

Enterprise Mobility Control



Table of Contents

Introduction	3
Growth in Mobile Data	4
Enterprise Perspective	5
Cost	7
Productivity and Risk	9
Limitations of Existing Solutions	11
Enterprise Mobility Control	12
Conclusion	14

Introduction

Right now, we're in the midst of a transition. We're moving from an era marked by the rapid adoption of smartphones and tablets, and into one whose main feature will be the increased use of the mobile platform for business and lifestyle purposes. And with this will come a massive increase in the amount of mobile data consumed by both consumers and businesses. According to industry analysts, over the next five years while the number of smartphone users will double the volume of traffic they generate will increase tenfold.

To date surprisingly little attention has been paid to the implications for enterprises of the growth of mobile data consumption. How many CIOs are aware that the mobile data volumes consumed by their employees are growing by over 100% year on year? And that most of this is due not to growth in business usage, but to the rise in high-bandwidth consumer apps?



Mobile data volumes consumed by employees are growing by over 100% year over year

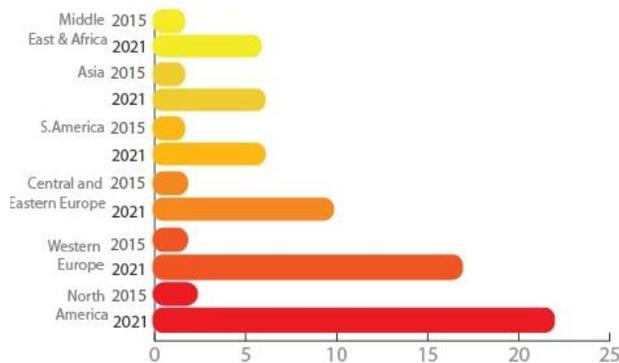
The purpose of this whitepaper is to examine this employee behavior and its implications for enterprises, and to explain how a new capability, Enterprise Mobility Control, can help organizations to reduce the costs and manage the risks associated with it.

Growth in Mobile Data

The launch of the first 3G-enabled iPhone in 2008 heralded the beginning of a period of extraordinary change in computing. Today, we take for granted that most people living in developed markets have a device more powerful than the computer on their desk tucked away in their pocket or handbag. It barely registers with us that high-speed internet connectivity is no longer limited to our home or office but is now virtually ubiquitous. We see the impact of these changes most clearly in the profound shifts in our everyday behavior. If we're not checking our smartphones for updates from friends, family or colleagues we're using them for entertainment or information, or to get a myriad of routine tasks accomplished on the go.

Along with these changes, we've seen exponential growth in the amount of data transmitted across both Wi-Fi and mobile networks. What's less appreciated is that this growth is not slowing down. A recent report by Ericsson, the network equipment provider, projects that average traffic from smartphones and tablets will increase tenfold over the next five years. And Ericsson isn't alone: Cisco is also projecting a virtual tsunami of data in the coming years, predicting that by 2020, the amount of data carried over wireless connections will exceed that over wired ones.

Monthly data traffic per smartphone (GB) 2015 - 2021



Source: Cisco VNI Mobile, 2016

This growth was initially driven by the increase in penetration of smart devices with Wi-Fi/3G/4G connections. The emergence of larger form factor devices, like the iPad, also played a part. Today growth is coming from increased use of high-bandwidth applications which stream sound or video. Application developers, like those at Facebook, have taken advantage of high-bandwidth connectivity to integrate new features—video, in particular—into their user experiences.

