear if the process will converge around a common, shared standard, or if the next decade will see a "standards war".

From the point of view of openness, an ideal outcome would be for connected TV to converge on a web-like standard, whereby "apps" would be unnecessary and end users could simply browse to the content provider of their choice. Whether this is in players' interests, and whether industry developments will spontaneously lead to this outcome, are questions that we will return to.

► *Traditional TV*

By contrast, in the Netherlands traditional platform operators are subject to a "**must-carry**" regime whereby public service broadcasters must be carried with no payments involved.

For other channels, the situation is different, with platforms having full discretion (other than having to offer a minimum number of channels to all consumers). This is a case of "walled gardens".

5.2.3 The government's perspective

Policy/regulatory status quo

In terms of legal obligations, our two ecosystems (connected and traditional TV) present a clear asymmetry. While traditional operators are subject to "must-carry" rules concerning carriage of linear channels, connected-TV players are largely unregulated, both with respect to carriage and prominence choices. Traditional operators' VoD offerings are also unregulated with respect to carriage and prominence (for all players, content regulations apply e.g. around the protection of minors).

► *European regime*

The European regime (mainly article 31 of the Universal Service Directive, USD) allows Member States to impose must-carry obligations on TV platforms where "a significant number of end-users use [these platforms] as their principal means to receive […] television broadcasts" (this is known as the **quantitative requirement**). The USD and subsequent case law also clarify that obligations can only be imposed in a way that is transparent, proportionate (in particular, in terms of the financial burden on platforms), clearly defined and in the pursuit of "general interest objectives" including plurality and cultural policy. The Directive allows Member States to determine appropriate remuneration if appropriate, but does not mandate it. [41]

Importantly, the Directive's scope is restricted to "undertakings […] providing electronic communications networks used for the distribution of radio or television broadcasts to the public". Its application to the case of "over-the-top" Internet platforms like the ones we are studying here is therefore potentially null.[42] Furthermore, the Directive is broadly interpreted as applying only to the carriage of linear channels and not to on-demand offerings (even on platforms for which obligations do apply for linear carriage).

As to prominence, article 6 of the EU Access Directive contains provisions allowing Member States to set prominence obligations on providers of electronic programme guides. However, such obligations are not implemented in the Netherlands.

41 See N. van Eijk et al, "Must-carry regulation: a must or a burden" in IRIS *plus* 2012-5,*Must-carry: renaissance or reform?* (Susanne Nikoltchev (Ed.), European Audiovisual Observatory, Strasbourg 2012).

42 In the Dutch implementation, the obligation is imposed on the provider of a 'omroepnetwerk'/broadcasting network: the natural person or legal entity providing transmission capacity via the broadcasting network. In the case of over-the-top platforms, this can be taken to be the ISP – whom, we observe, is not in a position to ensure that a content provider is available in a connected-TV platform. Elsewhere in the EU, the restriction is understood to imply that connected-TV platforms are exempt.

► *Dutch regime*

The Universal Access Directive is partly implemented in paragraph 6.3.2.1 of the Netherlands' Media Law, which provide for TV platforms to carry 15 TV channels at a minimum in all package tiers. The list of channels is selected at a local level by Programme Councils appointed by city councils (as regulated in paragraph 6.3.1.3), and must include the national and regional public-service broadcasters (PSBs) as well as two Flemish Belgian channels.

However, in 2006 the European Commission initiated infringement proceedings against this interpretation of the USD, on the grounds that having a Programme Council that can select any channels is an unduly discretionary imposition on platforms that goes beyond the notion of "general interest".[43] The EC eventually dropped its legal action in the understanding that the current Dutch law would only be enforceable for analogue channels, and that a new law would be introduced covering all channels. In October 2012, the Minister of Education, Culture and Science introduced a bill to amend the Media Act as well as the Telecommunications Act whereby Programme Councils will be abolished and the choice of "must-carry" channels (which will now rise to 30 digital channels) will be for operators to make (subject to it including the PSBs).[44] Effectively, the new law will amount to simply imposing that all (digital) TV platforms must have at least 30 channels in their entry-level digital packages, and that PSBs must be universally carried as part of this.[45]

Importantly, neither European nor Dutch law mandate that payments should take place between platforms and broadcasters. However, channels can request remuneration, in which case both parties negotiate on a fee. Importantly, if negotiations were to break down, an operator would be allowed not to carry the channel.

It should also be noted that Dutch laws or regulations (whether existing or proposed) pose no obligations on any platforms regarding carriage or prominence of non-linear content (i.e. video on demand, or VoD).

43 In a related case, in 2007 (UPC et al vs Belgium) the Court of Justice of the European Union found that must-carry obligations must pursue a public interest such as the protection of pluralism in accordance with cultural policy. See N. van Eijk et al, *ibid*.

44 IRIS bulletin 2013-1, p 19.

45 Must-carry channels include the national/regional/local Dutch PBS channels and the three channels of the public Belgian broadcaster.

► *Summary*

The regulatory and market situation with regard to carriage and prominence in the traditional and connected TV ecosystems is summarised in Figure 5.7 below:

Figure 5.7: Carriage and prominence: summary of policy and market positions [Source: Analysys Mason, 2013]

Type of discrimination	Type of content	Ecosystem	Policy position	Market status quo
Carriage	Linear	Traditional	Must-carry for PSBs Minimum 30 channels chosen by operator (including PSBs)[46]	Negotiated compensation
	VoD	Traditional	Copyright only/carriage only by mutual consent	Negotiated
	Linear	connected TV	Carriage only by mutual consent[47]	Negotiated
	VoD	connected TV	Carriage only by mutual consent	Negotiated
Prominence	Any	Any	Unregulated	Platform decides/negotiated

The case for intervention

At first sight, the situation described above gives rise to two interrelated questions:

- Given that our starting point is the provision of openness as a public interest, is there a case for intervention so as to ensure openness in connected TV? If so, are the costs commensurate with the benefits?
- Should the clear regulatory asymmetry shown in Figure 5.7 be eliminated or diminished, so as to achieve a level playing field between traditional and new platforms?

However, in our view addressing these questions directly would be the wrong approach. As discussed in Section 4.2.2 (see especially Figure 4.3), openness is not so much an ultimate end in itself as a means towards two other interests, namely pluralism and innovation. Moreover, the benefits of obtaining a level playing field (which might be a benefit of eliminating regulatory asymmetries) should be weighed against all the other public interests at stake.

46 After proposed amendments (proposal 33426). Must-carry channels include the national/regional/local Dutch PBS channels and the three channels of the public Belgian broadcaster. Operators must include a minimum of 30 digital TV channels and/or 15 analogue channels in all packages. Obligations also cover carriage of radio stations (not discussed here). Parliament has recently asked for clarifications as to whether the requirements will apply to operators using IPTV.

47 The European Court of Justice recently issued a ruling clarifying that the unauthorised retransmission of TV signals over the Internet constitutes a breach of copyright (case C-607/11, d.d. 7/3/2013). See http://www.guardian.co.uk/media/2013/mar/07/tv-live-streaming and http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62011CJ0607:EN:HTML.

A more fruitful approach is to consider how the key public interests at stake can be achieved through openness, must carry or other policies, considering the particularities of each platform. Thus, we note that:

- in the case of traditional TV, the main aim of must-carry obligations is the support of cultural policy goals including pluralism, free expression and social cohesion. In turn this has followed from the characteristics of the traditional TV medium and its distribution platforms. Specifically,
  - given the economics of content production and distribution, the main interventions have historically centred on the provision of public service broadcasting channels that are themselves tasked with providing pluralism, and ensuring that these are universally available
  - distribution platforms' capacity limitations have meant that even without prominence obligations, public broadcasters' channels are easily findable.
- net neutrality's links with both pluralism and innovation have been predicated on the notion of essentially infinite capacity, at least in terms of the number of voices and online services that can be carried (here we see net neutrality as the paradigmatic case of an openness requirement).

The situation is summarised below.

Figure 5.8: Rationale for openness and must-carry policies [Source: Analysys Mason, 2013]

Policy objectives	Net neutrality	Must carry
Pluralism and free expression	✓	✓
Innovation	✓	
Social cohesion		✓

In turn, this prompts the following question: how can pluralism, innovation and social cohesion be best promoted in the context of each TV ecosystem?

In the case of traditional TV, a full answer to this question is ultimately about the continued role of linear television in a context of ever-increasing choice and potential substitution by connected TV. While these are important questions, the issues involved are substantial and are outside the scope of this study.

As to connected TV, openness, if it can be achieved, should go a long way towards delivering the two goals of pluralism/free expression and innovation, save for one concern: given the potentially infinite choice of content providers in open platforms, the proliferation of personalisation technologies, and the multiple commercial interests involved in capturing audiences' attention, there is a risk that connected TV may result in a net decrease in the level of pluralism in the content to which audiences are exposed (as distinguished from the context to which they have access). This also could have an undesirable effect in terms of social cohesion.

This thus leads to two questions: how, and to what extent, should openness be pursued in connected TV? And how can policy ensure that a wide variety of voices are visible to audiences?

► *Promoting openness in connected TV*

As noted above, current developments in the connected TV ecosystem might go a long way towards delivering openness without any public intervention. As connected TV platforms voluntarily move to an "app store" model, open carriage means simply that a content provider's "app" should be available in the store, and that inclusion in the store should not be subject to (commercially) discriminatory terms. This may already be in line with some content platforms' plans, which suggests that requiring carriage on an open basis may be unnecessary.

However, there are reasons not to be complacent. An application of our framework from Section 4 suggests two main reasons why the market might fail to provide openness:

- **Conflicting business models:** we cannot rule out that there may always be platform owners for whom an open approach is commercially unattractive.

