WHITE PAPER

Why BYOD Needs Unlimited Wi-Fi to Be Successful

Changing the Economics of Mobility and Revolutionizing the Connectivity Experience

Executive Summary

There was a time—not long ago—when your company provided the equipment you needed to do your job: A cheap desk, a rotary phone, and the ability to knock on the boss' door and say, "Can you look at this?" Then the computer changed the workplace forever. In three decades, a dizzying array of laptops, smartphones and tablets have transformed how and where we work. Your company tried to keep up with the rapidly changing technology needed to maintain a productive and satisfied workforce… but it couldn't. Hundreds of personal devices now demand a piece of the corporate network and thousands of employees demand them, too. Most enterprises have waved the white flag and found ways to coexist with the barbarian devices laying siege to their infrastructure.

This is the world of Bring Your Own Device, or BYOD. Like BYOB (Bring Your Own Beverage), a more familiar acronym to many, it keeps your whole team at the table, while giving them the freedom to choose what suits them best.

As more corporate resources migrate to the cloud, it makes even more sense to allow end users to access data and applications whenever and wherever they want. Allowing them to choose their own devices empowers employees and makes them more amenable to working longer and more productively from previously unconnected places. It's been a victory for everyone: BYOD increases employee satisfaction and performance while also reducing up-front capital expenses for equipping today's global mobile workforce.

BYON: Let's Get This Networking Party Started. Smart enterprises know that devices are relatively cheap, while the wireless networks they run on are expensive. Consider, for example, the unwary traveler who, on an international trip, forgets to turn off cellular data roaming – and is shocked by a mobile phone bill that could have bought an iPhone…or three, or financed the entire trip. So these businesses are devising not only BYOD guidelines, but "Bring Your Own Network" (BYON) policies to right-size the wireless access costs as well. Cellular data plans are still notoriously hard to figure out, with countless sources of potential cost overruns when users exceed

TABLE OF CONTENTS

their plan limits. And let’s be honest - if Netflix has just released the newest season of House of Cards, plan limits are going to be exceeded. Without a clear plan for purchase of wireless access, employees may make costly decisions (all in the name of “getting things done”), pay for them out-of-pocket or bundle them into travel expenses, pushing connection costs into a budgetary black hole, the same place your ticketmaster fees seem to go. Others may simply go dark, choosing not to connect and work in fear of exorbitant charges. Your expense accounts should not rival a small country’s GDP.

The answer: Just like a good BYOB party needs the right atmosphere, no BYOD plan is complete without BYON. Enterprises need to control connectivity costs for all workers, develop policies for the use of corporate and end-user devices, and differentiate between the level of support for wireless costs by employee groups as appropriate. With a solid, smart menu of choices, employees can be confident they are staying within guidelines while having the freedom to work where they want to, on the device of their choice.

The bottom line: BYON and BYOD are an inseparable pair, much like peanut butter and chocolate, or Steven Seagal and a strong male ponytail.

You CAN Take It With You...(And You Should)

Bring Your Own Device (BYOD) is rapidly sweeping the enterprise IT world for several reasons, including greater user productivity and satisfaction, and immediate corporate cost savings.

The basic reasons behind BYOD’s popularity are simple: People generally buy mobile devices they like, and are happy when they can also use those devices to make themselves more effective at work. All the better for selfies, Facebook, and Angry Birds. You know, “work stuff.”

In general enterprises can save a lot of upfront dollars by having employees make work-device purchases out of their own pockets. And as long as the work gets done, it doesn’t matter if your employee’s screen saver is a duck faced selfie or Darth Vader. (Although, come on, as if there’s even a choice).

Bring Your Own Catch

But, as with most things in life, there’s a hidden cost. Even free ice cream still has calories.

On the surface, BYOD is a boon for enterprises—lower equipment costs and employees who work longer hours. But underneath, there’s a potential trapdoor to BYOD success: the sour taste that comes with hidden network access costs, where a binge of unexpectedly expensive megabytes could swallow up any potential savings BYOD brings to the table.