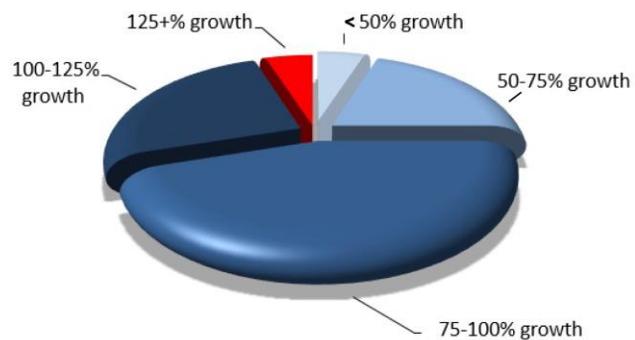
Enterprise Perspective

How is all of this playing out in the enterprise? Through our work with a wide range of enterprises, Corrata has unique insight and perspective into trends in enterprise mobile data usage. Work-related usage continues to be dominated by low-bandwidth applications, like email and data entry/workflow-related tools. Even relatively high-bandwidth applications like Lync or Dropbox do not generate traffic volumes comparable to music, video and social networking apps, which are massively popular among consumers.

What is surprising in light of this is the massive growth in mobile data consumption by enterprises. Enterprise mobile data volumes—specifically over cellular connectivity—are growing at rates anywhere between 70% and 140% annually (see graph opposite). This growth is coming not as a result of increased usage by a small number of data hogs, but is due to a marked increase across the employee base. The growth is caused by increased use of high-bandwidth consumer applications and services. Essentially, employees are bringing their consumer usage habits to their use of enterprise mobile services. As the proportion of digital natives increases within the employee population, typical employee usage patterns are converging on those of the average non-business user.

Year on year growth in mobile data consumption

The annual growth in mobile data usage for a range of enterprises surveyed by Corrata is shown below. While a small number of enterprises showed growth of less than 50% the vast majority had growth rates far above this. The average growth rate across all organizations was 96%.



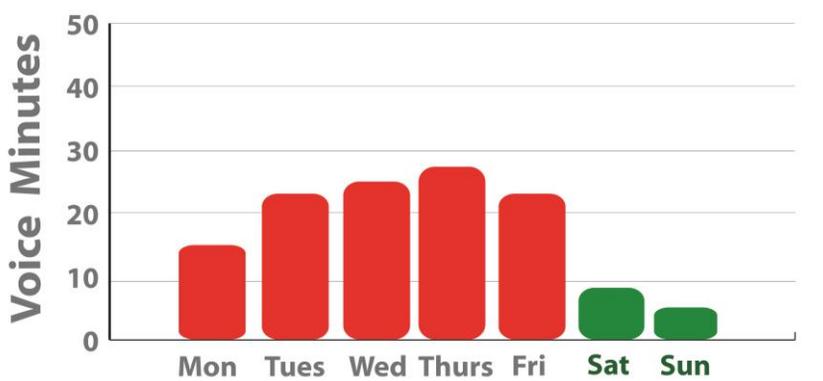
Source: Corrata, 2017

Enterprise Perspective contd.

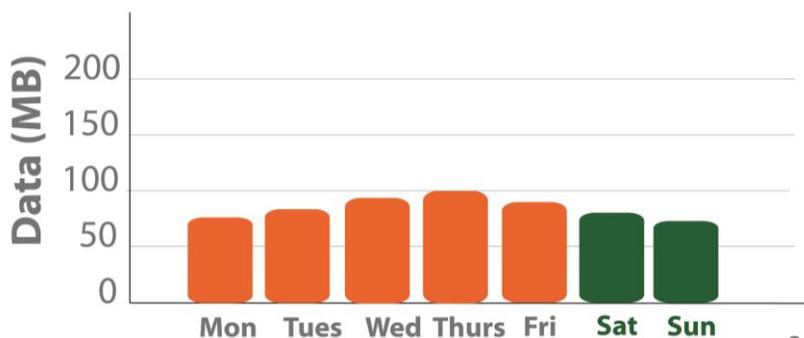
Two graphs that capture the merging of work and non-work data use are shown below. The first shows the average number of voice calls made by enterprise users by day-of-week. As you'd expect, the volume of calls falls sharply at the weekend. The second graph shows the same analysis for data usage. In sharp contrast, data usage hardly falls at all at the weekend.