  In this case, government may wish to consider the imposition of openness requirements. However, in our view this should be approached with utmost care. Platforms' tools and interfaces for navigating and searching for content are in their early stages of evolution, and intrusive regulations could risk de-railing innovation, as we discuss this in Section 6, The potential benefits and risks should be weighed with care,

- **Coordination problems and the need for standards:** as noted above, there are signs that the industry is moving by itself towards an open approach. Key players are moving to an "app store" approach, and in terms of technology there are incipient efforts towards the development of shared standards (e.g. HbbTV, OIPF, MHP, ITU and the Smart TV Alliance). At the most open end, players like Google[48] are working towards the creation of a web-like platform for connected TV, whereby "apps" would only be optional and any user would be able to "dial in" the "website" of any content provider and interact directly with it without the platform owner's involvement, permission or knowledge.

  However, these developments may stall – even if players are willing to invest in open and/or "web-like" standards – if lack of certainty on standards or strategic commitment of competitors leads to a "chicken and egg" stalemate in which no player invests in open solutions because it is waiting for other players to do the same. Government may be able to play an important role in avoiding the first obstacle by working with industry and standards bodies towards facilitating convergence on a shared, open standard.

[48] See https://developers.google.com/tv/web/.

► *How can policy ensure that a wide variety of voices are visible to consumers?*

Perhaps a more pertinent policy tool than "must-carry" is EPG prominence. Without high visibility, public service content may go unnoticed, and if only content providers of certain types (e.g. entertainment and sport) or persuasions are given prominence, plurality would suffer. Although no such rules apply in the Netherlands,[49] the nature of traditional platforms (i.e. a linear "dial" of channels in the EPG) means that public broadcasters are not difficult to find. By contrast, in connected TV platforms a public broadcaster might only be located through a search engine (if at all).

EU law already contains provisions for this in the case of traditional TV platforms, and the extension of this concept to the context of connected TV is expected to be one of the issues to be addressed in the forthcoming EU green paper on connected TV. [50] Introducing requirements on prominence in the Netherlands, for both traditional and connected TV platforms, might not only effectively harmonise the situation for all platforms, but also ensure the findability of public service content on new platforms. Exactly what requirements these should be, and what types of content should be covered, would be a key question for further study.

National/international dimension

Finally we turn to the national/international dimension. Key players in the connected-TV ecosystem are global in nature: platform (i.e. device) providers can be based in Europe (e.g. Philips) just as they can be based anywhere else (e.g. Apple, Sony). The same can be said of content providers: broadcasters are local, as are some OVDs like Videoland, which coexist with overseas-based OVDs like iTunes or Youtube. Jurisdictional issues are complex and varied, as for instance some overseas operators have European offices while others do not.

However if, as we have suggested, for the purposes of promoting openness (rather than must-carry), government is to focus on coordination efforts rather than legal or regulatory requirements, then issues of jurisdiction may be relatively unimportant. What may be more important is that industry coordination takes place at a scale large enough to be economically meaningful for key players – many of which, as noted, are international if not global. This suggests that EU-level efforts may be appropriate; for example, the HbbTV initiative and ETSI standards may point in the right direction.

49 Currently, both the UK and Germany mandate prominence of public service content on the EPGs of traditional TV platforms.

50 We note that Article 6(4) of the Access Directive refers to Member States' ability to impose obligations on providers of electronic programme guides (EPGs) and similar facilities. Whether these provisions already allow Member States to introduce findability requirements in connected TV (without further legislation) is a legal question without an established answer at the time of writing.

5.3 Case study 3: Privacy and interconnection in social networks

In the context of online social networks, there is a potential tension between the underlying advertising funded business model and the privacy concerns of end users. Also, network effects may lead to "winner takes all" situations in which a platform becomes dominant, which in turn may allow it to – for example – impose onerous privacy terms on its users. These concerns have been voiced extensively in connection to major social networks, and regulations are being drafted to address the main concerns.

5.3.1 Introducing social networks

Social networking is a highly concentrated space. Although the last decade has seen numerous social networks try to succeed, in each national market the space has generally tended to concentrate around one or two leaders. In general, this is the result of strong positive network externalities, which means that the value of joining a network increases with the number of contacts that a prospective member already has inside the network; this in turn means that once a network has reached a certain scale it is extremely difficult for a new entrant to challenge its position, because to potential members it may seem comparatively "worthless" even if its functionality (or privacy policy) is superior.

There are two exceptions to this, the first of which is geography. Since social network platforms rely on existing, real-world social links, two separate communities may (possibly by chance) take up different platforms, and again once a critical scale has been reached this position may become entrenched. However, in a globalised world no national community – much less northern European countries – is isolated from the rest of the world, and in recent years in multiple countries local players have given way to global leaders.

The Netherlands' experience bears this out. Local player Hyves was the number one social network in the country until 2011, when it was overtaken by Facebook. The table below shows the size of each social network platform in the world and in the Netherlands:

Figure 5.9: Main social network providers in the Netherlands and globally [Source: PCWorld, ComScore, Social Bakers, dutchnews.nl, provider's blogs and websites, 2013]

Social network	Global subs (million)	Netherlands subs (million)	Launch year
Facebook	975	7.5	2004
Twitter	500	5	2006
MySpace	125	insignificant	2003
LinkedIn	187	3	2003
Hyves	N.A	3	2004

The second exception is that sometimes different platforms cater for different user needs, rather than different user segments. Thus Twitter has a very different value proposition to Facebook (simple short messages visible to anyone vs. sophisticated functionality around a social graph), as does LinkedIn (a separate identity for one's professional life). The extent to which these market sub-sectors can remain

separate is an open question. However, we note that to the extent that these services are not substitutes for each other, their coexistence does not lessen the power that players in each sub-sector have over their users.

Importantly for us, most social network platforms are in the business of collecting and processing a wealth of information about their users, which they can also use for targeted advertising and other purposes. In addition to information explicitly given to them by their users (e.g. gender, age, location, education, etc.), platforms also collect "non-verbal" information such as:

- connections ("friends" in Facebook or "followers" in Twitter)
- activities (e.g. "wall-postings", "likes", "tweeting", "checking in" or even simply logging in from different locations, or following a link)
- pictures in which users are "tagged".

Armed with advanced software, platform providers are able to aggregate this data in sophisticated ways to build extremely rich pictures of their users.

5.3.2 Openness and privacy in social networks

Risk and potential harms

Online social networks have two key characteristics that make them worthy of policymakers' attention: (a) as closed communications networks they can exhibit winner-takes-all dynamics (see Section 4.3.2), and (b) their business model is predicated on the exploitation of information about end users.

This situation gives rise to two interrelated concerns:

- **Potential for abuse of market power:** as online social networks become increasingly central to modern life (especially for certain groups), it may be difficult for users to opt against joining (or staying in) a network.

- **Platforms' incentives mitigate against privacy:** platforms have strong incentives for collecting, processing and sharing data in multiple ways.

These two concerns interact. Platforms' respect of privacy is mainly driven by their need to retain their users' trust (as well as compliance with laws and regulations), but as platforms' power grows this link may be weakened. If users see no option but to join a specific platform, their trust may ultimately be only of secondary importance. In such a situation, legislation might be the main defence of end users.

Today, the main social networks are free for end users and are financed by revenues from upstream players such as advertisers and marketers. Rather than cash payments, the main (implicit) transaction that happens between end users and social network platforms is around personal information.

In this, platforms could use their power over users to impose unreasonable or abusive terms and conditions in take-it-or-leave-it privacy policies, which users rarely read, and could be unilaterally changed by the platform. Consequences for users could include unauthorised third parties having access to highly personal data and using it against users' interests.

Current observance of the public interest

Social networks today are at the centre of public debates about privacy. Key cases include:

- In 2012, MySpace enabled advertisers to match users' browsing history with their personal data (e.g. gender, age and name), thus violating its privacy policy and prompting the US authorities to intervene.[51]

- The US government intervened in response to concerns about Facebook's privacy practices, eventually reaching a settlement in 2012 in which Facebook undertook to observe users' privacy in specific ways (see below).

- In 2012, Instagram changed its privacy policy so that users' photographs can be used in advertisements without notification. This change had since been withdrawn due to users' strong opposition.[52]

- In 2007, Facebook introduced a controversial feature called "Beacon" whereby users' visits to sites unrelated to Facebook, but belonging to advertisers working with Facebook, were reported in users' timelines. Users were automatically signed up (the service was "opt out"). Facebook dropped the feature in 2009 following a lawsuit and a public apology.[53]

- In Germany, consumer credit firm Kreditech reportedly considers data from applicants' social network profiles (likes, friends, posts) when making credit decisions.[54]

In providers' defence, it should be noted that some of the major social networks have also taken steps to improve their communications on privacy issues with their users. A notable example is how in 2009, responding to controversy about unilateral changes to its privacy policy, Facebook introduced a system in which users were given the opportunity to vote before policy changes were made. However, the system only attracted a very small number of participants and after three years of low use it was recently terminated. This suggests that privacy concerns may be low on users' list of priorities.[55]

---

51 See http://thehill.com/blogs/hillicon-valley/technology/248775-ftc-finalizes-myspace-privacy-settlement.

52 See http://blog.instagram.com/post/38421250999/updated-terms-of-service-based-on-your-feedback.

53 See http://arstechnica.com/business/2009/09/facebook-beacon-shines-for-last-time-as-part-of-settlement/.

54 See http://www.slate.com/articles/technology/future_tense/2013/01/wonga_lenddo_lendup_big_data_and_social_networking_banking.single.html.

55 For the last vote before the scheme was shut down, only 0.038% of users voted. See: http://news.cnet.com/8301-1023_3-57449958-93/low-voter-turnout-means-new-facebook-privacy-policy-wins/.

5.3.3 The government's perspective

Policy/regulatory status quo

► *Data Protection Directive*

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data is the most relevant legislation for our study. In the Netherlands, it is implemented by the Data Protection Act, whose application is supervised by the Data Protection Authority (CBP).

The European Parliament is currently discussing a new General Data Protection Regulation which seeks to update the previous Directive so as to consider newer technologies and trends, such as social networks and cloud computing. This new regulation will be directly enforceable in all Member States when it goes into effect.

