

## **White Paper**

# **The Evolution of Policy Management: From QOS to QOE**

Prepared by

Graham Finnie  
Chief Analyst, *Heavy Reading*



[www.heavyreading.com](http://www.heavyreading.com)

On behalf of



[www.bridgewater.com](http://www.bridgewater.com)

*October 2007*

## TABLE OF CONTENTS

<b>I.</b>	<b>TELCO CHALLENGES &amp; EXPECTATIONS.....</b>	<b>3</b>
<b>II.</b>	<b>WHAT IS POLICY?.....</b>	<b>7</b>
2.1	Policy in Practice: Emerging Models .....	9
2.2	Policy in Practice: Real-Life Case Studies .....	11
	<i>Managing "Excessive" Bandwidth Use.....</i>	<i>11</i>
	<i>Creating More Personalized &amp; Differentiated Service Offers .....</i>	<i>11</i>
<b>III.</b>	<b>SUMMARY &amp; CONCLUSIONS.....</b>	<b>12</b>
	<b>ABOUT BRIDGEWATER SYSTEMS .....</b>	<b>15</b>

## LIST OF FIGURES\*

### SECTION I

Figure 1.1	Is a Policy Infrastructure Essential? .....	3
Figure 1.2	Catalysts to Deployment of Policy Control & Management .....	4

### SECTION II

Figure 2.1	Do You Now, or Will You in Future, Charge for Any of the Following? .....	9
Figure 2.2	Typical Policy Environment Today .....	9
Figure 2.3	Emerging Policy Environment .....	10
Figure 2.4	Evolution of Policy .....	10

### SECTION III

Figure 3.1	Master Plan or Piece by Piece? .....	12
Figure 3.2	Varying Influences on Policy Decisions.....	13
Figure 3.3	Policy-Driven Enhancements to Services.....	14

---

\* All charts and figures in this report are original to *Heavy Reading*.

# I. Telco Challenges & Expectations

Interest in policy management and control has risen rapidly in the past year, driven by the transition to IP networks and IP Multimedia Subsystem (IMS), the deployment of demanding new IP services, and the need for telcos to differentiate themselves from competitors. However, policy management is a broad-ranging concept that includes many definitions, tools, vendors, products and standards. For those planning to deploy policy tools, it is a potentially confusing picture.

The purpose of this White Paper is to bring some clarity to the policy field by relating the key challenges that telcos face in the transition to IP NGNs, to the tools that are now becoming available. The paper identifies the key policy tools – which include, among others, bandwidth and resource management, policy servers, subscriber management, application and content management, and identity management – and explains how they can be used and how they relate to one another.

We conclude that approaches to policy can be roughly divided into "negative" and "positive" approaches. Negative policy is primarily concerned with protecting network resources, and protecting the quality of new services provided by telcos themselves. This approach gives preferential access to these services, and blocks services or traffic seen as harmful. Positive approaches, on the other hand, are designed to refine and personalize customers' experience of broadband services in a way that both reduces churn and increases revenue.

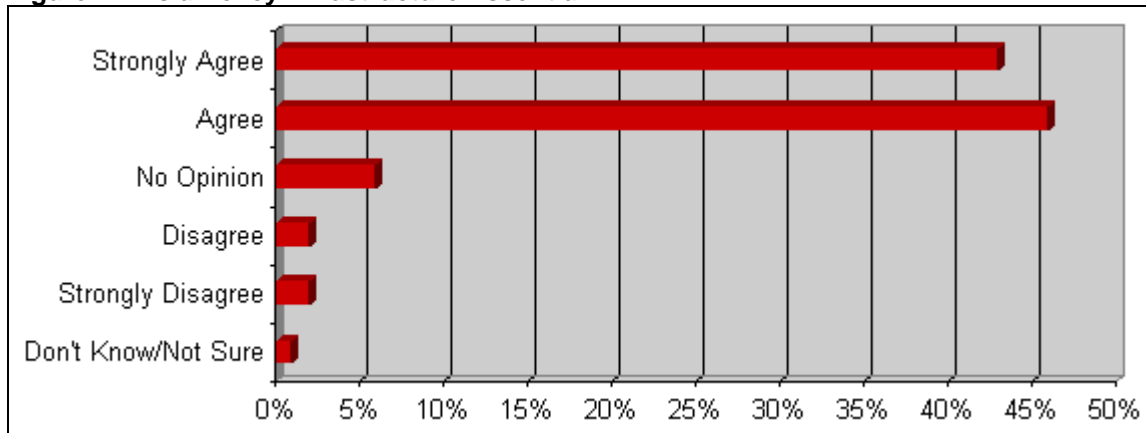
For the time being, most telcos tend to see policy in the first, negative, sense. However, our research with telcos, reported in this paper, suggests there will soon be a move toward a more positive view, in which the primary objective is to use policy tools to broaden and personalize service offerings and increase revenue per broadband line. A more positive view of policy entails integration of quality of service (QOS) and bandwidth tools with policy tools based on subscriber profiling and meeting subscriber needs.

This paper is based in part on a recent *Heavy Reading* survey of service provider attitudes to policy management. The survey, conducted in the first quarter of 2007, drew 100 usable responses from 64 different service providers. The survey base included a broad mix of incumbent telcos, cellular wireless operators, broadband service providers, cable MSOs, enterprise telcos, and others from all regions of the world.

**Figure 1.1**, based on our survey results, shows that the vast majority of telcos – nearly 90 percent – believe that policy management is becoming a "must have" and a key competitive tool, even if many have only the most rudimentary controls in place today.

