

# Analyzing Consumerization - Should Enterprise Business Context Determine Session Policy?

Rebecca Copeland  
Core Viewpoint Limited, United Kingdom

Noel Crespi  
Institut Mines-Telecom, Telecom SudParis, Evry, France

**Abstract**—This paper analyzes the impact of the fast-growing BYOD (Bring Your Own Device) trend in the corporate mobile market, which blurs lines between business and personal usage. To enable selective funding and resource optimization for BYOD, we propose that the enterprise determines its own service delivery policy, using an enterprise Business Context (eBC) Policy tool. The enterprise is best placed to ascertain session context and priorities from its internal context sources, kept only by the enterprise, to retain privacy. While NETWORK policies are controlled by network operators, the enterprise could and should determine the SESSION policies that are based on its business goals. The eBC policy can be further utilized for optimizing resource usage and influencing employee consumption. The enterprise goals need to be translated into standard policy rules and conveyed to the carriers via existing 3GPP standards, to fit in with existing networks. This is paper raises several new ideas which are further researched in follow-on papers.

**Keywords**-Consumerization, BYOD, PCRF, Policy, Context, Sponsor, VNO, QoS, DPI, SLA

## I. INTRODUCTION - CONSUMERIZATION PROGRESS

### A. Consumerisation trends

Consumerization is not just about consumers' goods that infiltrate business. It has grown to mean a new paradigm where personal devices are used for work as well as leisure. This is also referred to in the press as BYOD (Bring Your Own Device). This is not just about smart devices, but includes a shift towards web applications. In [2] senior managers reported high levels of use of Facebook (35%), LinkedIn (23%), Twitter (22.9%) and YouTube (14.0%) for work.

Some trends take decades to mature - not BYOD. It has moved fast from a 'toy' to a 'threat' and now to being 'obvious', as stated in [4]. It has already reached maturity, with employees owning only one personal/business device. This is changing the way enterprises deal with employees' communication needs. At first companies stop prohibiting personal devices, then they allow connecting to corporate Internet servers, next they connect personal devices to corporate applications. Finally, companies cease to provide phones and laptops and adopt the 'ultimate BYOD' strategy - no Mobile carrier contract. BYOD is already widespread, according to many reports ([1] [2] [3] [12]). It is often coupled with the move towards Virtual Desk Infrastructure (VDI) and Cloud services, which establish secure centralized storage to assist in service mobility for BYOD devices.

BYOD is now unstoppable. It is also disruptive - in more ways than described by the press. BYOD can be compared to

the PC revolution that eventually liberated employees from the 'tyranny' of the mainframe. In the same way, the scope of what employees are allowed to do with BYOD devices and the risks of such freedom are only beginning to unravel. The evidence from the industry press shows that BYOD is now the 'inevitable future'. Corporate IT departments are already adjusting their budgets and increasing security to accommodate BYOD devices.

### B. The spread of BYOD

The rapid rise of consumerization was raised in the Mobile World Congress 2012, followed by several published studies. In [1], 88% of companies surveyed globally said that employees are using their own devices for work, and 79% are budgeting for it in the next 12 months. As shown in Figure 1, according to a survey conducted in June 2011 in the U.S., Germany and Japan, BYOD is adopted by a wide spectrum of organizations. It is penetrating all sizes of organizations and it covers all types of devices, even traditional mobile phones.