This new regulation has attracted numerous controversies, especially in relation to US companies lobbying against certain proposed aspects. Key issues under discussion include:

- **Purpose limitation:** the principle that personal data collected can only be used for specific purposes by the service providers storing and processing the data. Users ("data subjects") must agree to the specific uses to which their data will be put; under certain circumstances data may be used for purposes other than those informed to users when data is collected, but these may not be incompatible with the original purposes.

- **Right to be forgotten:** this involves giving users the right to compel companies that hold their personal data to delete it. Concerns about this – voiced, among others, by Facebook – include the complications that arise from the fact that much data is shared between multiple users; for example, when a user "likes" another's post, to whom does the "like" belong?

- **Definition of consent:** controversies include when consent can be "implied", and when/whether consent should necessarily be given prior to, and not as part of, performing an activity that results in data being gathered.

- **Data portability:** data portability is the right to take one's information away from one provider and onto another provider. With this right, if users are not satisfied with the way a social network platform deals with data privacy, they can port their personal data over to another platform. However, while data portability may marginally lead to an increase in switching, we do not expect this effect to be significant while social networks retain their network effects (which stem principally from a lack of interconnection, not of data portability).

- **Unilateral changes to terms and conditions (Ts&Cs):** often, service providers change their terms and conditions, which could concern privacy settings and data usage, without seeking users' agreement. This could be curtailed under proposals being discussed.

► *E-Privacy Directive*

The 2012 EU e-Privacy Directive, referring to the Data Protection Directive, requires advertisers and website owners in the EU region to provide information about their purposes for gathering user data, and to obtain consent from users. Because the Directive applies mainly to the storage of information on consumers devices (i.e. the use of cookies), its relevance to our case is limited (since social networks can but do not fundamentally need to rely on cookies for their tracking). Furthermore, some of the same issues are being discussed in the context of the Data Protection Regulation (above). For these reasons, we omit a more detailed account of this directive here.

► *Safe Harbor Privacy Principles*

International social networks based outside of the EU, such as Facebook or Twitter, transfer user data from the EU to a destination outside of the zone. According to the EU Data Protection Law, transfer of personal data to a third country is allowed only if the country in question has adequate or on-par data protection standards. Originally this posed a problem, as an audit of the US data protection regulation failed to meet the more exacting standards of EU data protection principles.[56] However, the assurances given in the Safe Harbor Privacy Principles[57] issued by the US Department of Commerce solved this problem, and since then it is now legal for data to be transferred from the EU to the USA.

► *Facebook/FTC settlement*

In 2012, Facebook reached a settlement with the US Federal Trade Commission (FTC) on its data use policy. As part of this agreement, Facebook undertook to:[58]

- obtain users' consent explicitly before implementing changes that override their privacy settings
- prevent anyone from accessing a user's data more than 30 days after the user has deleted his/her account
- establish and maintain a comprehensive privacy programme designed to address privacy risks associated with the development and management of new and existing products and services
- protect the confidentiality of users' information
- get an independent third party to conduct privacy audit to certify that its privacy policy is in line with the requirements of FTC for the next 20 years.

It is our understanding that the requirements placed on Facebook by the FTC are stronger than those placed on social networks by existing or planned European laws and represent a high watermark of intervention to date.

56 See ENISA: "Study on data collection and storage in the EU, 2012" Available at http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/data-collection.

57 See http://export.gov/safeharbor/eu/eg_main_018476.asp.

58 Source: http://ftc.gov/opa/2012/08/facebook.shtm.

Case for intervention

The underlying causes for platforms potentially failing to respect privacy stem mainly from their strong bargaining power versus end users, which in turn is a result of network effects leading to high market power. The situation is detailed in Figure 5.10 below, which applies our general framework from Section 4.3.

Figure 5.10: Our economic framework as applied to social networks [Source: Analysys Mason, 2013]

Driver of market under-provision	Relevance to privacy and lack of openness in social networks
Concentration/limited alternatives	• As a result of a lack of interconnection, social networks are highly concentrated
Switching costs	• Even if a competing platform is attractive (because a user may have many contacts in it), a lack of data portability means that migration of data (personal data, history, connections, etc.) is difficult
Asymmetric information	• It may be difficult to assess how well a provider respects privacy • Users do not necessarily know which data is being collected, how the collected data is being used and who the data or access is given to
Experience goods	• Users may be indifferent to privacy concerns until a major incident concerning their personal data occurs
Closed business models	• Being closed is likely an essential aspect of providers' business models, as witnessed by their general failure to interconnect
Business model based on exploitation of consumer data	• Social network providers have a second type of customer other than consumers – i.e. advertisers – who may either seek access to consumers' data (where allowed), or may expect the service provider to process consumers data on their behalf (e.g. so as to target advertisements)
Low private demand	• Users may not sufficiently value or care about privacy[59]

Potential policy approaches to addressing the issues above include the following:

► *Addressing closed business models and the lack of meaningful alternatives*

Possibly the most effective way to address providers' market power would be to address the underlying barriers to entry. These are related to the fact that the key platforms are closed and do not interconnect. Hence, an effective measure could be to mandate interconnection.

However, this would be a highly intrusive measure that could have important unintended consequences. For example, conceivably, the prospect of similar interventions could have a deterrent effect on start-up entrepreneurs or investors considering new closed networks; and the current "free to the end user (in exchange for some personal information)" model offered by major social networks might be ended. We thus do not recommend this approach. We return to this point in Section 6.

59 For example, Facebook polls on its policy changes regarding the elimination of user voting system only saw around 680,000 users participating, which shows that the majority of the general public is indifferent about Facebook's Data Use Policy changes. Source: http://news.cnet.com/8301-1023_3-57449958-93/low-voter-turnout-means-new-facebook-privacy-policy-wins/.

► *Addressing switching costs*

Mandating data portability should go a long way towards helping users switch between networks. However, we note that without meaningful alternatives (that is, alternatives that are not only technically good, but that also allow users to continue communicating with their contacts) consumers are unlikely to switch.

► *Addressing asymmetric information*

If evidence emerges that providers are not respecting their stated privacy policies, government could consider mandating independent auditing of platforms' operations. An alternative would be litigation by end users or tighter legislation aimed at ensuring transparency.

► *Addressing the exploitation of data*

Given the central role that data plays in platforms' business models, it is unlikely that any steps that the government takes can decrease providers' incentives to exploit data. Given the significant complexities involved in data exploitation, it is unlikely that end users will be able to effectively negotiate a privacy policy, even in a context of full transparency. Given this, we believe that the direct regulation of data exploitation will be required to some degree – as is being done through the EU Data Protection Regulation.

► *Addressing the lack of private demand for privacy and experience goods*

Perhaps the main intervention that could be considered on this front is education of end users – whether directly by the government, or by working with platform owners.

► *Summary*

Figure 5.11: Social networks: issues, current position and possible interventions [Source: Analysys Mason, 2013]

Issue	Status quo	Possibilities
Concentration/lack of meaningful alternatives and closed business models	• Social networks have high market power as a result of network effects	• Forced interconnection (not recommended)
Switching costs	• Switching platforms is difficult	• Ongoing EU discussion of mandating data portability
Asymmetric information	• Users may have no visibility on uses to which their data is put	• Education of end users either by governments or by social networks • Consider audits, if in future stated policies are not observed
Business model based on exploitation of consumer data	• Social networks' business model is based on the exploitation of consumer data – this is unlikely to change	• Regulate data exploitation – as per EU Data Regulation Directive
Under-valuing of privacy	• Users seem unmotivated to engage with privacy options	• Education of end users

National/international dimension

Given the global nature of the players involved, for regulatory approaches, at a minimum an EU-level approach is needed, since this allows enforcement for players with EU subsidiaries. Nonetheless, we note that emerging and/or specialised social networks may have no EU offices and are likely to pose jurisdictional and enforceability challenges.

5.4 Case study 4: Availability and cloud infrastructure services

In our final case study, we consider the issue of (problems with) availability in cloud hosting services – that is, the underlying infrastructure behind many online services. Unlike the situation in other case studies, here we see no compelling evidence or arguments suggesting that the market is likely to under-provide availability at an adequate price. This is not to say that there are no potential concerns. Two concerns are the possibility of systemic failure stemming from complex interdependencies among providers, and the possibility that small start-ups may be priced out of adequate availability. Intervention options include education of small businesses on ways of maximising resilience in case of cloud outages.

5.4.1 Introducing cloud hosting

Cloud computing in general

By cloud computing we understand the provision of IT resources as services. By "as services" we mean that resources can be provisioned and discarded with little or no notice, typically automatically. Key characteristics of cloud computing include:

- virtualisation and sharing of underlying physical resources, which leads to better utilisation of capital, and hence efficiencies
- scalability and elasticity, so that extra resources can be provisioned as demand grows, sometimes in a matter of minutes.

Cloud computing can be self-provided by large firms with sufficient resources to invest in cloud infrastructure, and sufficiently diverse internal demand for IT resources to allow the benefits above to be exploited ("private cloud"). Firms can also outsource the running of a private cloud to a third-party provider. In this case, the provider can optionally increase efficiency (and offer a lower price) by relying on virtualisation technologies to share resources across customers ("virtual private cloud"). Finally, customers can also hire virtual resources in isolation ("public cloud").

Under the "public cloud" and "virtual private cloud" models, cloud computing is typically charged on a variable, utility-like basis e.g. server-hours, storage space used, etc. For customers, this means a shift in the cost structure associated with IT infrastructure from fixed capex to variable costs, which in turn removes risk and allows small companies to perform computing tasks that would normally have required large amounts of infrastructure capital (for example, serving web pages to millions of daily

visitors). This in turn has been a key enabler for innovative start-ups which can scale up rapidly without increasing their risk.[60]

The Internet can be involved in cloud computing in two ways. First, it can be used to link the customer (that is, the firm hiring computer resources) with the cloud resources hired. Second, if the customer firm is in the business of running a web service (for example, a consumer-facing social network), then it can rely on a cloud provider to host the necessary infrastructure to serve its end users. In this case, the cloud provider needs to offer not only basic computing resources but also specialist infrastructure needed for hosting public-facing online services (e.g. high-speed, redundant connections to multiple transit providers).