This data reflects average patterns, but it's also not unusual to find employees whose weekend use is many multiples of their usage during the week.

Daily voice usage



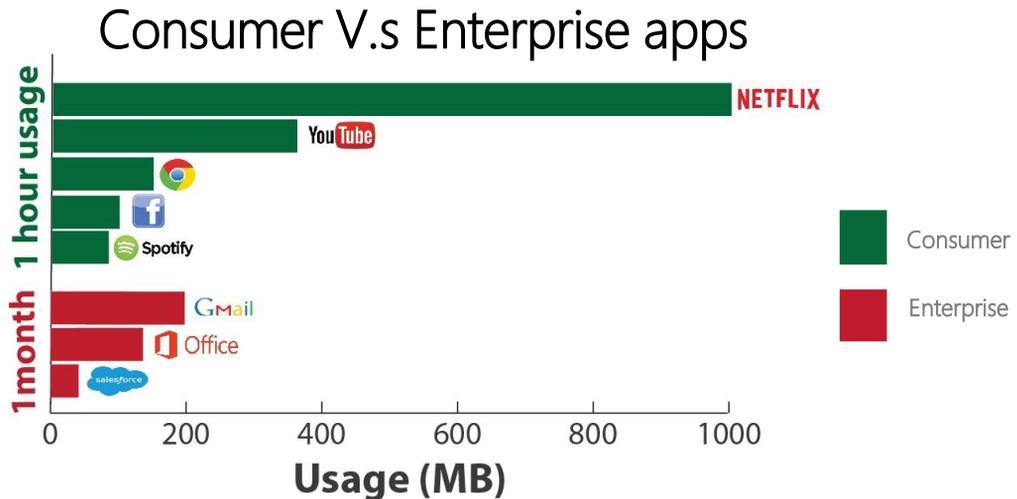
Daily data usage



Source: Corrata, 2017

Cost

The rise in employee mobile data consumption driven by the merging of work and personal usage patterns has implications for organizations in three areas: cost, productivity and risk. The rest of this whitepaper will spell out these implications before explaining what enterprises can do to address this issue.



High levels of data usage on the company plan, be they personal or business, will come at a cost to the enterprise. The benefit of reduced prices per gigabyte is not reflected in reduced telecom expense because of the explosion in data use. Without controls, there is a real risk that mobile data volumes will grow tenfold over the coming years. Thus, while per-gigabyte costs may continue to decline, this will not be reflected in reduced costs for business.

High non-business data use generates costs in three areas. The first, and typically the most high-profile, is the high cost incurred when employees use even moderate amounts of data abroad. A gigabyte of roaming data can cost as much as \$10,000.

Every organization has horror stories of staff who inadvertently run up bills in the thousands of dollars while travelling—streaming your hometown’s football game in a hotel in Hong Kong with the mistaken impression that you’re on Wi-Fi, or returning from a family vacation to discover that your children have used your work phone as a mobile hotspot and used up your company’s entire roaming allowance. The stories are legion.

Cost Contd.

The growth of domestic data usage is a more insidious source of avoidable cost. Increasing data use requires businesses to buy large data allowances. These allowances can be designed in multiple ways—an allowance that's exclusive to an individual device (an exact mirror of the typical single consumer plan); a per-device allowance where any underutilization can be used by others in the enterprise (similar to a family plan); or an enterprise wide data pool.

Regardless of the type of plan, the fundamental issue is that none of this data is free. Further, paying for an exponentially increasing amount of data over the coming years is a missed opportunity for organizations to drive down expenditures on what is today a commodity product.

A final way in which exploding data usage drives cost is the administrative burden of mobile expense management. With growing usage and regular bill shock events, enterprises have to put in place administrative arrangements to ensure these items are monitored and dealt with. Unexpectedly large bills need to be investigated, data plans need to be reconfigured, and roaming arrangements need to be reviewed. All of this distracts staff and resources from more productive activities.