*Question: Do you agree or disagree with the statement: "Deployment of policy infrastructure is essential to our ability to differentiate service offerings, and thus to our future competitiveness."*

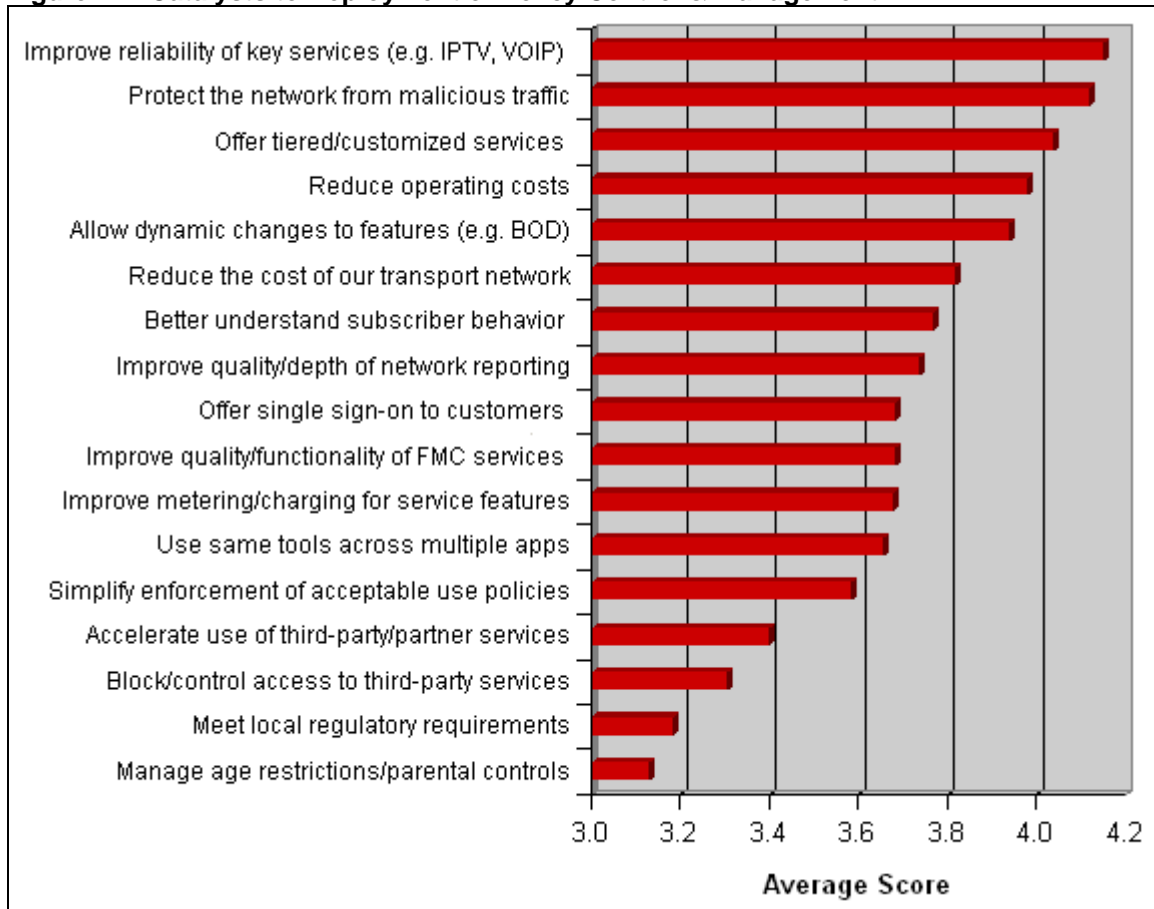
**Figure 1.1: Is a Policy Infrastructure Essential?**



Why has interest risen so quickly? And what kind of policy management do telcos think they need? **Figure 1.2** shows that the catalysts for deploying policy management vary widely – reflecting the broad set of goals that can theoretically be achieved using policy tools – but that guaranteeing QoS for key services is the main motivator today.

*Question: On a scale of 1 to 5, with 5 being "very important" and 1 being "not important at all," please rate the importance of the following catalysts in deploying policy control and management infrastructure in your company.*

**Figure 1.2: Catalysts to Deployment of Policy Control & Management**



The top seven items on this list reflect a diverse range of requirements, including refining subscriber offers, protecting vital new services, and reducing costs. This in itself suggests that there is an underlying need for a broad-ranging policy platform, but that has not necessarily led to a clear understanding of how these priorities translate into telco policy architecture.

In order to understand why this is so, we need to step back for a moment and examine the challenges that telcos currently face. In our view, telcos face two major challenges that could be met in part by deploying policy management tools. Although these challenges are interconnected, they tend to imply different kinds of policy tools.

The first has to do with the transition to an all-IP NGN architecture. While almost all telcos accept that this is now inevitable, it raises some big issues, especially for those with a large base of "legacy" customers. In particular, how do telcos control the reliability and availability of their key revenue-generating services, including telephony and IPTV, if they are all provided on the same network that carries a shifting mix of best-effort Internet traffic and applications?

Most telcos have concluded that simple over-provisioning and "best-effort" IP are not good enough for these services, and that they need tools with an increasingly granular ability to discriminate among different applications and allocate resources to meet the particular needs of those services. By implication, this also discriminates against other kinds of services, including not just services or traffic that is deemed "malicious," but also against many other so-called "over the top" (OTT) Internet services. For these reasons, we have characterized this kind of approach as "negative" – not because it is intrinsically bad, but because it is primarily defensive in nature.

We found in one-to-one interviews with a range of telcos that most tend to the negative (defensive) view of policy. For example, when we asked a strategist with a major North American telco about the main purpose of policy tools, he said: "We need to be a *lot* smarter about how we manage resources, and how we handle applications that are harming the network."

Similarly, a major incumbent cellular wireless telco saw policy almost entirely in terms of allocation of bandwidth to its own key IP applications. "As a general principle," the interviewee said, "real-time services that are part of the telco package and are being charged for need policy between the end points that [we] control."