Our focus in this case study is the use of outsourced cloud services as the infrastructure behind online services targeted at end users. This includes the three service models that will be introduced below (SaaS/PaaS/IaaS) but only inasmuch as they are provided on a wholesale basis to online players to power their services.

Segmenting the cloud space

For the purposes of our analysis in this case study, cloud computing offerings can be segmented along two dimensions of customer need: value-add and geographical sensitivity:

► *Value add – the "stack"*

Cloud computing services can be categorised according to the level of functionality (or "abstraction") offered, ranging from raw computer power (i.e. the renting of a server on an hourly basis) and storage, to web-based enterprise software such as customer-relationship-management (CRM) software. A common categorization is shown in Figure 5.12 in which each "layer" can rely, and build on, services provided on the layers below it: [61]

Figure 5.12: The cloud functionality "stack" [Source: Analysys Mason, 2013]

Service model	Description	Examples	Key players
Software-as-a-Service (SaaS)	Business-level functionality. Includes end user-facing applications and API-based services as building blocks in other solutions	• Customer Relationship Management (CRM) • Enterprise Resource Planning (ERP) • Email	• Salesforce.com • NetSuite • Box.net • Outlook.com

60 For example, if the advertising revenues for each web page served are just marginally above the variable cloud costs per page served, then a start-up can scale up its traffic to any size as quickly as demand grows without requiring any extra capital (other than perhaps working capital).

61 The terms SaaS, PaaS and IaaS relate to our Internet value chain in Figure 5.1 (p 45) as follows: providers of all three types often sell services to online service providers for use in their end user-facing propositions. When they do so, they are the focus of this case study and correspond to sector 2.3 in our value chain. However, providers of all these types also offer services, over the Internet, to customers who are not in the business of providing online services; such activities are outside the scope of this case study (and may fall under sector 1.2 of our value chain). Finally, the literature occasionally refers to certain consumer-facing online services such as storage or music streaming services as "consumer cloud" or "consumer SaaS". In our scheme these are simply consumer-facing online services (sector 1.1); we reserve the term SaaS for business-facing services only.

Service model	Description	Examples	Key players
Platform-as-a-service (PaaS)	As IaaS plus key common building blocks of technical functionality needed by common applications	• Pre-configured database systems • Integrated content distribution networks (CDNs)	• Amazon SQS • Rackspace • Microsoft Azure • Google App Engine • Salesforce.com
Infrastructure-as-a-Service (IaaS)	Core computing infrastructure, provided remotely usually in virtualised form	• Virtual servers • Storage	• Amazon EC2 • Microsoft Azure • Google compute • Rackspace • Savvis

► *Geographical sensitivity*

Thanks to the Internet, cloud service provision is to a large extent a global market. When customers are indifferent as to where their data is stored or processed, they can obtain resources from anywhere in the world. However, in practice they are not always indifferent as to location. Factors that may prevent customers from sourcing providers globally include:

- **compliance with law or contracts**, e.g. EU or national requirements regarding personal data protection, or private contracts specifying details about how information is to be processed and where[62]
- **connectivity:** firms transferring large amounts of data or requiring low **latency** to and from their cloud provider may need high-quality, dedicated connectivity
- **confidentiality:** firms may prefer suppliers whose security arrangements can be verified in-situ and/or who may be able to sign ad-hoc confidentiality agreements
- **unique technical requirements:** firms may require unique contractual provisions and/or custom technical arrangements, all of which may be best handled by a local provider
- **cultural factors:** firms may prefer to source their services from a trusted local provider with whom they may have a face-to-face relationship.

In terms of these dimensions, the following six high-level categories can be identified:

62 Reportedly, customer concerns about the possibility that US firms might have to surrender their customers' data to US authorities under the US Patriot Act have led some European providers to offer "Patriot-Proof" services – see http://readwrite.com/2012/02/02/the-ups-and-downs-of-the-ameri

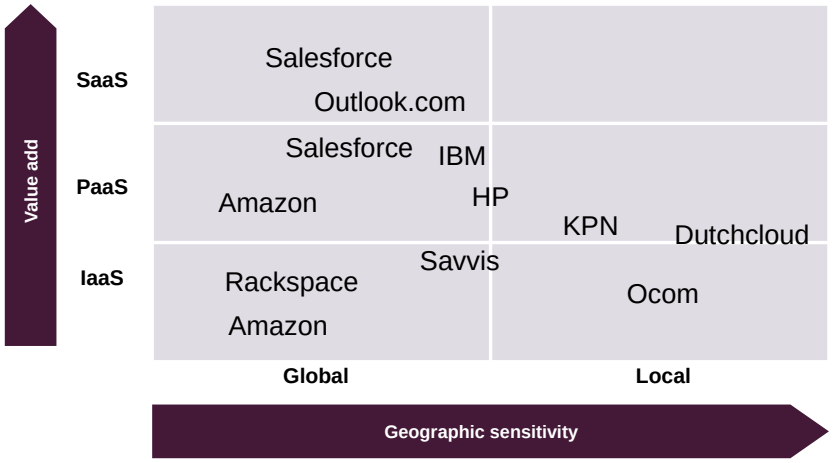


Figure 5.13: Segmentation of the cloud services space (firms' positioning is indicative; some firms are present in more areas than indicated) [Source: Analysys Mason, 2013]

Strategic analysis

The following points about strategy will be relevant to our later discussion of the case for intervention in this space:

- The bottom-left corner is a global market, itself further sectored into
  - a commodity market where competition is largely based on **price/cost** leadership driven by economies of scale and experience. It is dominated by large global players like Amazon and Rackspace. Providers employ a self-service, zero-fixed-costs model that is particularly attractive to small Internet start-ups (although larger players also use these services)
  - a large variety of other providers offering different levels of customization, performance, security, etc. – at different price points. Some of the (many) players in this space include Savvis, IBM, Joyent, HP and major telecoms groups.

- As customers' requirements grow in sophistication and go up the "stack" (middle and top rows), the basis of competition shifts towards **differentiation** in terms of innovation and unique technology. Providers' use of proprietary interfaces means that customers must develop vendor-specific solutions, which increase **switching costs** and can lead to lock-in.

- On the right side of the framework (local market), market conditions are similar, except that lower competition (given geographical considerations) means that suppliers have more power. Also, suppliers' smaller scale means that they might struggle to match the costs of an Amazon in terms of entry-level utility computing and storage.

5.4.2 Availability in cloud hosting

What a lack of availability means

By a lack of cloud availability, we mean a loss of service in a cloud service supplied to an online service provider, so that the online service's availability to end users is disrupted, and/or the service

owner cannot control its own service. Clearly, a cloud outage can have significant consequences and can affect millions of end users. For example, an outage of Amazon's EC2 service can result in:[63]

- online services like Netflix or Dropbox, Spotify or many others becoming unavailable to end users, and/or
- the owners of Netflix or Box.net not being able to control their services so as to e.g. invoice and bill their customers, suspend delinquent users, manage their film catalogue, etc.

Technical causes

While adopting cloud computing has many advantages, its implications for availability can be varied. In certain online services' set-ups, a cloud vendor may act as a **single point of failure**, which means that if the vendor fails, so does the (end user-facing) online service. When this is due to a single vendor providing the bulk of the infrastructure for a given service, the problem can be partially mitigated through:

- encapsulated resilience: a vendor can offer (possibly for an additional fee) services supported by resilient infrastructure, offering higher availability
- cross-provider redundancy (see Section 4.3.1): customers can set up parallel infrastructures with multiple cloud providers so none of them is a single point of failure. However, this requires additional engineering effort and ongoing costs
- intra-provider redundancy: some providers run multiple separate cloud infrastructures, in different geographical locations, and allow their customers to manage their services on each – much as in the case of cross-provider redundancy.

Nonetheless, even if best practices like the above are adopted, a possibly more fundamental problem is created by the **increasing complexity** of the **interdependencies** between the systems involved in many online services. For example, a given online service may rely on one provider to host its core infrastructure (under an SaaS/PaaS model), on another to provide geographical intelligence service[64] and yet another to handle its advertising (under an SaaS model). In certain situations, any of these could act as a single point of failure. Furthermore, each SaaS provider could rely on different IaaS/PaaS providers for its basic infrastructure. For major cloud providers like Amazon or Rackspace, this suggests a potential for systemic failure associated to "too big to fail" players, somewhat analogous to the way that major banks have the potential to single-handedly disrupt the entire financial system due to complex interdependencies between financial players. We stress, however, that at this stage this is rather speculative and more research would be needed to ascertain whether a concern would be justified.

63 In 2011, Amazon's AWS infrastructure was estimated to account for 1% of all Internet traffic in North America; see http://www.wired.com/wiredenterprise/2012/04/amazon-cloud/. It has also been estimated that up to 1/3 of Internet users each day use a service powered by Amazon; see http://gigaom.com/2012/04/20/just-how-big-is-the-amazon-cloud-anyway/

64 Geo-location services allow online services to determine the geographical location of their users for purposes such as copyright compliance.

Current observance of the public interest

Typically, PaaS and IaaS solutions are designed to high specifications to minimise downtime. As a result, outages are rare. Recent research[65] by cloud firm Rightscale found that in 2012 there were only 27 "notable" cases worldwide, of which only about a third (around 10) involved services in the SaaS or IaaS categories, and 21% were due to natural disasters; the average downtime was around eight hours. Some key events include the following:

- in February 2013, Microsoft's Azure service became unavailable for twelve hours globally as a result of an expired SSL certificate[66]
- in December 2012, Amazon's cloud service suffered partial unavailability[67] that led to major services like Netflix becoming unavailable
- in October 2012, Amazon's cloud services suffered a partial outage, but due to adequate planning major customer Netflix was able to offer uninterrupted service[68]
- in February 2012, a power outage brought down Microsoft's Azure platform.[69]

5.4.3 The government's perspective

Policy/regulatory status quo

In general we are not aware of sector-specific regulations or legislation relating to the provision of cloud services regarding availability. Perhaps the most relevant legislation is the EU Directive and Dutch Act on data protection (discussed in Section 5.3.3 above), but its relevance to availability is limited.