Changes in Europe

In June 2017, roaming charges within the European Union (EU) were eliminated. This means that a resident of any country in the EU who visits another EU country doesn't incur roaming charges. In effect, for EU residents, visiting another EU country will be equivalent to a US resident visiting a different state. Non-EU residents will continue to be subject to roaming charges when they visit the EU.

There are some nuances to the changes—for instance, if you have a low cost all you can eat data plan not all of it may be usage abroad—but overall, it's a big benefit for EU residents. The decision by Britain to leave the EU (Brexit) may lead to the reintroduction of roaming charges both for British residents visiting the EU and for EU residents visiting Britain. However such a move could only happen once Britain has finally exited the bloc at the end of March 2019.

Productivity and Risk

We finished the last section by highlighting the headaches and distractions involved in mobile expense management. But there can be far broader productivity implications from granting employees unrestricted access to the vast array of mobile apps and services now in use.



In 2016 674 new security threats to smartphone devices were identified - an increase of over 32% on the previous year's figure.

Constantly checking your phone can obviously lead to unnecessary distractions—as you follow that Facebook meme on the talking dog or the cat and the cucumber prank it's easy to see how your time can be frittered away. In the same way that some companies have seen the benefit of restricting access to content on PCs and laptops, a similar approach may be necessary on enterprise smartphones and tablets. And in high risk environments such as construction or manufacturing distractions can have more serious implications than just wasting valuable time.

As organizations becomes more reliant on mobile devices, the cyber security, legal and reputational risks to their operations continue to rise. In 2016 674 new security threats to IOS or Android devices were identified by security researchers - an increase of over 32% on the previous year's figure. With over 5 million apps available from both the Apple App Store and Google Play the risk of attack through this vector has increased greatly. In addition there is the risk of phishing attacks through email, browsers and messaging apps. Together these factors make a strong case for the need to prevent employee devices from connecting to inappropriate or malicious domains.

Productivity and Risk contd.

In addition to concerns around cybersecurity enterprises need to be aware about the reputational and legal risks they run by allows unrestricted internet access on smartphones and tablets. Picture this scenario: a major global brand finds itself embroiled in an embarrassing public incident involving an employee having accessed known Jihadist websites. In certain circumstances, companies can be found legally responsible for their employee's actions online.

Having an appropriate acceptable usage policy in place is essential. It's also worth considering putting in place a technology solution to prevent access to inappropriate content. Even if no legal penalty arises the reputational damage of an incident might well be significant.

Limitations of existing solutions

Most organizations today are completely unprepared for dealing with the coming avalanche of mobile data. This is surprising given the widespread adoption of **Mobile Device Management (MDM)** solutions and the investment by carriers in online billing analytics portals for enterprises. To understand why, we need a short detour into the world of carrier billing and MDM.

The vast majority of carrier billing systems predate the smartphone era. Adapting them to deal with the world of data and apps is an ongoing challenge for carriers worldwide. Their fundamental building block remains the “call detail record” which, as its name suggests, is based on the traditional telecom paradigm of a phone call. As a result, they have very limited ability to provide granular detail on data usage—most carriers will only provide you with a daily total of data consumed, split between domestic and roaming.

This data is often only made available on a monthly basis meaning, for instance, that you won't know about excessive roaming usage until many weeks after the event.



Most carriers only provide you with a daily total of data consumed

Mobile Data Management (MDM) as the name suggests, is aimed at the management of the device. It controls how the device is configured, can toggle on and off certain features and can remotely control certain aspects of the device. What MDM is not designed to do is manage the data the device consumes. This requires an entirely different solution—one that has visibility and control of the data flowing into and out of the device.

Traditional technical solutions, such as web proxies and internet gateways, are ill-equipped for the specific challenges that the rise of cloud computing and the IOS and Android operating systems have brought. At Corrata, we call this new capability **Enterprise Mobility Control**.