In other words, a small group of new IP applications provided by telcos themselves are at the heart of much thinking about policy, and nearly all telcos believe the network will need to become more application-aware to handle them.

However, there is a second challenge facing service providers that implies a different kind of approach. This challenge has to do with the increasingly competitive market environment:

- Saturation of the market for basic services, including telephony and basic broadband Internet access
- Commoditization of services, resulting in largely undifferentiated services sold mainly on price
- Entry by OTT Internet and Web-based service providers into a widening range of existing and new telco markets

These pressures have created a crisis of confidence in which the business case for investment in next-generation IP and broadband infrastructure is increasingly difficult to make, raising some fundamental strategic questions. What is the role of telcos in the value chain? What are their unique strengths? Which services should they supply to end users in their own right, and which should they handle through third-party relationships? Most of all, how can they turn all the new broadband pipework they are deploying in both wired and wireless networks into real revenues and lasting customer relationships?

In these areas, we believe, policy may have a more positive role to play. To combat revenue saturation and decline, telcos can use policy to refine service packages and options in order to improve the customer's overall quality of experience (QOE). Looked at from this point of view, policy is used not simply to control access to basic network resources, but to build and deliver personalized service packages, attributes, and features on the basis of policy decisions that are ultimately determined by the subscribers themselves. These attributes may include enrichment of services with location or presence information; the ability to use services across different networks with the same login and dashboard; or personalized upselling and subscriber offers based on the subscriber's own behavior and profile.

Just as importantly, a QOE-based approach to policy can be used to build more positive relationships with third-party Internet and Web-based service providers – and that fits well with a growing tendency among telcos to see themselves not just as *providers* of services, but also as *enablers* of services. Telcos increasingly recognize that they can't possibly provide all revenue-generating services themselves, and that they must develop stronger commercial relationships with the third

parties that build and provide new applications and services. In this way, they can offer customers a broader portfolio that includes both their own and third-party services – again improving QOE.

Hence the Scandinavian incumbent telco TeliaSonera argued in a recent presentation that telcos must evolve from "network service providers" to "connection enablers" – a view that necessarily entails use of new policy tools that allow relationships with third parties to be automated and managed across quality, service, billing, and other parameters.

In this way, telcos can use policy tools to provide a much wider range of options to customers and third parties. They can offer not only access to new services, but also different ways to consume and connect to those services; and not just their own services, but also those of third parties that can tap into policy tools to request specific kinds of enablers. This approach is likely to become much more important over the next few years. Indeed, we believe that application of policy in third-party situations will be not just an optional extra, but an essential capability.

However, our recent survey and our interviews with telcos suggest that it is not wholly understood that policy tools can help in these areas. One telco strategist acknowledged that techniques such as application and content management would become much more important as the company's content-based products went mainstream, and as the company sought to work more effectively with third-party content providers. There would be a need, he suggested, to expose policy features to those third parties, in part to avoid creation of yet another technology silo. Yet he said, "We don't necessarily see this in the policy arena at present. We are aware of [it], but haven't yet done much to address it."

Indeed, many telcos told us they did not really see concepts such as "identity management" and "applications management" as aspects of policy management – primarily because they still see policy in its negative aspect, as a mechanism for managing bandwidth and allocating resources.

However, the rapid – and accelerating – changes in end-user demand and in the way broadband connections are actually used suggests that, at an architectural or philosophical level, maximum flexibility and breadth in policy tools will be very important. At the same time, there is a need for as much automation as possible once the rules are set, so that operating expenses do not run out of control. Finally, it implies that the circle that connects static subscriber profiling and dynamic resource or bandwidth management is completed. Policy must be applicable to multiple subscriber circumstances. But how, and where?

## II. What Is Policy?

As our initial discussion of policy has made clear, conceptions of policy can differ widely. In order to clarify the situation, this section discusses in more detail what policy is, and how it has evolved.

Policy in telecom networks has evolved gradually over the past five to ten years as a result of the emergence of fast-changing multiservice networks based on IP and broadband access. Traffic patterns in these networks are increasingly unpredictable, and service providers have only partial control over the applications running on the network. Hence most early policy tools were created to control or partition access to resources, especially broadband network resources.

Traditionally, this entailed the use of traditional class-of-service (COS) techniques, available and deployed in networks based on MPLS for a decade or so, primarily to meet the needs of valuable enterprise customers. With only three or four statically defined classes, COS is limited and somewhat inflexible, but nevertheless a very useful way to ensure that certain applications, such as VOIP, get the treatment they need.

Newer developments have helped to refine resource-oriented policy tools. Deep packet inspection (DPI) is making inroads as a means of inspecting packet streams and identifying applications, and is often used to restrict the bandwidth available, for example, for video or music downloading. More recently, call admission control (CAC) techniques have recreated the ability to admit or deny a bitstream based on its type, mimicking circuit-switched connections. These more stringent admission control techniques may guarantee the quality of specific applications, but generally take little account of individual subscriber value or needs.

Meanwhile, other tools – not necessarily offered under the policy umbrella – have emerged in the subscriber management area. On the mobile side, a good example of a simple but more network-centric (and dynamic) subscriber-oriented rule or policy is implicit in a prepaid mobile service, where the network stops accepting calls when the subscriber's credit has run out.