Nonetheless, as part of its Digital Agenda, the EC has recently published a strategy document[70] outlining potential areas of intervention. Relevant points include:

- concerns about vendor lock-in
- corresponding need for cross-vendor standards and certification
- cloud customers' difficulties in negotiating contracts, especially in the case of small firms purchasing services from large providers who may offer "take it or leave it" contracts.

Although the EC's document reflects expert opinion, it does not provide clear evidence that the issues above are acute, or that market players may not be able to address them without intervention..

65 See http://blog.rightscale.com/2013/02/27/lessons-learned-from-recent-cloud-outages/

66 See http://www.cio.co.uk/news/3428291/microsoft-azure-outage-caused-by-expired-ssl-certificate/

67 See https://aws.amazon.com/message/680587/

68 See http://gigaom.com/2012/10/30/once-again-netflix-shows-how-to-avoid-a-cloud-meltdown/

69 See http://www.cio.co.uk/news/3341136/microsoft-azure-outage-downs-g-clouds-cloudstore/

70 European Commission: "Unleashing the Potential of Cloud Computing in Europe". Available at http://ec.europa.eu/information_society/activities/cloudcomputing/docs/com/com_cloud.pdf

The case for intervention

Faced with limited evidence of problems, our approach is to combine our strategic analysis of the cloud space in Section 5.4.1 with our economic framework in Figure 4.8 (p 39) to develop a view of what issues *may* require policymakers' attention.

A preliminary application of our economic analysis to the case of cloud providers suggests a strong overlap with the issues identified by the EC.

Figure 5.14: Our economic framework as applied to availability [Source: Analysys Mason, 2013]

Type of market under-provision	Relevance to availability in cloud services
Concentration/limited alternatives	• Market concentration around low-cost players could mean buyers unable to negotiate adequate availability guarantees
Switching costs	• If switching costs are high customers may be forced to accept poor service quality or higher prices
Experience goods	• If outages are extremely rare, customers may be unable to adequately assess the risk or unavailability and (hence) negotiate appropriate contracts
Lack of liability	• A lack of proportionate liability might lead providers to under-invest in availability

However, as we discuss briefly below, a consideration of our strategic analysis in Section 5.4.1 and the evidence of outages discussed in Section 5.4.2 suggest that some of these concerns may be unjustified (we stressed the word *may*; our analysis is only tentative). In particular:

► *Concentration/lack of choice*

Although the market is relatively concentrated at the low-price commodity end, it also contains a variety of higher-priced "enterprise class" providers (e.g. Savvis, IBM, Joyent, HP) that offer higher levels of reliability at a price. Indeed, being able to specify redundancy at a technical level is one of the advantages of the "private cloud" model.

Even mass-market providers offer additional resilience options at extra cost (e.g. so-called "availability zones" on AWS, which allows geographical diversity to be built in).

► *Switching costs and lock-in*

Switching costs may be a concern, especially at the high-functionality end if customers develop "asset specific" software using vendors' proprietary APIs. However, key developments suggest that market providers may address these issues without intervention. For example:

- standards like Openstack seek to provide a vendor-independent layer of functionality so that users can switch providers seamlessly; and
- firms like Rightscale and Cloudability specialise in helping cloud users work with multiple providers at the same time, thereby both increasing overall availability through cross-provider redundancy and, as a result, greatly reducing switching costs (see our discussion in Section 4.3.1).

Whether the issues will be fully addressed by the market, and to what extent, is difficult to tell at this early stage of the industry's development. Government should monitor these developments.

► *Experience goods and tail risks*

The relatively high availability of major cloud providers may ironically be one of the sector's main problems. The less frequent outages are, the less experience customers have of the consequences that may be involved, and the less they may be able to pay for higher availability when negotiating a contract. As a key industry player observed in the wake of a major outage, "with [a provider's] overall stellar operating reliability it is easy to become complacent."[71] The problem is particularly relevant in the context of the potential systemic risks discussed earlier in this case study.

► *Lack of adequate liability*

On the face of it, lack of liability might appear to be a problem. For example, after a 12-hour outage Amazon compensated its customers with only a 10-day credit voucher.[72] However, our point above applies here: given the wide variety of alternative providers, including local firms, customers' failure to secure contracts with adequate liabilities may be due mainly to a low willingness to pay. We note that small customers whose budget may not be sufficient for anything but entry-level public cloud IaaS may not be able to negotiate better contracts; however, it is feasible that such low prices would not be possible if providers were required to accept high liability. It is also possible that the resulting availability of these entry-level public cloud services is greater than availability with equivalent spending on other, non-cloud IT solutions.

► *Summary*

In summary, in general we see no strong reasons to expect that the market would fail to provide adequate availability at a competitive price. Further, customers have ways of minimising the impact of unavailability, and new providers are working on helping customers decrease their reliance on single providers.

The main point that appears to be problematic is the "tail risk" and "experience good" nature of cloud outages – because they are rare, customers may be unprepared and fail to invest in the necessary redundancy. Government may be able to help mitigate this by educating cloud customers – especially small firms – about the need to plan for outages. If necessary, government could also work with industry to help produce the standards that would help customers achieve cross-provider resilience.

Concerns about lock-in remain, but their ultimate justifiability seems at this point unclear. Likewise, although we acknowledge (as the EC notes) that small customers may have a hard time negotiating contracts with high liability on the provider's part, this may well be a matter of costs of provision rather than market power. We suggest that policymakers should continue to monitor these issues in the coming years.

71 Rightscale CTO Thorsten von Eicken – see http://blog.rightscale.com/2011/04/25/amazon-ec2-outage-summary-and-lessons-learned/.

72 See http://www.pcmag.com/article2/0,2817,2384631,00.asp.

National/international dimension

Regulatory and standards-based options call for EU-level approaches; standards-related work may also call for global-level coordination. On the other hand, education-based options can be pursued at a national level.

6 Openness, innovation and a level playing field

Although so far in this report openness has been presented as one among many different public interests, in many ways its role is more important than that. Arguably, openness in the form of net neutrality is one of the Internet's defining characteristics. It has key impacts on online services, traditional telecoms services, and ISPs. In turn this raises questions about the relationship between openness, innovation and competition between online and traditional services.

In the literature on openness and the Internet,[73] openness is often associated with entrepreneurship and innovation. It is claimed that an open Internet allows online start-ups to flourish, that open standards lower barriers to entry for small innovative technology companies and that the sharing of open software leads to better technologies. While all of this may be true in some cases, it does not follow that openness is always and everywhere positive for innovation, or, more generally, that its overall effect on market participants in positive. In what follows, we discuss the complex set of impacts that can be expected from net neutrality as a paradigmatic case of openness, and then discuss wider implications for openness policies in general.

6.1 The effects of net neutrality

Openness by ISPs (i.e. net neutrality, even before it was law in the Netherlands) has been a foundational, defining characteristic of the Internet. By providing online service providers with universal access to consumers at low cost and on a non-discriminatory basis, it has allowed a large number of online sectors and sub-sectors to flourish. In turn, this has implications for:

- competition among online service providers, many of whom (perhaps paradoxically) turn to closed models
- non-Internet service providers, which experience disruption
- ISPs, whose service becomes more of a "commodity".

We discuss these impacts separately below, and then discuss implications in Section 6.2.

6.1.1 Competition among online services

Net neutrality means that online players cannot compete on the basis of differential ability to reach end users through exclusive or preferential access to the last mile, since this is something that all online players possess. But this does not mean that other sources of competitive advantage are unavailable. Just like their counterparts elsewhere in the economy, online entrepreneurs and investors look for business models that can limit the effects of competition within their sectors so as to maximise profits.

[73] See e.g. Barbara Van Schewick, *Internet Architecture and Innovation* MIT Press, 2010.

Importantly, in many cases these business models rely on a lack of openness. Thus, for example:

- Social networks and closed communication platforms (e.g. Skype, Whatsapp) exhibit "direct" network effects whereby the value that a service offers to its users increases with the number of users that join. In certain cases, this can lead to "winner-takes-all" dynamics in which once a player achieves a certain size, other competitors become unviable, producing a monopoly-like situation.

- Certain online content platforms rely on vertically integrated business models, whereby the device can only connect to its manufacturer's own online service (e.g. Kindle), or give its manufacturer's online service preferential treatment (e.g. iPhone, Android). In other cases (e.g. some connected TV platforms), devices can only access those content providers with whom they have signed deals – which may be exclusive.

Thus, paradoxically, although online services rely on ISPs' openness for their existence, many have business models that are predicated on a *lack* of openness within their own sectors. We discuss the potential implications of this below.

6.1.2 Impact on incumbents

As Internet connectivity improves, service providers that do not rely on the Internet as a distribution mechanism are disrupted by online players that can deliver competitive services "over the top" (OTT). The main cases here are traditional operators' voice and TV services, but the disruption extends to their suppliers too, e.g. TV channels and telecoms equipment vendors.

As non-Internet players begin to be challenged by Internet-based competitors, competition is not necessarily on a like-for-like basis. At a technical level, Internet and non-Internet platforms present multiple differences that mean that each has its advantages and disadvantages (e.g. traditional cable distribution allows for fewer content providers but offers a more reliable service than OTT alternatives).

Different conditions also apply in the regulatory domain, as traditional players are usually subject to more restrictions than their online counterparts. Earlier in this report (Section 5.2.3), we discussed the asymmetry between current regulations for connected TV and traditional TV platforms. Similar asymmetries between traditional and OTT services are commonplace in the Internet. Some key examples are listed in Figure 6.1 below:

Figure 6.1: Asymmetries in obligations [Source: Analysys Mason, 2013]

Type of obligation	Traditional players	Internet players
Carriage of content providers in TV platforms	• "Must carry" obligations concerning public broadcasters	• No obligations in place
Interconnection	• Voice telephony interconnection is mandated at regulated prices	• No interconnection/interoperability is mandated for voice apps (unless they use telephone numbers) or social networks
Privacy	• Obligations apply explicitly to telecoms operators	• New Data Protection Regulation will likely lead to level playing field

Type of obligation	Traditional players	Internet players
Availability and security	• Recent "duty of care" legislation for voice providers; EU Publicly Available Telephone Services (PATS) provisions	• PATS provisions apply to subset of Internet voice players

6.1.3 Impact on ISPs

By its nature, Internet access is a service allowing only limited differentiation – all providers offer access to the same thing, namely the entire Internet. The more consumers' bandwidth requirements are met, the more they buy Internet access as a standalone product (which "cord cutting" and OTT services may one day do), and the more the service becomes a commodity and competition becomes price-driven.