With corporate applications quickly moving to the cloud, mobile is rapidly becoming not just a feature but the reference architecture for how employees interact with the enterprise network. The “company laptop” and “company phone” are becoming just part of the “mobile stack” of devices, which now includes personal tablets and smartphones that stay with mobile workers all the time. Let’s hope selfie sticks don’t work their way onto this list anytime soon. Corporations who don’t get on the BYOD train may find themselves with a frustrated workforce, one willing to “go rogue” and use unapproved devices and services.

But to really empower a mobile workforce, corporations must look beyond the “D” of BYOD and remember the “N”—because in the long run, like razors and blades, devices are cheap but networks can be expensive. A successful, future-looking enterprise BYOD strategy will evolve to something you might call BYON, aka Bring Your Own Network. It’s a new twist that embraces not only a choice in end-user devices, but also mixes in a flexible, smart plan for secure, consistent connectivity to fuel the new mobile apps transforming how business gets done.

From Fax Machine To Apple Watch, In The Blink Of A Google Glass

Just how did we get to this brave new world of mobile centric computing? Many of us are old enough to remember how big a deal it was to get corporate email on the company-purchased BlackBerry. Note to under 25’s: Blackberry was once cool. But the real revolution to a truly mobile workforce started with Apple’s introduction of the iPhone in 2007, and the App Store in 2008. The combination of a powerful, portable device that could easily access web pages and an easy, fast way to build mobile applications broke the stranglehold that wireless carriers had held on mobile-device functionality.

The subsequent introduction of similarly powerful devices running the Android operating system and then the iPad in 2010 helped the mobile revolution spread quickly. Application developers, freed from having to “qualify” their programs for specific carriers and devices, now could build quickly for one or two widely used platforms—or could simply design so-called “cloud” services that could be accessed by any device with a browser and an Internet connection. Overwhelmed at first by the sudden demand for mobile data, wireless carriers across the globe quickly ramped up plans to expand and improve cellular networks, while many retail businesses, hotels and corporate campus administrators made similar moves to expand their local Wi-Fi services to address the insatiable quest for a mobile connection.

Someday this historic shift will be amazing when it is fully quantified, but even as it evolves, the numbers point pretty clearly to a workforce quickly moving from desk- to mobile centric as the main way things get done. One recent survey[1] of remote workers found over three-quarters of the respondents (77 percent) claimed they were more productive when they worked remotely. And great news for management, over half of them (52 percent) said they were less likely to take time off as a result.

As another key industry report[2] noted:

Mobile technology and cloud-based applications have enabled a rapid increase in telecommuting and work shifting. The strict “9-5 at the office” paradigm no longer works in people’s lives today.

[1] Remote Working Behavioral Study, Connected Solutions 2015

[2] Mobile Workforce Report, iPass. 2012

According to a recent study from Cisco[3] , rather worryingly, 42 percent of people surveyed would choose Internet access rather than their sense of smell. Goodbye roses, hello candy crush.

Gen X & Y prefer smartphones to TV's. The majority of Gen X and Gen Y professionals when asked said they would select their smartphone instead of their television.

Note to under 20's: A television is a box people used to stare at but was too heavy to carry in their pockets.

One massive by-product of the shift to a mobile workforce and mobile-connected lifestyles is the blending of work and personal lives—and the fairly normal desire to carry around the fewest number of devices possible. That means that people who want an iPhone want to use that iPhone to access work applications. They don't want a separate "work" phone. That, in a nutshell, is how BYOD began. According to Infonetics[4] , most businesses in 2014 planned to increase Wi-Fi capacity by 20percent, an assertion supported by HP who found that 73.5 percent were doing so to support growth in mobile devices and BYOD phenomenon[5].

According to Gartner[6], by 2020 up to 85percent of businesses will implement a BYOD program. But, since many firms currently don't have clear BYOD policies in place, mobile workers are often on their own when it comes to finding mobile connectivity, opening up the potential for expensive or insecure network access methods.

The dawn of BYOD appears to link strongly with mobile workers who've revealed that they are a resourceful group and will do anything to ensure ubiquitous connectivity, including workarounds that could unwittingly threaten the security of a company. However, they also feel a sense of responsibility and care deeply for what they do. They are far more willing to use their personal devices for work, but much less willing to use their work devices for personal reasons. The impact on IT departments can be onerous.