Policy tools currently sold by vendors include the following, either as stand-alone products or as features and options in products such as routers:

- Basic QOS and COS software, often implemented in routers
- More sophisticated tools often called bandwidth managers or resource managers, and often including call admission control technology
- Deep packet inspection tools that can identify applications, either as stand-alone tools or built into other equipment
- Policy servers, increasingly based on standardized concepts that include policy decision points (PDPs) and policy enforcement points (PEPs), and on standards developed by 3GPP (IMS) and ETSI (Tispan) among others
- Subscriber and profile management tools, including authentication, authorization and accounting (AAA) functions
- Identity management, including concepts such as federated identity and management of identity across different types of networks and across different subscriber "roles"
- Content management, including filtering of content by subscriber entitlements, subscription, or via options such as parental control
- Applications management, including for example third-party access to subscriber information, and providing integrated access to user profile information

This list is not exhaustive, but it gives a sense of how varied conceptions of policy are, as well as the difficulties that telcos face in deciding what to deploy.

In order to understand the emerging possibilities here, it is necessary to take a step back from the details and define policy at a high level. From the perspective of this paper, "policy" is nothing more than a set of formally constituted business rules that trigger specific responses to specific formulated requests and conditions.

These policies follow simple logical rules to create complex services. For example: If customer A subscribes to the Tier 3 package, and if it is the weekend, then customer A may download an unlimited number of music videos. This list can be extended by simply adding conditions – for example, information on the age of the customer, or on how much he has previously downloaded. And dynamic information (e.g. where the customer is, or network conditions at the time) can be added to the rules invoked in a particular case.

Policy can be applied manually or automatically – with many shades in between – but a key objective is to automate policy as far as possible, in order to reduce operational expenditure and increase organizational flexibility, agility, and service velocity. This also enables the creation of new services, possibly multiple services, from a single application (e.g. event-based services).

In other words, telco policy management automates (in the context of a digital network) business concepts that have been used in large organizations for many years to simplify and accelerate decision-making.

This definition has two important implications:

- It makes it clear that policy is concerned not merely with technical fixes for network problems, but with business decision-making. Companies can make business decisions (e.g. "We must provide the following range of capabilities to our partners"), and then use policy management to automate the way this happens.
- Relatedly, there is no obvious reason to restrict policy to QOS and adjacent concepts: So long as policy architectures are sufficiently abstracted and flexible enough to define rules in a broad (perhaps indefinitely broad) range of situations, they can be used to help solve a broad (perhaps indefinitely broad) range of business challenges. Yet many telcos do restrict their view of policy to only a subset of techno-centric business issues.

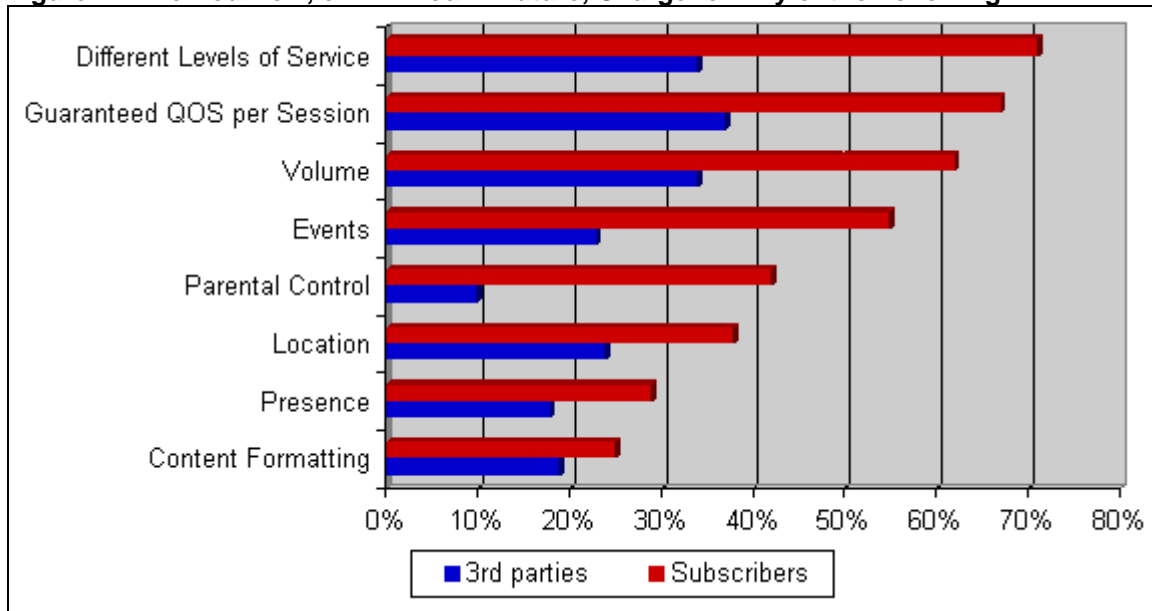
This gap in understanding may be based in part on the belief that dynamic resource decisions based on second-by-second network monitoring cannot be connected in real time to business-centric subscriber profile information. Subscriber profiles are often seen as static, off-line entities: Profile information can be rapidly called up (say, from an HSS) but cannot be dependent on the state of the network at any one time.

But where state information *is* available and usable by the policy engine, then the two can be closely coupled when making policy decisions. State information can include information on the subscriber's current IP address, the type of terminal in use, the user's current location, and the applications in use. In other words, an integrated approach to policy likely requires an ability to detect and use state information. This kind of dynamic interchange is likely to be particularly useful where third-party service providers are involved.

As **Figure 2.1** shows, the ability to charge not only subscribers themselves, but also third parties, may be an important catalyst for more sophisticated policy-based subscription management. The graphic shows that the desire to charge by quality – either for different levels of service (such as the "gold/silver/bronze" schemes familiar in enterprise services) or on a per-session basis – dominates. And a fair percentage of respondents intend to charge third-party service providers as well as end users in the same way – a practice that is not widespread at present.

Well over half of the respondents expected to charge (or already charge) for events – a desire that again implies better subscription management, and shades into content management.