6.2 Policy implications

Just as in our discussion of openness in the particular case of TV distribution, at first sight the general situation described above gives rise to two interrelated questions for policymakers:

- Should openness be imposed on online services?
- Should regulatory obligations be harmonised for Internet-based and non-Internet-based players, so as to achieve a level playing field?

However, as in the case of connected TV, in our view addressing these questions directly would be the wrong approach. Openness is not so much an end in itself as a means towards other ends – namely, innovation, pluralism and improved communications for consumers – and the value of these goals should be weighed against the importance of obtaining a "level playing field". The answer is likely to be context-specific, and in each case the decision may be ultimately political.

Nonetheless, here we propose some general considerations that policymakers may wish to bear in mind when considering these questions:

6.2.1 Considerations regarding openness requirements for online services

The case for introducing openness obligations on online services should be weighed against the following:

- The profits that closed business models can generate may be key drivers of investment and **innovation** in online sectors.[74] Any potential short-term, static benefits of mandated openness should be weighed against the potential dynamic, long-term effects on future investments in online sectors.

[74] For a recent, informative discussion of this in the context of social networks, see Justin Fox, "The New Monopolists" in *The Atlantic*, January 2013, available at http://www.theatlantic.com/magazine/archive/2013/01/the-webs-new-monopolists/309197/.

- The likelihood of any resulting market power being **durable** should be assessed carefully. For example, Myspace was a dominant social network only a few years ago, only to be relegated to relative obscurity by Facebook. The same could happen in the next few years. "Schumpeterian innovation" may be a natural antidote to online players' market power.

- The potential **harm** to the public interest that can be caused by a lack of openness varies from one case to the next. For example, the public interest is relatively unharmed by an online game that does not interoperate with other games.

6.2.2 Considerations regarding harmonisation

Although we are sceptical about the merits of an across-the-board harmonisation of obligations between online and non-Internet providers, at a general level there is arguably a case for some of the key legislation to be revised and/or re-interpreted in the light of technical developments. Much of the underlying regulations concerning traditional operators were written at a time when the Internet's separation between service and network provision was not common, and when "television" and "broadcasting" were more or less synonymous. Thus, for example, many of the relevant provisions in both the EU Universal Services Directive and the EU Access apply to undertakings providing "electronic communications networks" and to the distribution of "television broadcasting services" – which technically may not apply to online service providers, even if the underlying rationale would be similar. There may be a case for a general review of relevant legislation with a view to ensuring that, where appropriate, rules are technology-neutral.

6.2.3 Considerations regarding the ISP sector

Finally, if net neutrality is to remain in place for ISPs and consumers opt for "over-the-top" services, there is a possibility that Internet access might become an undifferentiated commodity. However, this does not necessarily imply that the ISP sector would become unprofitable or unattractive to investors. The provision of a valued commodity may well be a profitable business, depending on the level of competition to be expected (or encouraged) within the ISP sector. In turn, this depends on questions related to the regulation of last-mile network investments (e.g. unbundling obligations, spectrum policy, etc.) that are beyond our scope. We point out, however, that in this scenario the ISP sector might not be characterised by constant innovation in terms of the service offered to end users. To a certain extent, the imposition of openness implies a pre-determined service and business model for ISPs and, consequently, a constraint on innovation by ISPs.

6.3 Openness and industrial policy

In general, the effect of openness (whether mandated or not) on market players is to render certain inputs available to all market participants. This means that those inputs are no longer a source of competitive advantage so that players must compete on a different basis.

This applies not only to the case of net neutrality discussed above in the context of ISPs, but also more broadly. For example, openness in connected TV would mean that all content providers could count on

being able to reach all consumers that use open platforms, and in turn this would mean that competition in their sector would not be based on negotiating the best distribution deals but (perhaps) on offering the best content at the lowest price. Similarly, competition among platforms would revolve around aspects such as features and price, and not around which content providers each platform's users can access. Just as in the case of ISPs, while this does not mean that connected TV platforms would be an unprofitable business under mandated openness, it does mean that the sector would have certain constraints in terms of its products and business models, and at least to some extent this would limit innovation in platforms (even if it encourages innovation among content providers).

More generally, openness obligations may constrain innovation in the sectors where they are imposed, even if at the same time they encourage innovation elsewhere. Where this is the case, the relationship between openness and innovation is ambiguous; it cannot simply be said that openness leads to innovation, but rather that openness may encourage certain types of innovation in certain sectors, while at the same time possibly constraining it in others.

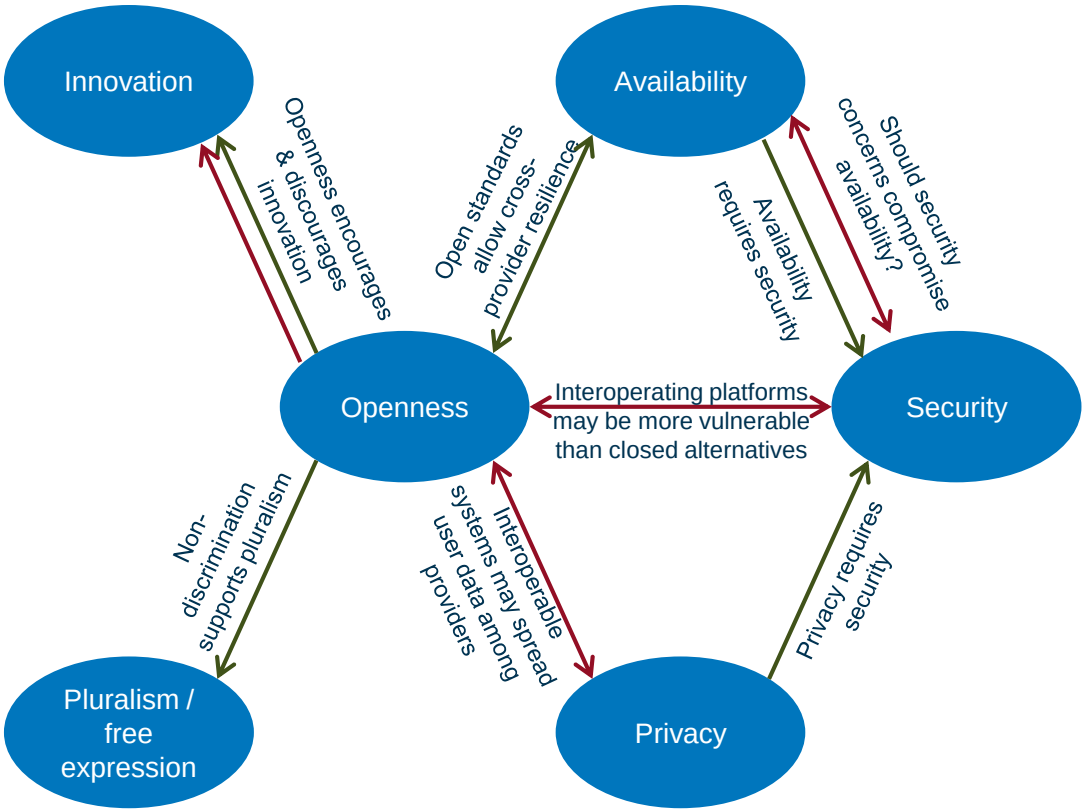
To the extent that this is the case, openness regulations entail a certain degree of industrial policy, turning certain resources into "infrastructure" on top of which other businesses can be built, possibly by other firms, based on new types of barriers to entry. While the potential benefits of success may be significant, the risks of "betting on the wrong horse" cannot be ignored.

7 Concluding remarks

Our aims in this study were to provide a picture of the Internet value chain, show how the public interests relate to different types of player, and on the basis of this produce a framework for government intervention when market provision is unlikely to meet the public's needs. We have also explored how this applies to four case studies, both as a way of exploring certain key issues and of showing how our framework can be applied.

As we discussed earlier, the various public interests involved in the Internet include difficult trade-offs that are inherently political decisions. The main relationships between public interests are shown in Figure 7.1, in which red arrows denote tensions and green arrows denote dependencies:

Figure 7.1: Key relationships between public interests [Source: Analysys Mason, 2013]



Key relationships that we explored include:

- The positive link between openness and pluralism – as discussed in Section 4.2.2.
- The ambiguous link between openness and innovation, encouraging innovation in sectors that rely on the inputs that openness makes available, while potentially also limiting innovation in the sectors where openness is imposed – as discussed in Section 6.

- The trade-offs between availability and security – for example, when a provider must decide whether to shut down a service that may have become compromised, even though the service is essential to its users – as in the case of Diginotar discussed in Section 5.1.

Other important relationships include:

- Tensions between openness
  - and security, since open and interoperable platforms with open APIs may be more vulnerable to cyber attacks than closed alternatives
  - and privacy, since data protection requirements may be difficult to audit or enforce across multiple interoperating systems
- The clear dependency of privacy and availability on security.

Over the next decade, as the Internet's importance to society grows even beyond current levels, this complex set of relationships between public interests is set to become increasingly important to policymakers. There are no easy solutions, and with industries pitted against each other the arguments on each side of the main trade-offs are likely to be articulated in increasingly sophisticated ways. Policymakers will need to master the issues and be prepared for a series of potentially difficult, case-by-case decisions. We hope that this report will provide a useful start in this area.

Annex A Glossary of terms

API – *Application Programme Interface*

A set of tools and protocols to build software applications.