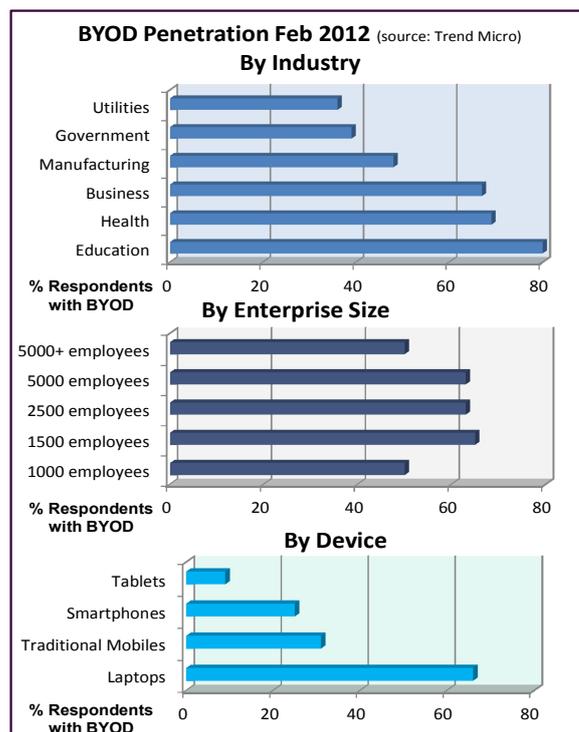


Figure 1: Penetration of BYOD in March 2012

We have identified three categories from the many variations of BYOD strategies: (a) corporate devices providing employees little choice, but allowing personal use; (b) personal devices with partial business Internet and application access; (c) fully supported BYOD devices (funded or not), with full access to enterprise applications. As BYOD matures, strategy (c) is the path that is leading towards the ‘ultimate’ BYOD, in which the enterprise does not provide user equipment but refunds business communication expenses.

### C. Consumerisation benefits for the Enterprise

Corporate managers welcome consumerization (see [1]), citing benefits such as convenience of working from anywhere (58%), willingness to work after hours (42%) and rising productivity (50%). BYOD appeals to the enterprise finance managers, where users pay for their own devices and the internal application farm is replaced by free web services. Figure 2 shows perceived benefits from having a choice of devices, rising productivity, easy access to systems and lower costs (see more in [3]). Figure 3 shows that the rapid adoption is met with general satisfaction. If added together, 75% of BYOD policies are seen as ‘successful’ or ‘somewhat successful’.

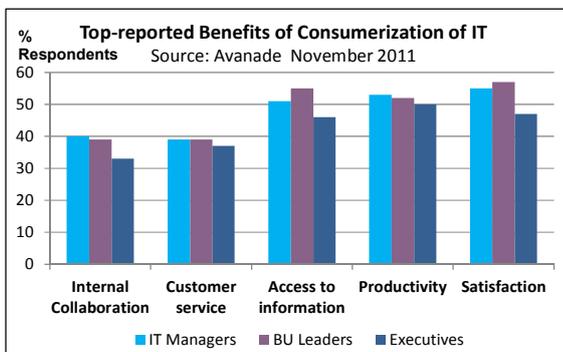


Figure 2: Perceived benefits from BYOD

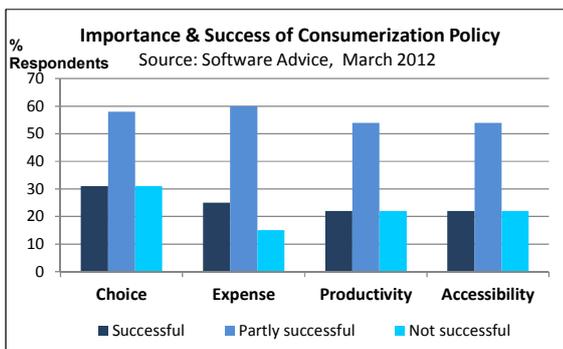


Figure 3: Enterprise attitudes to BYOD policy

### D. Consumerization concerns

BYOD security concerns are the first concern to emerge and are already addressed by many service providers and vendors. Small and light portable devices can be lost or stolen easily, and with them - confidential corporate data and access to enterprise facilities. In [2], nearly half of companies with BYOD strategy reported serious breaches of security.

There are various security solutions offered (see [5], [11]) to overcome these issues, e.g. data encryption and remote wiping of data on stolen devices. Security considerations also influence routing policies, such as routing via specific gateways or secure tunnels. BYOD security measures are also linked to Cloud security, e.g. remote data access authorization and encryption of data ‘at rest’ as well as ‘in motion’.

The topic of security for BYOD, public Cloud and VDI is still evolving and is out of scope for this paper. Suffice to say that these security issues are an integral part of the new reality of popular Internet-based services, smart devices, ubiquity of service and high mobility, all of which are generating new risks. By all signs, these risks - though must be mitigated - will not halt the progress towards BYOD and Cloud.

As BYOD matures, more issues will surface. One of the main issues that is at the heart of the eBC concept is that business usage on personal devices still needs to be reimbursed, while allowing users to take responsibility for their own personal spending. This requires ‘selective funding’ of business use.

Enterprise network capacity has to support the surge of traffic generated by smart devices. With BYOD, the enterprise could see unacceptable increase of personal traffic. Unchecked, personal use at the company’s expense can dramatically increase enterprise costs. At the same time, IT managers need to ensure that valid business sessions have adequate QoS (Quality of Service), even when competing with personal use. Business use of bandwidth-hungry application should also be rationed, according to the perceived business priority.