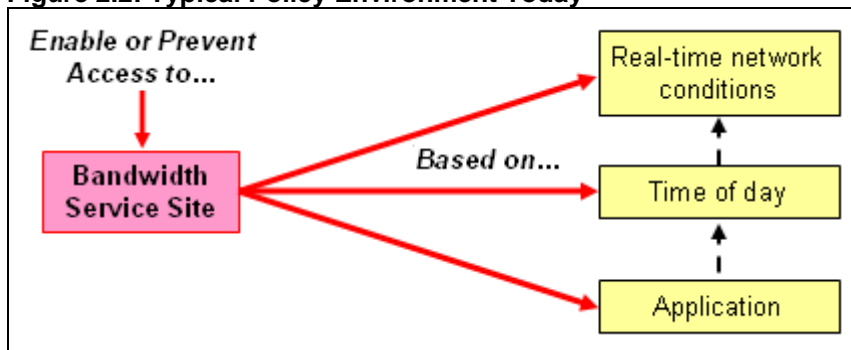
**Figure 2.1: Do You Now, or Will You in Future, Charge for Any of the Following?**



## 2.1 Policy in Practice: Emerging Models

What does this mean in practice? **Figure 2.2** presents a highly simplified view of a typical QOS-centric policy environment today, without showing the actual flow of information.

**Figure 2.2: Typical Policy Environment Today**



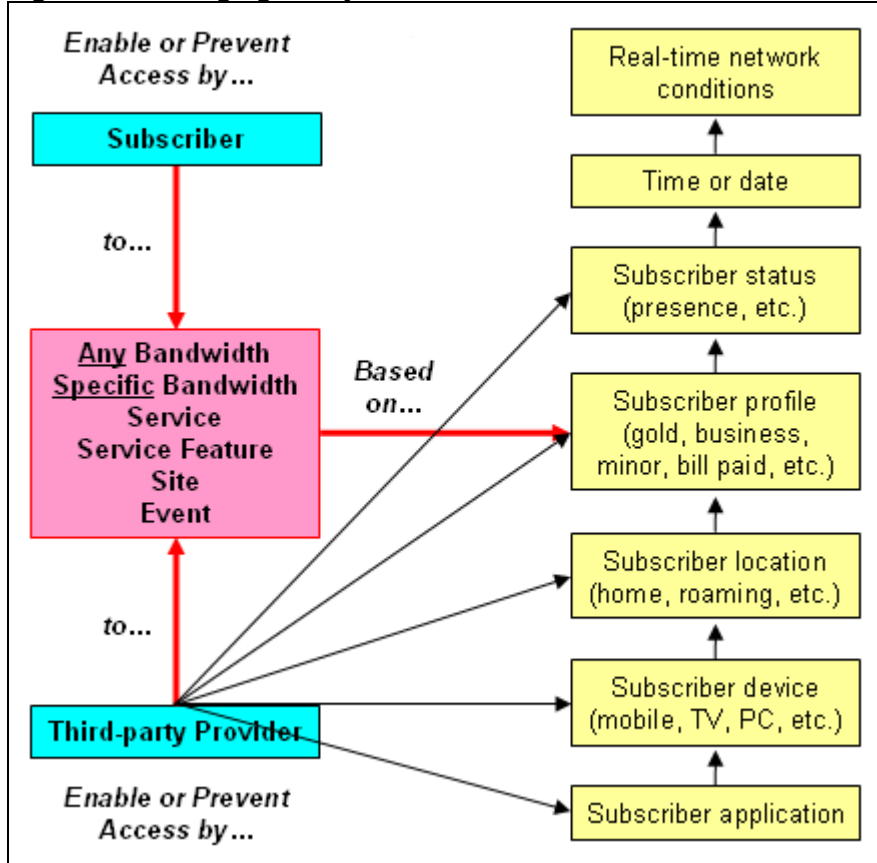
**Figure 2.3** looks at how this environment is evolving to handle a more complex set of requirements in a more integrated and connected way. As the figure implies, new policy approaches are particularly important if telcos are to develop a more positive relationship with third-party Internet providers. For example, most mainstream telcos are providing IPTV and VOD directly to customers, often as part of a triple-play service package; but their own customers are also increasingly viewing video that comes via OTT sites such as YouTube. What should telcos do about it?

In a recent survey, we found that most telcos do recognize that they need to react to these threatening new developments. But what should they do? In recent research on the topic, we identified four possible responses:

1. Block access to OTT video services
2. Charge for higher-quality content delivery
3. Open their own IPTV platform to OTT content
4. Use OTT to expand their own video service footprint

Clearly the first, most defensive response is closely related to the negative conception of policy we outlined earlier. More positive conceptions – especially options 2 and 3 – imply different kinds of policy tools, which will probably include bandwidth and resource management, but also likely subscriber and profile management, identity management, and other kinds of tools. And using policy rules, telcos can ensure that third-party content providers only have access to the specific pieces of information (for example, about the subscriber's current location or current device) that are required to successfully provide the service. Similarly, third parties themselves can protect their networks from indifferent quality by using the telco's policy engine to check the subscriber's status before allowing access to a particular service.

**Figure 2.3: Emerging Policy Environment**



Although a range of policy tools has evolved separately, they are now increasingly being integrated into an overall proposition, or policy architecture, that can handle many or most of the tasks described in this section. The key to understanding this change is the replacement of QoS by QOE. While the former tends to be defined in terms of making bandwidth and resources available for particular applications, the latter is defined from the point of view of the subscriber, and is seen as a means to make services more valuable to customers, as **Figure 2.4** illustrates.