CDN – *Content Delivery Network*

An interconnected system of computers on the Internet that provides online content rapidly to numerous users by duplicating the content on multiple server s and directing the content to users based on proximity.

DNS – *Domain Name System*

The way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address.

DRM – *Digital Rights Management*

A system for protecting the copyrights of data circulated via the Internet or other digital media by enabling secure distribution and/or disabling illegal distribution of the data.

FTA – *Free-To-Air*

Television (TV) and radio services broadcast in clear (unencrypted) form, allowing any person with the appropriate receiving equipment to receive the signal and view or listen to the content without requiring a subscription (or other ongoing cost) or one-off fee (e.g. Pay-per-view).

IM – *Instant Messaging*

The exchange of text messages through a software application in real time. Instant messaging differs from ordinary e-mail in the immediacy of the message exchange and also makes a continued exchange simpler than sending e-mail back and forth.

ISP – *Internet Service Provider*

A company that provides consumers with access to the Internet. An ISP has the equipment and the telecoms line access required to have a point-of-presence on the Internet for the geographical area served.

IXP – *Internet Exchange Provider*

A company that provides the physical infrastructure through which ISPs exchange Internet traffic between their networks (autonomous systems). An IXP allows networks to interconnect directly, via the exchange, rather than through one or more third-party networks. The advantages of the direct interconnection are numerous, but the primary reasons are cost, latency and bandwidth.

Last mile

The final leg of a telecoms network that carries signals from the broad telecoms backbone along the relatively short distance (hence, the "last mile") to and from the home or business. Or to put it another way: the infrastructure at the neighbourhood level.

LLU – *Local Loop Unbundling*

A local loop is the wired connection from a telephone company's central office in a locality to its customers' telephones at homes and businesses. Local loop unbundling (LLU) is the regulatory process of allowing multiple telecommunications operators to use connections from the telephone exchange to the customer's premises (the local loop).

MNO – *Mobile Network Operator*

A telecoms service provider organisation that provides wireless voice and data communication for its subscribed mobile users. They are independent communication service providers that own the complete telecoms infrastructure for hosting and managing mobile communications between the subscribed mobile users with users in the same and external wireless and wired telecoms networks.

MVNO – *Mobile Virtual Network Operator*

A mobile operator that does not own spectrum or have its own network infrastructure. An MVNO has business arrangements with traditional mobile operators to buy network time, which it then sells to its own customers.

PKI – *Public Key Infrastructure*

A PKI (public key infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.

OSP – *Online Service Provider*

A firm that provides services through the Internet.

OTT – *Over The Top*

The delivery of content or services over an infrastructure that is not under the administrative control of the content or service provider.

OVD – *Online Video Distributor*

A firm that distributes video content through the Internet.

SaaS – *Software-as-a-Service*

A software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.

STB – *Set-top box*

A device that enables a television set to become a user interface to the Internet and also enables a television set to receive and decode digital television (DTV) broadcasts.

Transit

The connection to and use of a telecommunication path provided by a vendor.

VoIP – *Voice over IP*

An IP telephony term for a set of facilities used to manage the delivery of voice information over the Internet. VoIP involves sending voice information in digital form in discrete packets rather than by using the traditional circuit-committed protocols of the public-switched telephone network.

VPN – *Virtual Private Network*

A network that uses a public telecoms infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network.

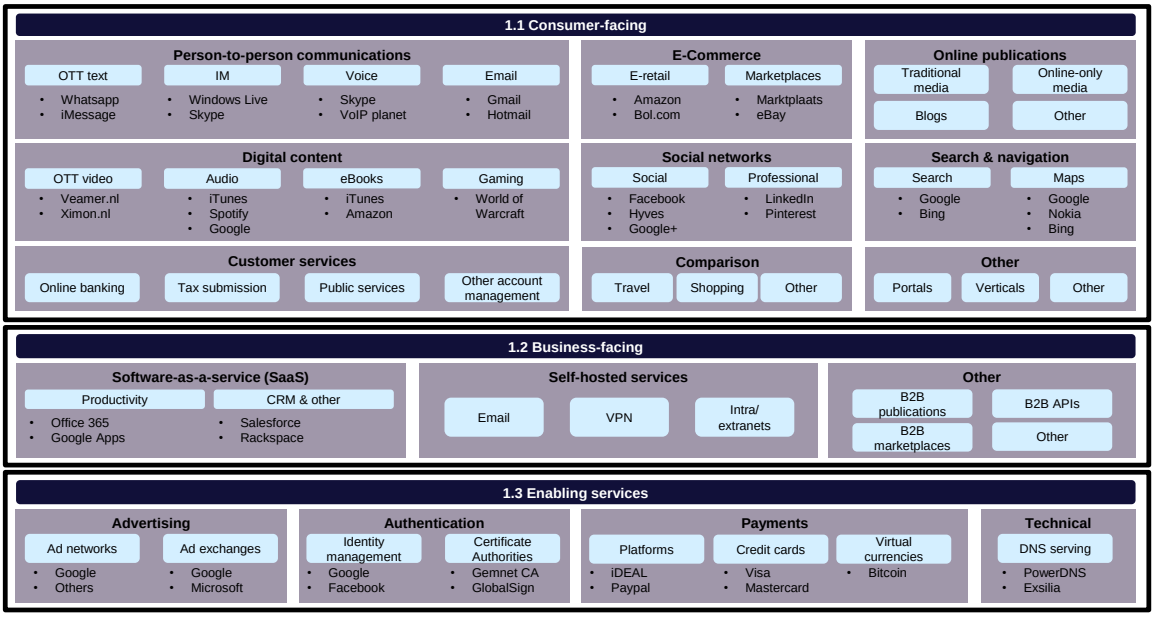
Annex B Detailed Internet value chain

In this annex, we provide a sector-by-sector detailed look at the value chain described in Section 3 of this report. This is a purely visual annex without commentary; readers should rely on the numbering scheme in Figure B.1 as a guide to the rest of the annex.

Figure B.1: High-level view of the Internet value chain [Source: Analysys Mason, 2013]

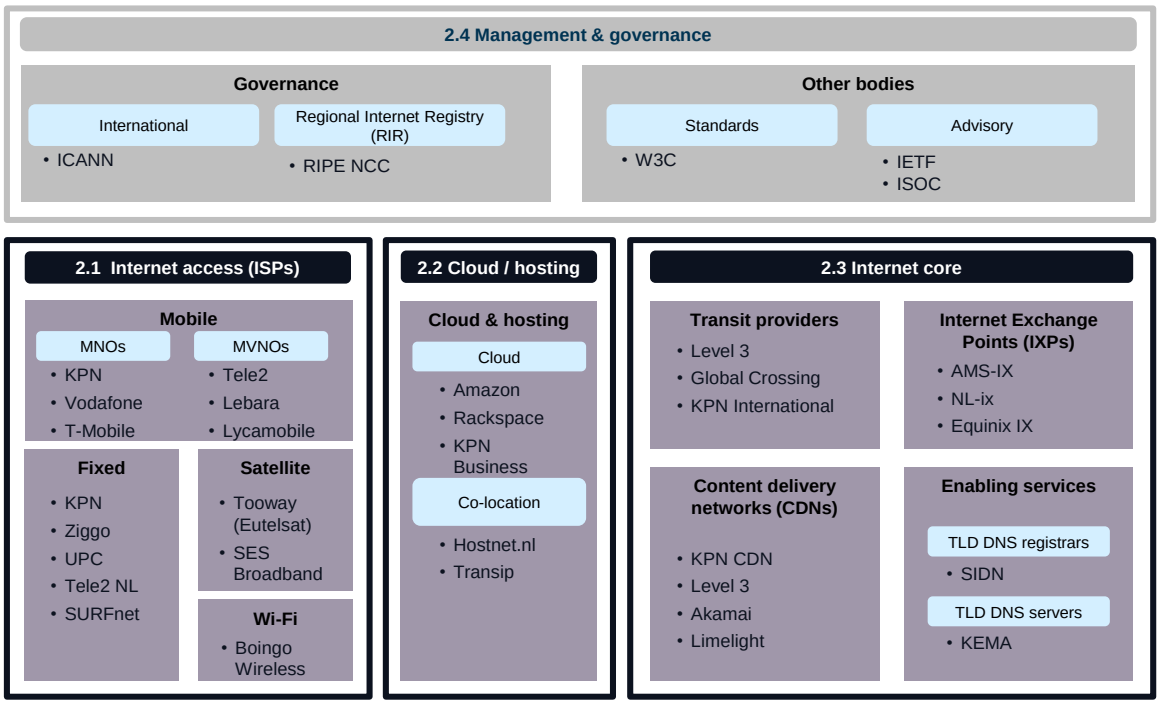
B.1 Online services

Figure B.2: Detailed view of the online services sector [Source: Analysys Mason, 2013]



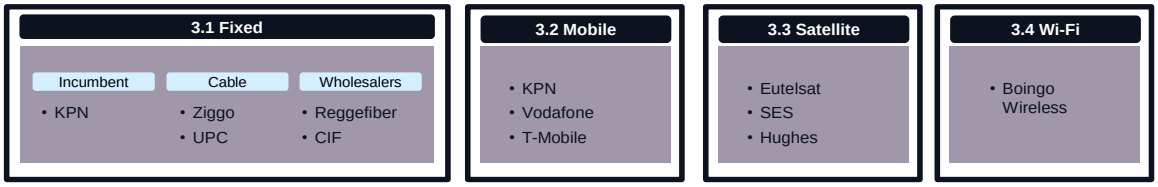
B.2 Internet connectivity

Figure B.3: Detailed view of Internet connectivity sector [Source: Analysys Mason, 2013]



