Executive Summary
This paper discusses the penetration of tablets in public sector and options that organizations are considering as they evolve their IT infrastructure to address new user needs in the world of mobile devices. Android-based tablets have a lot of obvious appeal considering low acquisition costs against tight public budgets. However, when judged against 4 areas critical to public sector and education - Ease of Use, Security, Productivity and Lifecycle - Android-based solutions fall short. An in-depth comparison shows that Windows devices are a superior choice, offering better security, a more productive experience for users and an improved ability for IT to manage mobile devices within the boundaries of existing PC cost structure and technical infrastructure.

Tablets in the Public Sector
The growth of smart mobile devices has impacted all sectors including governments and education. General policy initiatives to develop digital literacy, digital inclusion and deliver greater information access have led public sector leaders and institutions in both developed and emerging markets to search out ever cheaper devices. For many scenarios, the touch-centric user experience of the tablet offers an appealing and modern way for constituencies and especially a large number of young students to access the Web, communicate and work.

Android and the Public Sector
With the proliferation of devices, Android has now garnered the largest mobile OS share. The low hardware requirements for Android, the apparent lack of software royalty and the lack of a central governance body to maintain standards enabled OEMs to offer low cost devices with differentiated software experiences. These are often the same criteria which have made Android appealing to government and education deals – within a limited budget, on the surface, lower cost Android units should enable more people to benefit from 1:1 device programs. Additionally the goal of many governments is to foster “openness” and transparency, and thus the “open source” element of Android also holds tremendous political appeal.
Challenges and issues with Android

There are significant challenges and issues with Android in general which often get amplified with low cost Android device programs. While Google does release the core Android operating system source code as open source, free for anyone to use, the fact remains that many of the key apps that make an Android device useful (Gmail, Google Maps, YouTube, Google Play, etc.) are all proprietary to Google, and there is no blanket open license to use and redistribute that code. Google often designs these key first party apps and services for the latest hardware, and thus even if there are redistribution rights, they may not work well or at all the cost reduced hardware designed for 1:1 device programs.

Security issues are found all the time in software, in particular, the Linux kernel which is used by Android to get security patches and fixes on a regular basis, but Google and OEMs do not go back and update all older versions of Android (and devices) with those patches. More than half of the Android device installed base is still running Android 2.x or older, but those devices are no longer being supported by Google and the device manufacturers, leaving them vulnerable to security threats, old and new.

Even if Google were to update all older versions, there is no common, streamlined way to get those updates out to the install base of Android devices. That is because organizations who have adapted Google’s open source Android code have to sink engineering resources into each and every Android update. They need to test those changes against their code updates, and figure out a distribution mechanism to get software updates to the already deployed devices. This can be quite a complex chain when there are ODMs, OEMs, telcos and government entities involved in these 1:1 device deals and often Android OEMs skip updates or stop updating their less popular devices altogether, leaving users hanging.

Hence, the American Civil Liberties Union has recently filed a complaint with the Federal Trade Commission against major US telcos that Android users are woefully unprotected.

The open source nature of Android is touted by Google as a feature, not a bug, but the hackable nature of Android continues to leave big potential security holes. Most Android devices still feature a user selectable setting to allow installation of apps from unknown (unsigned) sources - enabling and encouraging third party app stores such as the Amazon (Android) App Market or various app stores offering pirated apps. However, this opening also enables malware, and with Android malware threats growing by over 30,000 over the last year alone, the security risks could be significant. As an example...
of how easy it may be to create and distribute Android malware, note that within 24 hours of Facebook releasing their “Home” apps (turning Android into a Facebook friends centric experience), the Android app packages (APKs) for Facebook Home were hacked and re-released to run on any Android device instead of the limited handful of devices that Facebook intended the apps to be used on.

Finally, it should be noted that a useful device running Android does contain IP of other companies besides Google, and thus in many parts of the world, Android cannot be used in devices royalty free.