Networks For Your Net Worth

When it comes to being a mobile worker, it's easy to identify the biggest point of frustration: finding a decent wireless connection. In the old days when it was just email on a BlackBerry, a regular cell signal was good enough to get the job done. That all changed with the advent of smartphones and tablets. Now a mobile worker is regularly exchanging big files, trying to work on web-based apps or even conducting video calls. It's a wireless data tsunami, one that saw traffic on AT&T's wireless networks increase by more than 5,000 percent in the few years after the iPhone's introduction. For BYOD to work, there needs to be a pretty big "N" – for Network - behind the scenes. The big question is, who pays for that network (assuming you're off the family plan) and what's the best way to connect?

[3] Connected World Technology Report, Cisco. 2014

[4] Wireless LAN Strategies and Vendor Leadership, Infonetics. 2014

[5] Networking for the BYOD Enterprise, Nemertes Research, HP. 2013

[6] Bring Your Own Device: The Facts and the Future, Gartner. 2013

For most mobile workers the default first choice for connectivity is the cellular network, which is pretty much ubiquitous. And of late it's getting better and faster at handling mobile data, thanks to the so-called "4G" network buildouts now taking place for most of the major carriers. But when it comes to heavy mobile connectivity needs, cellular isn't the best answer. This is especially true now that most of the largest cellular carriers have all but eliminated "unlimited" data plans, instead forcing their customers into plans where every bit must be paid for... or forcing them into coffee shops with crowded tables. Do you really want your work product surrounded by aspiring screenwriters, toddler playdates, and tourists waiting for the bathroom?

While that might sound fair, in reality it's still a black art to figure out exactly how much data your phone or tablet is using at any place and time, since throughput performance varies widely. Even though the carriers have become more forgiving for people who use more data than their plans call for (by allowing them to upgrade when they exceed data limits), there are still penalties for data "overages," especially during international travel. We've all heard the stories of the $60,000 roaming bill, and many mobile workers have experienced a similar pain, if not on the same scale.

An iPass remote working survey[7] found 43 percent of all respondents had received a data roaming bill that they considered unusually high. And, according to the 2014 iPass Mobile Workplace Report, a full 81percent of respondents[8] agreed that wireless data prices were way too high. There is a vicious rumor the remaining 19 percent haven't responded because they're still waiting to get online.

For most savvy mobile workers, the quick answer to cellular connectivity headaches is Wi-Fi, which is generally less expensive and typically provides a more robust signal than cellular. It's often found in conveniently located "Wi-Fi shops" charging a premium for accompanying liquid, teased out of beans in an elaborate fashion. In fact, according to the European Commission[9] 71 percent of all mobile communications flows over Wi-Fi. The 2014 iPass Mobile Workplace Report also showed 80 percent of business travelers prefer Wi-Fi over cellular connections for using mobile apps or making phone calls - usually via a voice application like Skype, Tango or Vonage. The latter two are companies you may not have heard of that will probably get sold for billions.

Making BYON as Easy as BYOB

Though many "free" Wi-Fi options exist—the ubiquitous Starbucks network is the prime example—seasoned mobile workers know that often with free Wi-Fi you get what you pay for, and it may not be what you need to get the job done. Since there is little, if any, monetary incentive for the provider, many free Wi-Fi hotspots offer just the bare minimum of performance, and often pose serious security concerns. With workers collaborating on sensitive documents over free Wi-Fi, you might as well have your CFO reply to every elaborate spam email plea for financial assistance.

For mobile professionals who need a solid, dependable Internet connection, what's usually preferred is a paid service that offers a high level of performance and some level of security guarantees. For BYOD

[7] Mobile Workforce Report, iPass. 2012

[8] Mobile Workplace Report, iPass. 2014

[9] Final Report: Impact of traffic off-loading on spectrum demand. European Commission. 2013

workers and the IT staff that supports them, the biggest questions surrounding such preferred methods of access are who pays for it, and how?

By 2019, Cisco predicts that 7 billion mobile devices will be connected to the Internet using some form of wireless access, accounting for 42 percent of all Internet traffic[10].