Enterprise Mobility Control

Enterprise Mobility Control refers to a technology solution that provides an organization with real-time visibility and control of the data traffic to and from its employees devices. Visibility should be possible on two levels: firstly real-time visibility of the volumes of traffic being consumed by enterprise mobile devices and secondly real-time visibility of the apps and websites generating this traffic. It should be possible to distinguish between cellular and Wi-Fi traffic, between tethered and non-tethered traffic, and between domestic and roaming traffic. Visibility provides benefits in a range of areas:

- ✓Employees can be provided with personalized and timely advice to help them minimize unnecessary usage.
- ✓The enterprise can be alerted to usage, which, if continued, will cause significant unnecessary cost.
- ✓Transparency around mobile data usage reinforces acceptable usage policies.
- ✓The ability to easily measure the adoption by employees of new productivity-enhancing applications deployed by the enterprise.

Control is the other element of an Enterprise Mobility Control solution. Control refers to the ability to enforce policies at the device level, and the ability to implement a set of rules to govern the use of a company-paid-for device at the employee level. Examples of specific controls include:

- ✓The ability to set limits on domestic and roaming data consumption.
- ✓The ability to whitelist critical business applications to ensure that access will never be restricted even where a data consumption limit has been hit.
- ✓The ability to restrict access to specific high bandwidth non business related applications.
- ✓The ability to block access to unsafe and inappropriate categories of content such as malicious sites, adult or gambling sites.

Enterprise Mobility Control contd.

By eliminating excessive non-business usage, these controls have obvious benefits: they reduce cost, eliminate bill shock, and simplify mobile cost control. Further, the cybersecurity benefit—with malicious sites being blocked—is also pretty obvious. But control also assists the employee by making it easy for them to avoid behavior not in line with their employer's acceptable use policy.



Corrata's Enterprise Mobility Control solution has three elements:

- An **employee app** to keep the employee informed about their usage and to measure data usage on the device.
- A **on device gateway** to enforce control over the data passing through the device.
- A cloud hosted **administration portal** for device enrolment, reporting and policy setting.

The Corrata solution is easy to deploy, is carrier independent and requires no integration with in-house systems.

Conclusion

The mobile device is today at the center of people's work and personal lives. For enterprises that provide their employees with devices, this presents new challenges. The abundance of apps and services for business, personal productivity, health and wellbeing, entertainment and lifestyle will drive massive growth in data volume and will inevitably expose organizations to new risks.



Corrata's solution is easy to deploy, is carrier independent and requires no integration with in-house systems.

Enterprises who fail to pay close attention to how their employees are using their company-provided phones are missing opportunities to reduce cost and to avoid unnecessary risk exposure. In the past, this might have been understandable due to the absence of suitable technical solutions for mobile platforms. Now, as the underlying platforms are maturing, robust, easy-to-deploy solutions are emerging. Perhaps it's time to take a closer look.

About Corrata

Corrata is a leader in Enterprise Mobility Control helping organizations manage the costs, risks and opportunities arising from their employees usage of mobile data and services. With deep expertise in wireless devices, networks and applications Corrata is ideally positioned to deliver the technologies that enterprises need to take advantage of the opportunities the combination of cloud and ubiquitous connectivity are creating.

The Corrata Mobility Control solution enables organizations to reduce risk, improve productivity and lower cost through real-time visibility and control of their employees use of mobile services.

Corrata is a private company and is headquartered in Dublin, Ireland

Contact
sales@corrata.com

Learn more
www.corrata.com



Dublin, Ireland
3rd Floor Block 3,
Blackrock Business Park,
Blackrock,
Co. Dublin, Ireland
Tel: +353 1 905 2943

London, UK
20-22 Wenlock Rd,
London,
N1 7GU
Tel: + 44 20 3287 2431

New York, USA
c/o Enterprise Ireland
345 Park Avenue,
17th Floor,
New York, NY, 10154
Tel: +1 917 5122 964