**Windows tablets and Microsoft-based solutions v. Android**

The table below summarizes a comparison between Android and Windows based devices and how they map to the government and educational customer needs:

<table>
<thead>
<tr>
<th>Government and Education customer needs</th>
<th>What do tablets offer today?</th>
<th>Android Tablets</th>
<th>Windows devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ease of use</td>
<td>Convenience and mobility</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Connected</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>New incremental device great for content consumption</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Security &amp; Management</td>
<td>Security &amp; Safety</td>
<td>×</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Ease of Management and governance for IT department</td>
<td>×</td>
<td>✔️</td>
</tr>
<tr>
<td>Lower solution cost to help with budget pressure</td>
<td>Low Acquisition Cost</td>
<td>✔️</td>
<td>×</td>
</tr>
<tr>
<td></td>
<td>Lower solution cost during the lifecycle of the device</td>
<td>×</td>
<td>✔️</td>
</tr>
<tr>
<td>Productivity</td>
<td>Productivity and a familiar experience for the user</td>
<td>×</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Preserve integration with existing systems</td>
<td>×</td>
<td>✔️</td>
</tr>
<tr>
<td></td>
<td>Great integration across devices and apps (unified development deployment and management)</td>
<td>×</td>
<td>✔️</td>
</tr>
</tbody>
</table>

A more detailed analysis reveal important differences between Android and Windows devices on how well they meet customer needs:

**Ease of use** – enabling new ways of doing things is a major draw to mobile devices and tablets in particular. Both Android and Windows tablets cater to convenience, mobility and connectivity and are great for content consumption and light use, the Windows tablets are designed to do far more, offering:

1. An engaging, **first-in-class user experience and familiar software tools** that are ubiquitious in the workplace.
2. Wide **choice** of manufacturers, form factors, styles, and price points for every need;
3. A **seamless experience across devices**, allowing users to collaborate, store and share their work through SkyDrive/SkyDrive Pro from any web-capable device, sharing apps and settings for a single user across multiple devices,
Security & Management – Government and Education institutions alike are facing major public scrutiny whenever confidential/private information is accessed without authorization or leaks out. Many citizens, particularly parents, are expressing serious privacy concerns regarding what data is stored where and how it is used. The security challenges to Android platform are increasing at a phenomenal rate. Malware is a significant concern due to users having access to Android apps from Google Play and 3rd party app stores. In the case of Google Play, the app store does not pre-screen apps, thus malware can get on a number of devices before the app is reviewed and revoked. There are many 3rd party app stores for Android, and users can choose to allow unverified apps from these app stores on their devices, further increasing the malware risk to the organization and giving IT yet another major headache. These risks are augmented especially in emerging markets, where Google Play is not available and rogue apps are not generally revoked.

To make things worse, the process to get security updates for Android tablets is complicated and fragmented, relying on OEMs and/or telcos to manage security updates for their devices, which makes it difficult to deal swiftly with identified security threats. Even Google issued updates are following a long process until they get to the devices due to the need for OEM integration and testing.

By contrast, Microsoft’s Windows-based devices
1. Rely on a platform with built-in multi-layered security with Windows Defender, Windows Firewall, and Windows SmartScreen
2. Offer both offline and online service deployment options, giving IT better internal controls to safeguard privacy and effectively stop malware from spreading
3. ALL receive timely security updates via a streamlined process that is time tested.
4. Use app sandboxing, vetted security industry standards (TPM, UEFI, EHD) and leverage BitLocker* keys for IT-controlled recovery process (Windows 8 Pro only) or to encrypt data on a USB drive when critical data leaves the device (note: x86 devices only).
5. Use apps that were prescreened and vetted by Microsoft Store (similar process as Apple), providing solid additional protection against malware.

ALL Windows devices receive timely automatic updates via streamlined process that is time tested.

99% of all mobile threats target Android devices

Kaspersky 2012 Security Report

Deploying and managing tablets in addition to the existing PCs poses new challenges for the busy IT managers of many government and education institutions. It is important to compare how easily devices can be managed and the degree to which IT can enforce organization standards and policies.
Android tablets lend themselves to only light management using 3rd party Mobile Device Management solutions. By contrast, Windows devices are part of a comprehensive Microsoft solution focused on reducing client management infrastructure costs and complexity.

The Microsoft device management solution offers:

1. **A single console** for both security (identify and remediate both threats and non-compliance) and client management (unified settings and inventory management).
2. **Integration with solid and long tested technologies** that the IT managers are familiar with, like Active Directory, Domain/Group Policy and Windows Server.
3. **Flexible options to deploy** personal/pooled virtual desktops and applications using Windows Server 2012 Remote Desktop Services (RDS), providing users a high-quality graphical and audio experience even in less than ideal network conditions.