The enterprise needs to ensure that employees comply with legal requirements and respect content digital rights on BYOD devices, because it could be liable for employees’ misconduct. With BYOD, this responsibility may be extended to the personal use, for example, parental control when at home.

These concerns may be resolved by dynamically distinguishing business usage from personal usage, in order to apply differentiated enterprise-centric policies and funding decisions.

### E. Related Work

There are many studies of the methods to provide IT service authorization, including Role Based Access Control (RBAC), Task Based Access Control (TBAC) and Attribute Based Access Control (ABAC) and their hybrids, e.g. in [13]. These methods address access to data, but not the session delivery profile. Only few researchers address mobile broadband. In [9], web semantics to express mobility context aspects are proposed. In [15] mobile context vocabulary (PRISSMA) is used for access control of graphs. In [7], an ontology-based solution is proposed to integrate policies of disparate entities, assuming that they are all similar, lacking only a common language. However, mobile policy is very different from business policies, and the same terms have quite a different meaning for the enterprise.

This paper introduces the concept of the enterprise determining service delivery policy to support BYOD. This idea is studied further: In [16], controlling enterprise policy by



### III. WHY POLICY IS NEEDED FOR BYOD

#### A. *Selective Funding with a single identity*

With BYOD, it is assumed that a single identity on a device is used for both personal and business purposes. Separation of private and business communication on a single device is technically possible via two identities with a Dual SIM phone. Dual SIM can be used in stand-by mode (one SIM is active at any one time, which means that the stand-by is unavailable for incoming calls), or in an active mode (both operating simultaneously, which requires a more expensive dual-CPU handset and longer battery life). Despite the disadvantages, manufacturers such as Nokia and Samsung have recently started to market Dual SIM in developing countries.

The separation of functions and data between the two identities depend on the manufacturers, but some network features and services may not work properly as a result. Many features (including 3G authentication) rely on the unique binding of the hardware serial numbers with the SIM numbers.

Occasional use of an alternative SIM (e.g. by roamers) can be useful, but continuously switching between identities every time a service is requested is too awkward for users, who will neglect to select the right ID before requesting a service and end up using the wrong identity.

The funding of business expenses is becoming more important, even where flat rate is still the norm. Quota based charging is still the means of metering usage, but this may not always be so. With high-bandwidth services and greater reliance on them, users reach the thresholds of their quotas more readily than before, incurring higher charges for additional use. Usage of roaming data is also on the increase, as constant connectivity is now in greater demand.

If users are given two identities, one of which (the enterprise ID) means free services, they will always select it, rather than exhaust their personal quota. This means that the Dual SIM is ineffective and the enterprise will need to laboriously inspect itemized bills to identify legitimate business expenses.

Currently BYOD personal usage on mobile broadband remains at the discretion of the user, while business usage is rationed retrospectively via expense claims or by a monthly allowance. In both cases, employees cannot tell when they exceed carriers' quotas with their personal spending (which also includes business) or when they exceed the allowance in their business spending, which is not calculated for them.

After the novelty of BYOD wears off, enterprises cannot expect users to continue paying for devices and business services which should be borne by the enterprise. For all these reasons, we believe that distinguishing business usage dynamically is requirement for BYOD.

#### B. *Resource management for BYOD*

Usage management is not merely a matter of capping levels. It involves business prioritization of service requests. The absence of usage metering encourages indiscriminate resource consumption. Enterprise network resources must be

protected to ensure that business traffic gets the quality it needs, even when competing with personal traffic. To retain employees' satisfaction and encourage productivity, personal LAN (Local Area Network) usage need not be banned altogether. Instead, detected personal usage can be allocated lower priority. If personal usage during working hours becomes a drain on employees' time, video-based games, for example, could be selectively permitted only during the lunch break. This way, the eBC Policy can shape employee behavior.

For some service types, policy can decide whether to force changing the access network, as proposed in ([8]). This is not unlike the old IN (Intelligent Networks) service of 'Forced-on-Net', which selected calls that should run within the VPN. This can provide improved QoS and cheaper delivery per session, according to the media type and session context. Most often than not, this will be used to divert expensive sessions from 3G/4G to the enterprise Wireless LAN (WLAN), to optimize the utilization of enterprise network resources. This switch of access network should be governed by business context, since only refundable business sessions will benefit from reduced charges, while personal mobile broadband use is charged to the user and should remain on the carrier's network.