So, without a corporate policy in place, two bad things are going to happen when employees make their own decisions about access. First,

they overspend on pricey one-time access plans, at a hotel, airport or convention center, in the interests of “getting work done now.” One-fifth of workers pay for day pass access via a personal credit or debit card[11] , a method that can lead to access charges ending up in a “black hole” of expense accounting, hiding the real cost of connectivity from enterprise administration.

The second problem is when BYOD employees actively avoid mobile connectivity due to fears about cost overruns, leading to work inactivity which hurts both the employee and the company.

Numerous studies have found that mobile employees are shutting off their devices’ data connections when they travel[12] . An increasing number of workers also feel data roaming prices are too high and that the issue has become an important matter. Many mobile workers have personally dealt with these prices. Not to mention lost time in Starbucks lines.

Most workers want to do what’s right and will work harder and longer if given a clear path to mobile productivity. But it all starts with a plan for controlling cost and managing who pays for the network: If it was BYOB you would want to know what type of bottle you are meant to bring.

Mobile workers have shown they are willing to put in extra hours and be as connected as technology allows. Employees who feel they are being hindered by a lack of mobile connectivity will at some point communicate their inability to work to their full potential to their companies.

Whether employees pay the bill for their own smartphone use or whether the company provides prepaid plans, the key for a successful BYOD deployment is to make the network access component as clear as possible. From simple educational steps (like knowing when to switch from cellular to Wi-Fi) to full-featured solutions like iPass—which provide enterprises with the means to enforce expense and security policies while gaining visibility into device mobility needs enterprise-wide. There are many ways to allow enterprises to embrace the benefits of BYOD without fearing the hidden or sometimes confusing costs of network charges.

Pay It Forward, To Move Forward

Enterprises need to define the right combination of device and connectivity support based on the roles and responsibilities of different employee groups. IT now has a range of choices around controlling connectivity costs for all workers, developing policies for the use of corporate and end-user devices and

[10] VNI Global IP Traffic Forecast, 2014 – 2019, Cisco. 2014

[11] Ibid (page 6)

[12] Ibid

differentiating between the level of support for wireless expenses by employee groups as appropriate. With clear, smart policies employees can be confident they are staying within guidelines while having the freedom to work where and when they want to, on the device of their choice. The bottom line: you will need BYON to make BYOD a success.

IT can enable user productivity even while controlling cost and security by defining policies for managing devices, access to corporate resources and payment responsibility. A helpful way to consider these options is diagrammed below, with categories for devices and access managed, purchased and

approved by IT; those that are "tolerated," meaning they are purchased by the user who is granted access to apps and data; and those that are unsupported—meaning users can use them if they choose,

but IT does not support them and they may have limited access. And across these options, IT also has choices for whether the enterprise pays or the user pays for access.

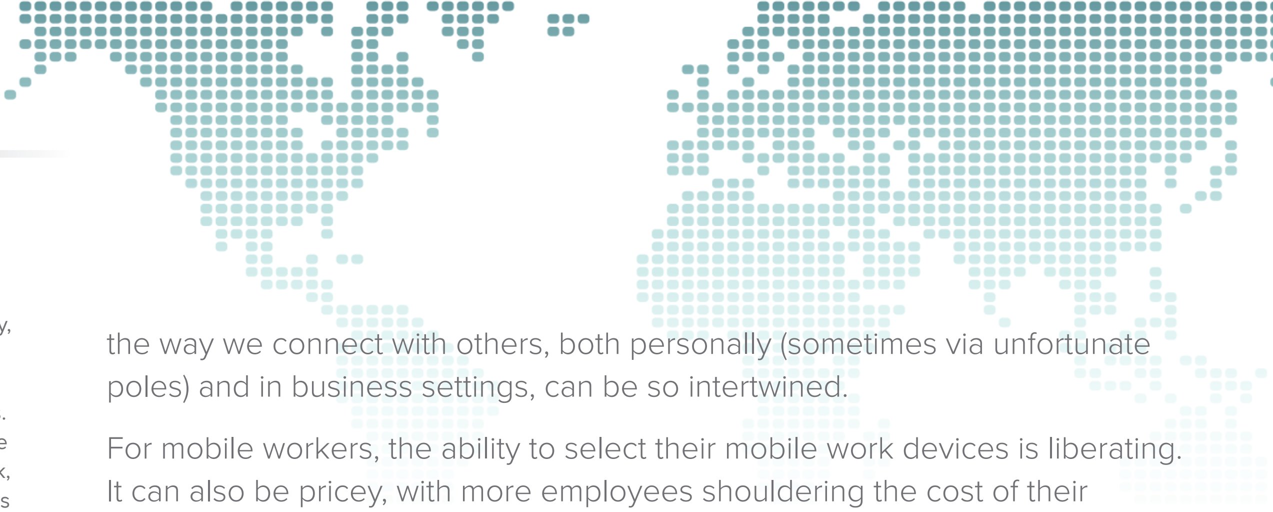
This strategy gives IT a mix of control and payment options for different employee populations. They may provide IT managed devices and pay for access for execs and sales staff; offer an IT Tolerated/IT Pays option for other key employees; and use the IT Unsupported option for the remaining employees, who may or may not be allowed to expense the cost of access back to the organization. This tiered system lets IT best enable those employees whose work is strategically important, while enabling productivity but tightly controlling cost for other employee populations who want to participate in BYOD.