Lower solution cost to help with budget pressure—solution cost is a major topic for all organizations, and an especially important one for budget driven institutions like the Government and Education institutions. While Android devices have lower acquisition cost, with prices seemingly declining further every year, the lowest cost devices most often don’t meet the needs and expectations of most organizations. Buyers who are initially tempted by the low price quickly become **dissatisfied with the experience** (touch inaccuracy, display lag, inability to run applications). A great example is the Aakash tablet, which repeatedly **failed to deliver to expectations of the Education customers in India**, despite strong commitment and support from the Indian government.

Most important, no matter how low the Android device acquisition cost is, the solution cost for the lifecycle of the Android device will look quite different in the end, as there are many other costs that are likely to incur during the lifecycle of the device. Any project will have costs associated with planning & deployment, costs related to secure information, risk management and software updates, training costs and costs associated with transferring the device to another user.

Solution cost during the lifecycle of the device is exactly why Windows devices are so competitive in the enterprise: the adoption of Windows devices is likely to follow closely the existing cost structure for PCs and in some cases it even produces savings as no new processes need to be developed, and PC-based devices have a strong track record of providing long-lived solutions, while mobile phone-based consumer technologies such as Android are often obsolete in 2 years.

No matter how low the Android device acquisition cost is, the solution cost for the lifecycle of the Android device will look quite different in the end...
Productivity - While both Android and Windows based tablets may be viable for casual gaming and browsing, Android tablets fail for many real productivity scenarios. They don’t integrate well into either home or work environments, often running into issues while connecting to existing devices, such as printers.

Android tablet makers have created enhancements and customizations on top of Android to suit their needs. But this flexibility comes with a steep cost due to Google’s inability to curtail Android’s massive fragmentation. Android devices often require new code to be written to make them work with the existing applications and app developers are forced to choose which version of the OS to write for. They must choose whether to use the latest APIs and test across all versions or stick with older, proven APIs and not take advantage of the latest and the greatest features that were just released. For Government and Education institutions, where software development cycles tend to be longer, such choices can lead to wide disparities in app support and user experiences, amplifying the risk for a program failure, especially considering the short lifecycle of each version of Android with limited upgrade opportunities.

Windows devices take user productivity to a new level with:
1. **Unique capabilities** like the Snap feature (side-by-side multitasking), accurate stylus input and multiple displays support.
2. **Microsoft Office (sold separately)**, which enables users to create and edit documents with confidence, both offline and online (using free web-based companions to Microsoft Office) and share them with anyone using SkyDrive.
3. **Great integration across devices and apps**, with unified development, deployment and management. Developers can leverage a wide choice of languages to choose from (C/C++, C#/VB, and HTML5/JavaScript) as well as powerful tools like Visual Studio, enabling them to write solid applications offering users the same great experience on notebook, tablet, AIO and wall screens.

![Quickoffice on Android vs PowerPoint on Windows RT](image)
Conclusion

The lower cost Android devices are hardly the answer for Government and Education institutions looking to deploy the right solutions for their needs, as they offer little beyond the low initial cost of acquisition. By comparison, Windows devices offer better security and utility, enabling new usage models AND more productive users, while giving IT flexible deployment options to evolve the existing infrastructure and in some cases even produce savings as no new processes need to be developed.
References:
1. TechRepublic: “10 things I hate about developing for Android (and some workarounds that help)”, Aug 2011
3. CVE Details, May 2013 – Linux kernel vulnerability statistics
4. V3.co.uk, May 2013 – “Google Android malware levels rocket as spam threats grow”
5. AndroidCentral, May 2013 – “Why you’ll never have the latest version of Android”
8. ExtremeTech, Dec 2011 – “Why OEMs need months to deliver Android updates to your phone”
10. ACLU.org, April 2013 – “ACLU Files FTC Complaint Over Android Smartphone Security”
12. McAfee, Jan 2013 - “McAfee Threats Report, Q4 2012”
13. Unleashthephones.com, April 2013 – “Facebook Home hacked to work on (almost) any Android device”
17. NTDV Gadgets, April 2012 – “Micromax Funbook review”
18. LiveMint & Wall Street Journal, Mar 2013 – “Government close to giving up on Aakash project”
22. PocketNow.com, May 2013 – “The Surface Pro is Now an Artist’s Dream Tablet”

(c) 2013 Microsoft Corporation. All rights reserved. This document is provided “as-is.” Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. This
document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.