#### C. *Enterprise controlling BYOD costs*

There are different attitudes to compensating employees for business usage and new considerations for the IT expenditure with BYOD. As it stands with full BYOD, the enterprise has no bargaining power over mobile carriers and equipment suppliers, even though it may be covering substantial costs of devices. Similarly, by compensating employees for business usage, the enterprise is paying consumer prices with no bulk discounts. With eBC Policy and direct carrier payments, the enterprise can negotiate bulk usage discounts and SLA.

Compensating employees currently takes several formats, each with its merits and de-merits. A monthly allowance will be regarded as earned benefit for tax purposes. Claimed expenses are a hated chore that employees resent, and the additional bureaucracy of processing expenses diverts staff to an unproductive activity. With the proposed eBC policy decision, the enterprise can pay the mobile carriers directly, and have a fully logged audit trail for the taxman.

BYOD companies already find that they need to upgrade their own network. This may be expensive if the enterprise does not curb employees' personal consumption and enforce selective funding. With service policy decision, an enterprise could manage levels of personal usage by diverting personal sessions from the LAN to mobiles broadband and let users decide how much they are willing to spend on their own accounts. Conversely, business sessions can be diverted to the LAN, optimizing costs of business usage that is reimbursed.

Another way of controlling costs with the eBC policy is smart budgeting. The enterprise can structure budgets for departments and let them manage their employee quotas that determine session funding. With eBC Policy, quotas can be dynamically shared between users within the department and between departments, thus optimizing the carriers' SLAs.

#### IV. PROPOSING CONTEXT-BASED SESSION POLICY

##### A. Levels of Policy Control

Service delivery policy is decided at several levels, by the entities that are involved in the service delivery. Figure 5 shows analysis of the ‘policy tree’. It shows that User Policy determines personal budgets, special privileges and maybe disability based choices. Service Policy is managed by the party that provides it, i.e. ASP, carrier or the enterprise. The type of service determines the media and the required QoS for it. Service policies can be based on the usage of media types, duration and the type of charging.

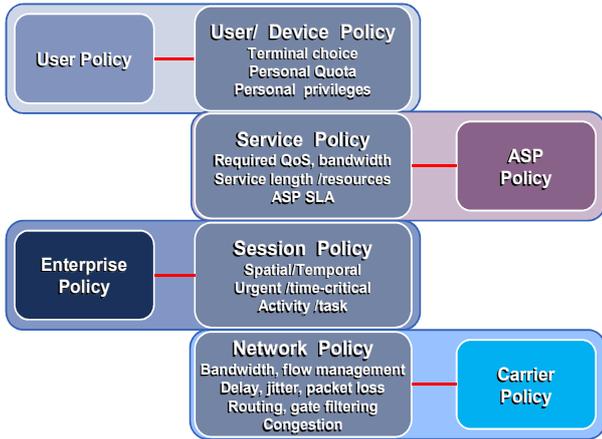


Figure 5: The Policy ‘tree’ – Enterprise to control sessions

Session Policy affects setting up sessions by assessing environmental aspects, current tasks and the level of urgency. Session policies include setting up funding limits, security levels and special routing that are dependent on the session attributes. Session policies are normally the carrier’s prerogative, but this paper proposes to transfer them to the enterprise.

Network policies are determined by the network operator. They deal with management of data flow streams with QoS profiles of bandwidth, delay, jitter and packet loss. They also include routing and gating. Credit control may be enforced at this level, but it is set up by the session policies. Other network policies are also influenced by the session policy, e.g. priority levels, guaranteed bit rates or monitoring triggers.

##### B. The scope of enterprise policy decision

Context data can come from internal resources (workflow, roster, email, LAN login) and from external sources (carrier, ASP or independent e.g. GPS for location).

Within the enterprise domain, the main areas that influence policy decision include:

- Service Request: details of the parties, service type, media etc.
- Enterprise Business: SLAs, sponsoring agreement, budgets, expenses policy etc.
- Enterprise Session Context: user roles and tasks, factors and attributes

- Network aspects: policies for the LAN/WLAN, switching access mode and inter-connections.

Aspects that are contributing to the session policy definition under the enterprise control are summarized in Figure 6.