**Figure 2.4: Evolution of Policy**

OLD MODEL	NEW MODEL
Policy oriented to quality of service	Policy oriented to quality of experience
Policy applied per application	Policy applied per subscriber
Policy driven by network/engineering issues	Policy driven by business/marketing issues

## 2.2 Policy in Practice: Real-Life Case Studies

### ***Managing "Excessive" Bandwidth Use***

This is an example of the use of a "negative" policy tool to control subscriber access to bandwidth. This North American Tier 2 service provider was experiencing problems with a small number of customers that were using a high proportion of its core bandwidth, typically for peer-to-peer file sharing. Bandwidth usage had been growing more quickly than previously, forcing the service provider to either spend more on bandwidth to meet the needs of only a few users, or run a highly congested network. Furthermore, the service provider had begun heavily marketing its triple-play service package, and needed to protect the quality of that service.

Its chosen solution – a deep packet inspection engine with policy features – is being used to identify the applications running to individual users; where use is considered "excessive" or the network is highly congested, bandwidth allocated to particular applications, such as peer-to-peer video downloading applications, is throttled back.

The objective here was to enable the service provider to control its own bandwidth costs while avoiding congestion affecting all customers. This has the obvious danger that some customers will choose to leave, but it has the benefit that the overall QOS for customers is improved. It also means that the service provider can ensure that its own services – in particular VOIP, as part of a triple-play package – are getting enough bandwidth to run effectively.

This is a typical example of how many telcos envisage policy tools today: as a means to control what is seen as harmful traffic and applications, and to protect the quality of their own services without spending excessively on bandwidth.

### ***Creating More Personalized & Differentiated Service Offers***

Our second example is a Tier 1 wireless telco that used policy in its "positive" role to simplify the provisioning of a large number of new added-value mobile services and features – creating a more personalized and "stickier" service bundle, as well as new revenue opportunities.

The telco's objective in this case was to create a family of value-added mobile services that included in particular mobile video and audio streaming. The challenge in this case was to add services and features without adding excessively to cost.

Among other things, there was a need to interface with multiple third-party application providers and their databases. This is typically one of the biggest challenges when providing a range of paid-for and properly-monitored services. Each is likely to have its own disparate database information, which includes a user's own "database" (e.g. of favorite Web pages), data on device type and similar information, and data on billing or authorization to access specific features and applications. In order to provide a usable and attractive service, there will be a need to aggregate data from these various sources for every new service launch, or even simply to add new features.

The main consequence of this complexity: Each service launch entails costly development work, and may take months, meaning that the cost may outweigh the benefits of the service. Moreover, in the fast-moving world of video and audio streaming, the opportunity may simply be missed altogether in the time it takes to develop the application.

Using a centralized application authorization solution, this telco was able to resolve many of these challenges, adding 20 applications to its network in only a month. A key benefit of this solution was that it provided a single platform that could handle any subscriber request for authorization, in effect replacing interrogation of individual database "silos." Moreover, since the application policy platform is rules-based, it can and may be used to easily add other services (not just media services) in the future.

### III. Summary & Conclusions

For telcos and service providers, the challenges presented by the transition to all-IP NGNs are formidable. There is widespread recognition that this transition is both unavoidable and desirable, but it involves significant investment right through the technology stack. Telcos have already invested heavily in IP and broadband, but most will need to invest a lot more in the next five to ten years, not least in the access network. Making that investment while protecting the integrity of services *and* maximizing flexibility in service provisioning (and therefore opportunities to increase revenues and customer loyalty) will be no mean feat.

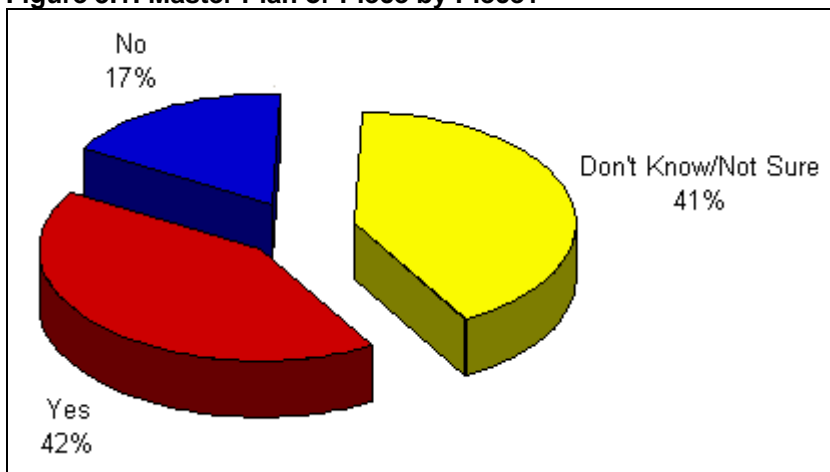
Policy management can help to meet some of these challenges. Policy tools are evolving and becoming more sophisticated, meeting a wider range of needs. However, taking the fullest advantage of the possibilities has a range of implications that telcos need to take into account.

In the first place, telcos need to go beyond mere technology (a.k.a. network engineering) decision-making and recognize the potential of policy in *business* decision-making. This requires a recognition that policy tools themselves can actually meet that wider potential.

This in turn suggests that a more joined-up approach to evaluating policy management tools is desirable. As **Figure 3.1**, again taken from our survey, shows, many companies expect to buy resource/bandwidth tools and subscriber/profile tools separately today, for a range of reasons, and many are unsure how to proceed.

