As consumers embrace mobile technology, more businesses have had to address the issue of employees accessing corporate data on their personal mobile computers and smartphones. While allowing the use of these individual-liable (as opposed to corporate-liable) devices could help improve productivity and reduce costs, they present challenges. MDM software helps enterprise IT departments manage personal and company-owned devices and their operating platforms. According to an Aberdeen survey on wireless expense management, 72% of responding companies allowed some level of individual-liable device use. On average, 23% of devices within these companies were individual-liable.

Some companies resist allowing individual-liable device usage because of the IT headaches it can cause. “We are seeing customers allow them for certain applications or ban them because they’re not ready and not prepared to support the devices,” says Joe Granda, executive vice president of marketing at Syclo. The biggest drivers for companies that do allow individual-liable devices are employee requests and cost savings.

The biggest challenge in allowing this is ensuring data encryption and segregating personal from professional data on the device. “Most will allow individual-liable devices, given a few constraints,” says Khoi Nguyen, group product manager for mobile security at Symantec. “For example, organizations will require that these devices utilize encryption, that they not be jailbroken, and that they support certain basic security settings. Advanced organizations will use solutions that manage and secure the corporate data while leaving the personal data separate.”

Individual-Liable Mobile Devices: Benefits And Challenges
An advantage for employees in an individual-liable scenario is they have more control over the type of device they carry. For example, employees who prefer an iPhone to a BlackBerry can access corporate information as well as personal information, contacts, and applications from the device they choose. Cost reduction can be another benefit, since companies don’t have to purchase devices or manage operating platform upgrades and can save on maintenance/support and taxes. “Allowing employees to use the same device for personal use, business use, and for accessing entertainment and carrier-provided services can provide increased productivity because employees are typically proficient with the technology,” says Nguyen.

However, while the potential savings are attractive, there are issues with managing individual-liable devices in the enterprise — not the least of which is ensuring that the devices are secure and the data encrypted. On top of that, IT departments may have difficulty managing and updating the wide variety of mobile computer and smartphone platforms available in the consumer market. “Most smartphones are designed for the consumer,” says Oscar Rambaldini, director of product development at SOTI. “This is a compromise to the business value of individual-liable devices as the enterprise is unable to ascertain ultimate control and security. With many smartphones, employees can choose among different devices, so managing the diversity is a challenge.”

You must also consider cost differences in supporting a corporate- and individual-liable device that could impact TCO (total cost of ownership). According to Aberdeen’s research, a personal device averages $92 in direct costs...
and processing costs, while corporate devices average $89 per month.

The operating system can also limit IT’s ability to manage smartphones because some platforms provide limited third-party MDM functionality. “Each mobile device platform [e.g. iOS vs. Android] and specific manufacturer [e.g. HTC Incredible vs. Motorola Droid] vary in the device management functions that can be performed due to the limitations of the mobile platform itself,” says Mark Gentile, CEO of Odyssey Software. “This requires the enterprise to evaluate each mobile platform and/or device to determine if it will meet their requirements.”

MDM Software Integrates Personal Devices

MDM solutions providers are working to expand their support. “MDM solutions are the necessary tool for IT departments to successfully include personal devices in the business network,” Rambaldini says. “New MDM features catered specifically to support smartphone operating systems address security concerns and offer simple methods of deploying secure corporate applications.”

When selecting an MDM solution, Granda cautions users to be aware of the difference between cross-platform and multiplatform MDM solutions. “Multiplatform systems mean you can run it on a bunch of different devices,” Granda says. “Cross-platform means that anytime there is a change to the devices, you can make that change on the server, and it cascades down to the users.”

MDM functionality may be limited by the operating platform, so keep that in mind when evaluating employee-owned devices. “Remote wipe and lock commands are feasible for today’s popular smartphones with MDM solutions,” Rambaldini says. “However, smartphone operating systems limit the extent of remote control fueled by the consumer’s best interests, not the enterprise’s.”

For billing, companies will generally compensate employees for a portion of their monthly bill, but this varies. “Companies want to minimize roaming charges — especially for data plans — so they will enforce MDM policies on devices, such as requiring manual sync while employees are roaming,” Gentile says.

With an effective MDM solution and well thought-out corporate policies, personal devices can be integrated into an enterprise mobile strategy. Companies must carefully weigh the potential costs and benefits to ensure that total cost of ownership is not adversely affected and end users are comfortable with the established policies.