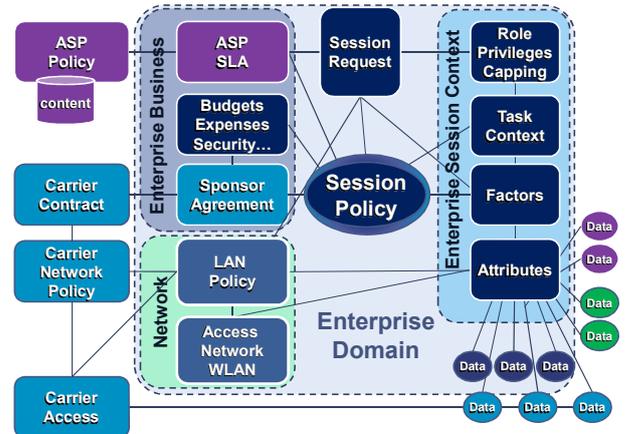


Figure 6: Aspects contributing to Session Policy

##### C. Context from internal, confidential data

While Telco policy servers can provide some context based variations, they cannot delve deeper into users’ activities and interpret corporate strategies. The enterprise has the advantage over carriers with its ability to discover employees’ context and apply business priorities. Context data can be drawn from employees’ booked appointments, contact lists, work-schedules, workflow, and LAN logins. The enterprise can utilize this knowledge to determine policy decisions. For example, travel approvals can indicate when users are on business trips and their costs should be covered.

Some data is considered by the enterprise as confidential, e.g. customers’ locations, internal work rosters or employees’ booked business trips. The enterprise is also required to maintain privacy of its employees’ information. Such information cannot be disclosed to external parties but can still be used by the enterprise internally. Access to personal employee information must be made according to privacy laws in the country, however in most cases the enterprise is entitled to access to its own data and can use it for internal processes, provided data is not divulged to external entities.

Selecting what data can be used must also consider employees’ attitudes, even within the enterprise rights. It is expected that employees will be inclined to consent to such use of their data if they benefit from direct funding and not having to claim expenses.

##### D. Session Context evaluation

In research papers the terms of Roles, Tasks and Attributes are often used to describe components of context. In IT, access method of RBAC, ABAC and TBAC have been proposed. Our enterprise Policy solution uses a hybrid of roles, tasks and attributes, but their definitions are not necessarily the same. For example, TBAC defines an IT based task, while our definition of a Task is a class of business activities that indicates user context, such as travelling or working at home.

The evaluation of Context that we propose is based on hierarchical context component architecture. As shown in Figure 7, four levels of context evaluation are proposed, each with their respective policies: Roles, Tasks, Factors and Attributes.

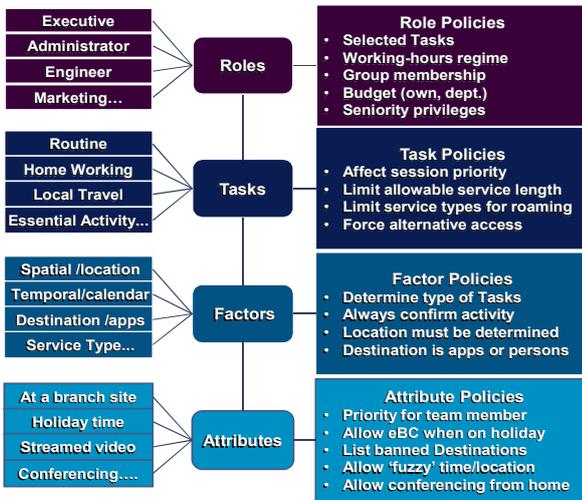


Figure 7: Relating nested policies to context components

Roles are defined by the enterprise according to job descriptions. They can be executive, administrator, shop-floor, engineer etc. The enterprise assigns to Roles credit limits and privileges regarding access to resources. Roles can be affected by departmental policies and group/team association. Roles influence the business context evaluation by the selection of tasks that are permitted for the role. Only these tasks are contemplated for the business status.

Tasks are general activity types that employees are engaged in, for example, Routine (at the office), Home working, Travel (locally and abroad) or Essential Job (critical activities). Tasks contain a set of Factors that define the differences between tasks. Policies for tasks define how they are prioritized and what may be limited. Task policies may be determined according to combinations of factors, e.g. if roaming (Location Factor) then only low bandwidth services (Service Type Factor) are funded.