*Question: Does your company currently purchase or plan to purchase resource/bandwidth management tools and subscriber/profile tools separately?*

**Figure 3.1: Master Plan or Piece by Piece?**

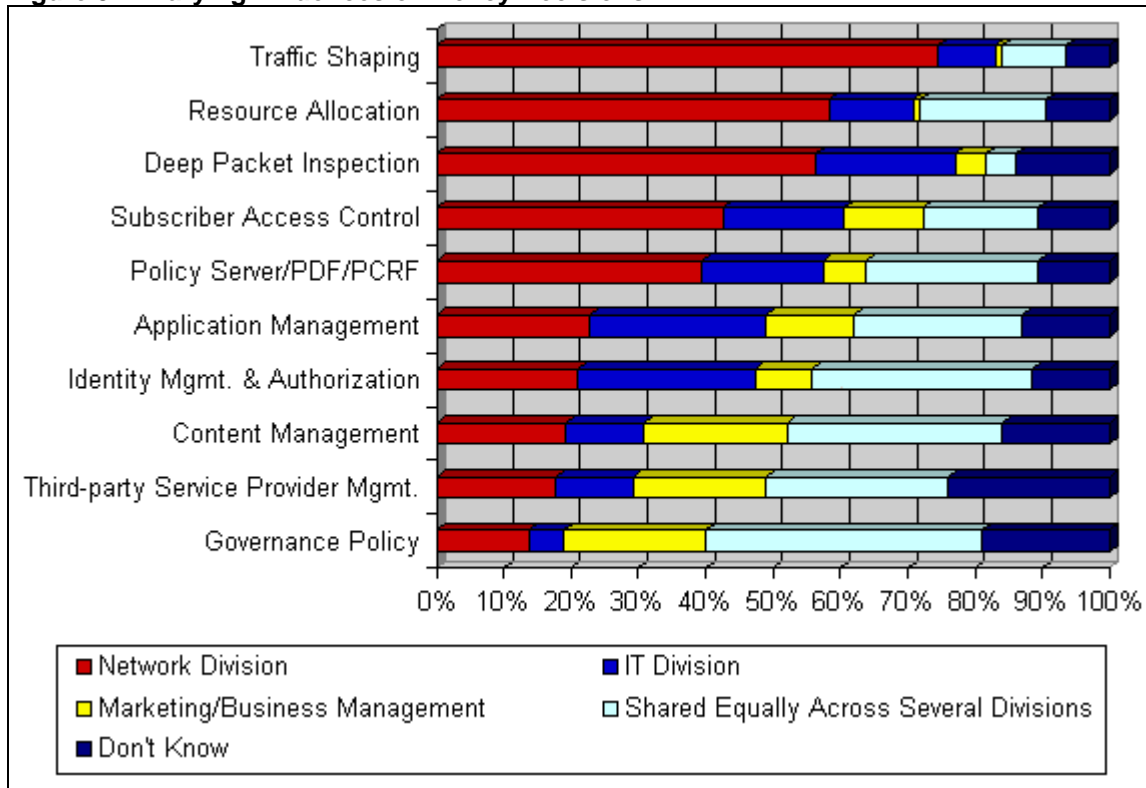


In our view, this confusion calls for an internal effort to ensure that *all* of the telco's key internal groups and divisions are involved in making decisions on how to deploy and use policy management tools. A more rounded view of policy is likely to involve a range of different departments, and there is a need to ensure that all points of view are being reflected in business-case development for policy.

As **Figure 3.2** shows, the degree to which different departments are expected to be involved will increase rapidly as telcos move beyond resource- and bandwidth-centric views of policy and toward a view that emphasizes service creation and service personalization.

*Question: For each of the policy aspects identified below, which part of your organization has (or will have) primary responsibility for defining strategy?*

**Figure 3.2: Varying Influences on Policy Decisions**



Similarly, in order to take maximum advantage of the flexibility of new policy tools, telcos will need to evangelize their benefits both internally and to third parties – especially Internet-based and Web-based companies – that could benefit from the application of telco policy enablers to their services. This obviously requires that telcos stop seeing those third parties as parasitic threats that simply pour additional traffic into the network, and begin to see them instead as sources of new subscriber value – and subscriber revenue.

A final task is to ensure that the standards developed for policy management fully reflect and meet the challenges that telcos face today. Most telcos still see policy standards in terms of the elements developed for IMS and Tispan networks by 3GPP and ETSI – that is, the Policy Decision Function (PDF), the Policy and Charging Rules Function (PCRF), and so on. These are valuable, and they have improved over time: The evolution of the PDF into the PCRF, for instance, allows telcos to build the value of a service into the decision on whether or not to allocate resources to it, while the evolution of the Home Location Register (HLR) into the Home Subscriber Server (HSS) – and the associated development of the Network Attachment Subsystem (NASS) by Tispan – has significantly enriched subscriber profiling.

Separately – often in a different department – telcos may be building policy initiatives using models developed, for example, via the TeleManagement Forum's Next Generation Operational Support Systems (NGOSS) initiative. But there is a clear need to encourage integration of these various efforts into a single policy architecture in time, and telcos must make their needs clear.

Next-generation integrated policy management will likely be an important means for telcos to refresh and renew their market propositions, and to build more constructive relationships with third parties. **Figure 3.3** sets out some possible use cases. With the Web and the Internet continuing to outstrip the traditional telco community in the generation of new ideas, services, and revenues, the onus is now on the telcos to rapidly turn policy theory into reality.