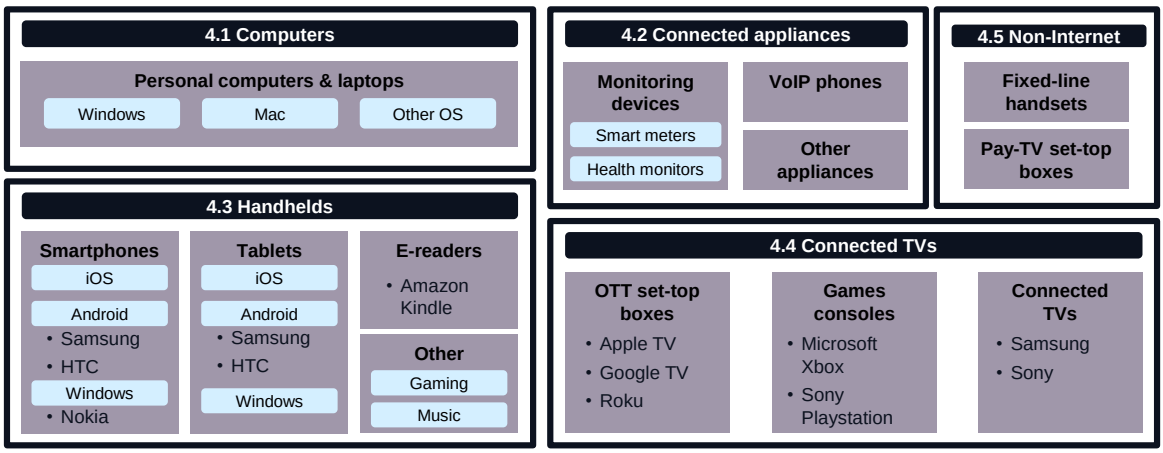
B.3 Access

Figure B.4: Detailed view of access network sector [Source: Analysys Mason, 2013]



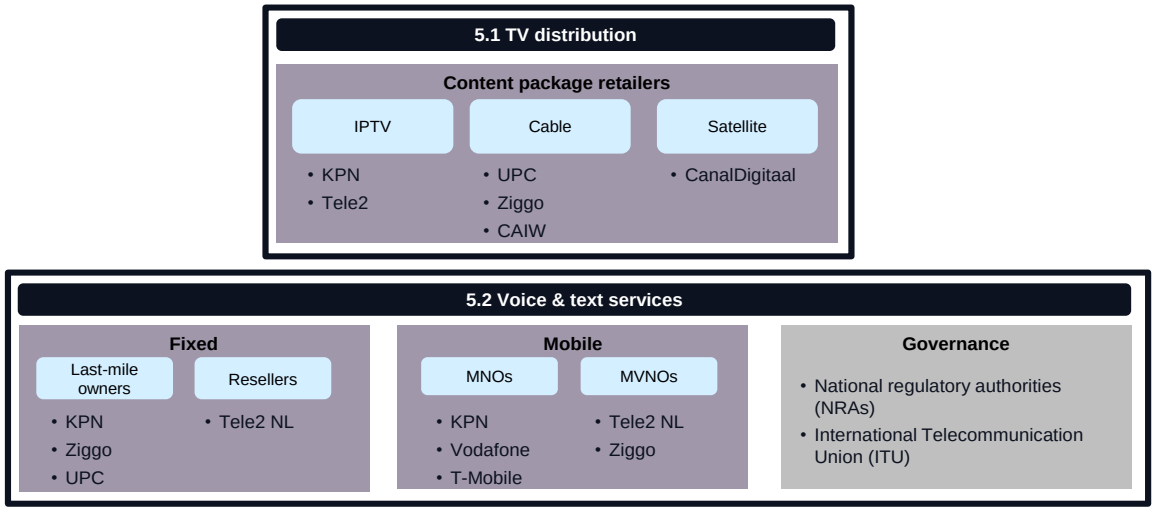
B.4 Devices

Figure B.5: Detailed view of the devices sector [Source: Analysys Mason, 2013]



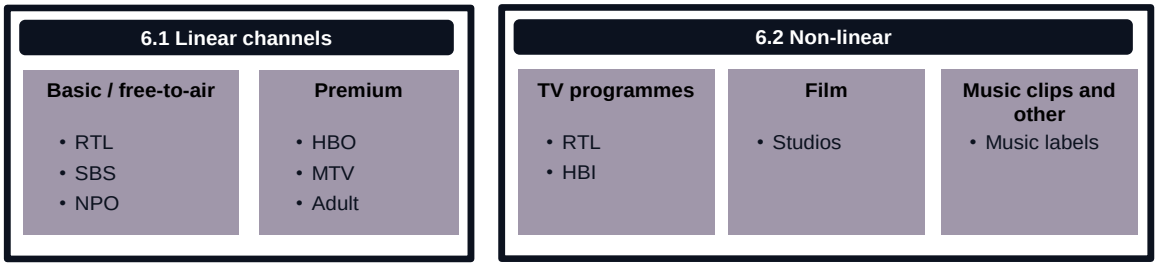
B.5 Traditional telecoms services

Figure B.6: Detailed view of the traditional telecoms sector [Source: Analysys Mason, 2013]



B.6 TV content

Figure B.7: Detailed view of the TV content sector [Source: Analysys Mason, 2013]



Annex C Sector-by-sector risk analysis

In this annex, we apply our thinking from Section 4.3, as well as our knowledge of known cases of market under-provision, to the task of identifying value chain sectors meriting further study.

This analysis was used for prioritising areas for our case studies in Section 5, where our economic framework in Figure 4.7 is applied systematically. At this stage, our analysis was only preliminary and of a high level.

Throughout this annex, asterisks denote cases of potential interest given their combination of potential harm, likelihood of under-provision and current policy position.

C.1 Availability

1. Risk	2. Potential harm	3. Likelihood of under-provision	Current policy
* Unavailability of specific **B2C online services** can disrupt personal / social life	Varied: High in cases where switching is not straightforward and services play a key role in consumers' lives	Medium/low (occasional)	Limited/no explicit regulations
* Unavailability of **B2B online services** (1.2) can disrupt the economy	High	Medium/low (occasionally observed)	As above
* Unavailability of online **enabling services**	High/ systemic	Rare	Only non-sector specific: For example, continuity-related obligations apply to providers of digital signatures, whether online or not
* Outages in **access networks or ISPs**	High	Low/rare, e.g. Vodafone fire	Recent "duty of care" legislation for voice providers; EU PATS obligations
* Failure of **cloud** hosting services (2.1) can disrupt hundreds of online businesses	Moderate/ high	Medium (occasional)	No known explicit regulations
Internet transit or CDN providers may became unavailable	**Low: Customers can mitigate risks by "multi-homing" or switching providers in real time**	**Moderate**	**No known explicit regulations**
Unavailability of a large Internet Exchange Point (**IXP**) can significantly affect the functioning of the Internet	Moderate	Low: Mainly related to security concerns or major incidents	No known explicit regulations

1. Risk	2. Potential harm	3. Likelihood of under-provision	Current policy
National-level **enabling services** (2.4) could become unavailable	High	Low	Managed under a letter of understanding with the Ministry of Economic Affairs

C.2 Openness

1. Risk	2. Potential harm	3. Likelihood of under-provision	Current policy
***Social networks** / **online comms** may fail to interconnect	Moderate/low	Already the norm	No explicit regulations
Online search and navigation players may discriminate	Moderate	Unclear	Under EC investigation
***Digital content platforms** can discrim-inate in terms of which apps/content to offer	Moderate/low	Moderate	No explicit regulations. Consumer protection applies
ISPs could discriminate between online services	High	Potentially high	Direct legislation
Internet transit providers could fail to interconnect, leading to blackouts	Significant	None: ISPs would be likely to immediately and automatically address a transit provider's failure by routeing traffic to other providers	No explicit regulations: Any obligation to interconnect would fundamentally alter transit providers' business models
*Connected **devices** vertically integrated with online services can limit choice	Moderate/low	Moderate	No explicit regulations

C.3 Privacy

1. Risk	2. Potential harm	3. Likelihood of under-provision	Current policy
B2C online services may collect unauthorised consumer data	Moderate	High	• Cookie Law[75] • CBP[76] • Right-to-be-forgotten (RTF)[77]
***Online communication services** (e.g. email), **social networks and search** can exploit sensitive personal data beyond agreed contexts	High	High	• CBP • RTF
Advertising and authentication providers (1.3) can track users across sites	Moderate/ low	High (common)	• Cookie law • CBP • RTF
Connected **devices** (energy meters, mobile phones) can track and upload some details of users' private lives without their' knowledge	Moderate/ low	High (common in anonymous form e.g. for traffic)	• CBP • Mandatory smart meter policy dropped
ISPs can monitor consumers' actions across the Internet using deep packet inspection (DPI)	High	High	• CBP • Restrictions on DPI use[78] • Data retention laws for law enforcement[79]

75 New Dutch cookie law forces websites to ask users for specific permission before recording their data, or providing this data to third parties. Websites are required to prove that consumers have consented to the tracking of their activities.

76 The use of personal data is supervised by the Dutch Data Protection Authority (CBP) in compliance with the Dutch Data Protection Act (case in point: Google was fined for violation of the Act).

77 The European Parliament is currently discussing new regulations on privacy, including right to be forgotten. Under consultation.

78 Recent net neutrality law allows DPI only with consumers' permission or as part of law enforcement.

79 Data retention laws for law enforcement only allow providers to keep information for a maximum of 6 months (for Internet) and 12 months (for voice).

C.4 Security

1. Risk	2. Potential harm	3. Likelihood of under-provision	Current policy
Users' **online** accounts may be hacked	Moderate/ high	Varied: Likelihood of risk materialising without appropriate public intervention	Being proposed
*If a user's account with **authentication services** is hacked, attackers can impersonate the user in a range of services	High	Varied	For regulated qualified certificate providers (not specific to online), ch 18 Tw
Advertising networks may be hacked and used to distribute malware	High	Moderate (has happened)	No sector-specific regulation
Digital content stores (e.g. app stores) may carry malware	High	Limited to small, rogue players	Limited/none
End-user **devices** can be attacked by spyware or other types of malware designed to extract confidential information	High	Moderate: Certain providers differentiate themselves through their strong security (e.g. Google two-step login)	Limited, but art 11.7a (cookies consent) applies