The Factors are defined as aspects that affect the service session and can be measured via their attributes. Factors aggregate attributes into context aspects that are easily addressed by enterprise staff. Factors can be, for example, Spatial Aspects, Temporal Aspects, Activity Type, Service Type or Destination (both human and machines). The Factors are used to assess business context through associated prioritization that characterizes the task. Factor policies can refer to multiple attributes, e.g. Activity must be confirmed by two attributes (due to possible ambiguity). Factors are emphasized when they are particularly important for the task, e.g. location is critical to the Travel Task.

The attributes are the building blocks, linking to raw, atomic context sources and defining status for one detail at a time. For example, 'at home' or 'enterprise branch' are attributes of the Factor Location, and 'lunch break' or 'holiday' are attributes of the Temporal Factor. Policies for attributes

affect the way they are processed, e.g. they can decide whether Fuzzy Logic is used to determine 'near-the-office'. Policies can apply to one specific attribute in one particular Task, e.g. whether the enterprise discourages video conferencing while abroad.

The evaluation of these four components of context is detailed in [17] and computed examples are given in [18].

### E. The enterprise policy decision process

The proposed process of defining enterprise policy decision has three phases:

a) The session context is assessed in the eBC Function, as described in [17]. If eBC status is granted, the enterprise is committed to fund the session. If eBC status is not granted, the service request is treated as 'personal' and is forwarded to the carrier to be executed as a normal consumer session.

b) For funded service requests, an eBC profile is evaluated from context attributes, factors, tasks and roles with their respective prioritizations. This determines levels of funding and priorities that are assigned to the session (see [18]).

c) For requests that are forwarded to mobile carriers, the eBC profiles are mapped into 3GPP policy messages [16], thus integrating the eBC Policy with mobile networks.

### F. The eBC Policy Network Integration

Supported sessions requests need to convey the policy decision generated by the eBC Policy as shown in Figure 8. Two existing 3GPP models can be used: the VNO model and the Sponsor model. Further details are given in [16].

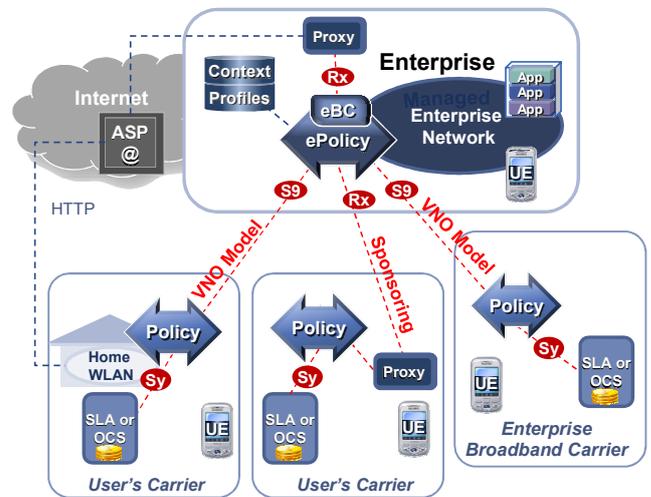


Figure 8: Enterprise eBC Policy as a VNO/Sponsor

The eBC Policy server can interface to carriers as a VNO (Virtual Network Operator) and convey full PCC rules over the inter-carrier link of the S9 interface [16]. As a VNO, the enterprise looks after its employees' accounts but defers personal calls back to the respective carriers.

Alternatively the enterprise acts as a service Sponsor, as described in Annex N of [6], with enhanced Rx service requests containing sponsoring details. As a Sponsor, the

enterprise has SLA with each carrier that employees may choose. Since there could be many to negotiate with, automatically negotiated SLAs as proposed in [10] would be welcomed. Sponsored requests have authorized spending and service duration, thus provide a measure of policy control, but not as much as achieved via the S9 as a VNO.

### G. Is implementing enterprise policy decision viable?

The idea of allowing the enterprise to determine network delivery policies without Telecom skills may seem as heresy to Telecom people. However, in our solution enterprise staff will be dealing with business rules and prioritization to redefine the Session Policy while the conversion into Network Policy is performed automatically. Figure 9 shows the steps of converting business objectives to session delivery parameters, included the three phases of eBC Policy establishment.



Figure 9: From Business Goals to Network QoS & Policies

Enterprises may not wish to take on the task of operating such a high-availability function that is critical to session admission. Like other VNOs, enterprises can outsource the operations of the eBC Policy server, yet still keep data confidential. They may opt for hosting by a VNE (Virtual Network Enabler), which has the added advantage for BYOD, having established inter-connections to many carriers.