User liable device with limited (e.g., email only) to no IT application support and the user pays for access.

	IT Pays for Access	End User Pays for Access
IT Managed Devices IT provisions and manages devices	IT managed laptops, smartphones and tablets where the organization pays for the device and for the cost of Internet access.	IT provisioned device, but the user is responsible for purchasing access. Common in situations where the user expenses access back to his or her department.
IT Tolerated Devices BYOD: User purchases device, IT allows access to applications	User liable devices where IT supports business applications on the device as well as directly pays for access. For example an executive who purchases his or her own Mac but IT pays for access.	User liable device (likely a smartphone or tablet) where IT supports business applications on the device and the user pays for access. There may be instances where the user can expense back access or get a stipend for business-related connectivity.
IT Unsupported Devices BYOD: User purchases device, limited to no IT support		User liable device with limited (e.g., email only) to no IT application support and the user pays for access.

Conclusion: Don't Worry About the Device. Do Worry About the Network.

Smart enterprise IT departments have already realized that their roles have changed, and the more they say "no" to end users, the less effective the security policy becomes. Because smart users will find a way to stay connected, whether it is secure and approved or not. This new situation is especially true when it comes to mobile devices, which are now incredibly personal and often an emotional choice because



the way we connect with others, both personally (sometimes via unfortunate poles) and in business settings, can be so intertwined.

For mobile workers, the ability to select their mobile work devices is liberating. It can also be pricey, with more employees shouldering the cost of their smartphones and tablets. With the wide variables of service pricing available, the BYOD trend is giving rise to a new challenge for both employees and enterprises: how to affordably ensure productivity by enabling mobile connectivity, even while controlling access costs.

The good news is that IT now has choices for supporting different employee populations with clearly defined, differentiated policies for devices, access control and expense liability. These choices will enable IT to make BYOD—and BYON—successful for both employees and the enterprise. And with the expanded productivity and increase in profitability that this evolution can help drive, office celebrations definitely won't be BYOB.

ABOUT IPASS

iPass is the industry pioneer in global, mobile connectivity, ensuring unlimited access to unlimited content on an unlimited number of devices. Founded in 1996, iPass is the world's largest Wi-Fi network, with over 53 million) hotspots in airports, hotels, airplanes, and public spaces in more than 120 countries and territories across the globe. Our hosted Wi-Fi-as-a-Service solution is easy, convenient, secure, and always on.

Expanding on its already established reputation as the premier provider of global Wi-Fi hotspots, iPass connects customers with the people and information that matter most. We are dedicated to delivering the highest quality, most cost-efficient solution on the market today.

Visit us at www.ipass.com

iPass

Corporate Headquarters
iPass Inc.

3800 Bridge Parkway
Redwood Shores, CA 94065
+1 650-232-4100
+1 650-232-4111 fx
www.ipass.com

Specifications and other information in this document may be subject to change without notice.