**Figure 3.3: Policy-Driven Enhancements to Services**

EVENT/REQUIREMENT	POLICY SOLUTION
Deployment of new service, such as higher-speed access	Provide "try and buy" access to particular subscribers who meet profile requirements
Unanticipated network congestion	Intelligent downgrading of bandwidth based on subscriber profile or the needs of particular applications, or offer temporary premium access option
Proposed launch of third-party location-based services	Offer real-time, state-based information on subscriber location and federated identity, while blocking access to other types of subscriber information
Provisioning video services across all types of fixed and mobile access network	Offer state-based information on subscriber terminal and type of access network to enable automatic adaptation to circumstances
Simplify service creation or improvement	Automating policy-checking aspects in service creation by applying policy to third-party providers
Enable differential control of access to own and third-party content based on subscriber ID	Implementation of sophisticated federated identity that enables e.g. a parent to control their child's access to content in any circumstances
Develop better understanding of subscriber behavior	Use policy tools to analyze subscriber activity; use that data to create special offers, more appropriate pricing, etc.
Fraud and identity theft	Use single sign-on facility to reduce fraud across both the telco's own and third-party services and networks

# About Bridgewater Systems

## **SUBSCRIBER-CENTRIC POLICY MANAGEMENT**

Bridgewater Systems' subscriber-centric policy management solutions enable service providers to create a unified view of subscribers across networks and applications. By placing subscriber and policy information as close as possible to subscriber access points, Bridgewater solutions deliver a more efficient and higher standard for network control and service delivery. Because our solutions are built from the ground up to be scalable and meet the most demanding performance needs, your network can comfortably scale to meet subscriber demands and business growth.

## **HOW IT WORKS**

Our subscriber-centric solutions create an intelligent subscriber-centric policy decision point that controls subscriber access to networks, resources, and applications from any device. Our solutions pull key information about the subscriber – static profile information related to entitlements, dynamic real-time state information, and subscriber history (both static and dynamic) – to build a unified view of the subscriber in real time.

As a result, service providers can create highly flexible policies tightly aligned to business needs and subscriber entitlements. This ability ensures a positive subscriber experience that improves retention, and drives up average revenue per user (ARPU) by personalizing the subscriber experience based on level of access, QOS, and context for applications.

## **BUSINESS VALUE**

- Improve subscriber experience:
  - Personalize the subscriber experience according to network capabilities, service tier, and access technology (e.g., mobile phone subscribers don't receive offers for high-definition streaming video).
  - Offer subscribers more options by responding to network changes more easily (e.g., offer increased level of service when extra network capacity is available).
  - Meet subscriber requests and demands quickly, because the network is more variable, flexible, and adaptable.
  - Extend subscribers' control over their experience with self-care options that reduce customer care and improve retention and service uptake.
- Generate revenue opportunities:
  - Be first to market with new applications and services.
  - Significantly reduce revenue leakage from applications and network access.
  - Easily create a range of service bundles for different market segments.
  - Monitor usage to ensure "fair use" (i.e., subscribers pay for the quantity/level of network resources they use).
- Reduce operating and capital expenses:
  - Optimize networks to direct network resources to areas with greatest revenue opportunity.
  - Run networks with a smaller computing footprint, less CPU, and less storage.
  - Reduce administrative errors with logically centralized essential functions.
  - Reduce operational costs with subscriber self-care, centralized management, and flow-through provisioning.
  - Support multiple networks with a single infrastructure and avoid re-provisioning of subscribers by leveraging a common platform over multiple networks.

## **MODULAR PORTFOLIO, CARRIER-GRADE PRODUCTS**

Because of where our products are located in the network, Bridgewater technology enables a single view of subscribers and subscriber groups across all networks and services. Access-technology agnostic and vendor-neutral, our modular portfolio is proven to interoperate with a broad range of network elements, OSS/BSS, and application platforms, offering a significant time-to-market advantage.

Our subscriber-centric policy management portfolio features Network Access Control, Entitlement Control, and Subscriber Management.

- **Network Access Control**

Products enable service providers to deploy centralized authentication, authorization, and accounting (AAA), dynamic host configuration protocol (DHCP), and IP address management across multiple access technologies.

- Control access to advanced services across all access networks quickly and profitably with our high-performance multi-protocol solution.
- Protect network resources and minimize revenue leakage by ensuring that subscribers get only the services they are entitled to.
- Effectively manage network resources – access ports, IP addresses, radio spectrum, bandwidth – and operating expenses.
- Support real-time session management to enable mobility, roaming, security, and usage tracking.
- Eliminate the need for custom mediation solutions with prepaid and postpaid charging.

- **Entitlement Control**

Products allow service providers to control and monetize the dynamic entitlement relationship between subscribers, applications, and network resources. Extend centralized application policy control over a broad application ecosystem:

- Generate new revenue streams, differentiate services, and increase ARPU.
- Create flexible targeted services and bundles at pace with subscriber demand.
- Decrease time to market by offering new, differentiated services that are easy to use, access, and monetize.

Enable real-time policy control of network assets:

- Deploy key applications – such as QOS on demand and metering for fair use – to prevent bandwidth abuse and improve the overall subscriber experience.
- Control and manage the subscriber experience in real time for improved retention.
- Maximize network infrastructure investment and control opex through control of network assets such as bandwidth.

- **Subscriber Management**

Products allow for rapid access to the static and dynamic subscriber data required for network access and entitlement control in multi-vendor network environments.

- Support Radius and Diameter protocols, enabling migration to IMS.
- Easily expand as more services are migrated to IMS.
- High-performance Home Subscriber Server (HSS) based on proven carrier-grade technology.

## WHY BRIDGEWATER SYSTEMS?

- **Carrier-grade solutions:** Deployed in more than 90 service provider networks.
- **Scaleability and performance:** From 5,000 to 69 million+ subscribers. Trusted to handle volumes of 14 billion+ transactions in a single month.
- **Access-technology agnostic solutions:** Easily integrated into multiple networks or a converged network environment.
- **Vendor-neutral:** Proven integration with a wide range of network equipment, application platforms, OSS and BSS systems, and multiple applications, giving service providers a time-to-market advantage.
- **Business enablement:** Enables new, profitable services at pace with demand – dynamic self-care applications, QOS management, service portability, and new business models.
- **Breadth of subscriber-centric portfolio:** Enables new revenue opportunities by controlling and monetizing subscriber access to networks, resources, and applications across any type of network.

## FOR MORE INFORMATION

Visit [www.bridgewater.com](http://www.bridgewater.com)