## V. CONCLUSIONS

Consumerization has already moved from a buzzword into an unstoppable disruptive force that is reshaping the enterprise market. It brings great savings but also some serious concerns. We argue that empowering the enterprise to make its own session policy decision can solve consumerization issues and provide selective funding with smart resource allocation.

In maintaining its own context-based policy decision, the enterprise will not abandon Mobile carriers altogether (as in ultimate BYOD model), but will become a service Sponsor or a VNO for its employees. Policy control enables managing corporate resources per service request and curbing employee spending while allowing employees full freedom for personally funded services.

While service providers normally define Service policies, and carriers do control Network policies, the enterprise should determine the Session policies, which are concerned with environmental aspects, undertaken tasks and activities. Such session policies are derived from business goals that are mapped to the various session aspects and are assigned significance and desirability via prioritization.

The enterprise is well placed to use its internal data sources to deduce business context. This data may be confidential and cannot be made available to carriers, but can be used internally to generate much more accurate business context.

The process of defining eBC Policy has three phases: first the eBC status is granted for funded sessions and personal use sessions are deferred to personal carriers. Next, an eBC profile is produced by evaluating the session attributes, factors, tasks and roles, to determine levels of funding, QoS and priorities. Then, for requests bound for mobile networks, the eBC profile is used to determine PCC rule parameters that are compatible with 3GPP networks.

In summary, an enterprise-own context-based Policy solution supporting consumerisation is a bold idea for a rapidly disrupted corporate market segment. It is cost effective due to the large enterprise cost savings, from selective funding, smart resource policy, SLA sharing and budget control. This solution represents a new opportunity for vendors and service providers who could offer it as a managed service.

## REFERENCES

- [1] Avana® Research & Insights “Global Survey: Dispelling Six Myths of Consumerization of IT” January 2012
- [2] Decisive Analytics “Mobile Consumerization Trends & Perceptions IT Executive and CEO Survey” February 2012
- [3] Software Advice <http://blog.softwareadvice.com/articles/hr/byod-or-bust-survey-results-report-103212> March 2012
- [4] D Moschella, D Neal, P Opperman, J Taylor “The ‘Consumerization’ of Information Technology, Position Paper”, CSC 2012
- [5] “Safe BYOD Networking with NAC, An InfoExpress White Paper” InfoExpress March 2012
- [6] “Policy and Charging Control (PCC) architecture”, 3GPP TS 23.203
- [7] I. Miloucheva, D. Wagner, Ch. Niephaus, D. Hetzer “User-centric identity enabled QoS policy management for Next Generation Internet” IRECO Journal, July 2008
- [8] Jens Schumacher et al, “Providing an User Centric Always Best Connection”, 2010 Second International Conference on Evolving Internet, PERIMETER project
- [9] H Shen, Y Cheng “A Semantic Context-Based Model for Mobile Web Services Access Control” 2011 in MECS
- [10] F Zulkernine, P Martin, C Craddock, K Wilson “A Policy-based Middleware for Web Services SLA Negotiation”, ICWS 2009
- [11] “Consumer Technology in the Workplace: Managing Security Risks and Maximizing Employee Productivity” 2010 Unisys Corporation
- [12] Trend Micro “Trend Micro Enterprise Security” July 2011 <http://bringyourownit.com/2011/09/26/trend-micro-consumerization-report-2011>
- [13] M A. Al-Kahtani R Sandhu “Induced Role Hierarchies with Attribute-Based RBAC” ACM June 2003
- [14] Good Technologies <http://www.eweek.com/c/a/Mobile-and-Wireless/Kindle-Fire-Gets-Enterprise-BYOD-App-From-Good-872461/>
- [15] L Costabello, S Villata, N Delaforge, F Gandon “Linked Data Access Goes Mobile: Context-Aware Authorization for Graph Stores” LDOW2012 April 16, 2012
- [16] R Copeland, N Crespi “Controlling enterprise context-based session policy and mapping it to mobile broadband policy rules” IEEE ICIN 2012
- [17] R Copeland, N Crespi “Establishing enterprise Business Context (eBC) for service policy decision in mobile broadband networks” ICCCN ContextQoS 2012
- [18] R Copeland, N Crespi “Implementing an enterprise Business Context model for defining Mobile Broadband Policy” IEEE CSNM 2012
- [19] SearchConsumerization <http://searchconsumerization.techtarget.com/news>