COPE or BYOD? Mobile Communication Device Ownership Options for Fleets

The proliferation of advanced communications and computing devices and applications for personal use is driving the debate over device ownership and the "right" model for Transportation companies. The questions of whether employees should be allowed to connect their personally owned devices to the company network or whether employees should be allowed to use company-owned devices for personal as well as business use have made device ownership a sensitive issue. This on top of security, privacy, cost and supportability issues gives fleet owners plenty to think about when selecting mobile technology. This blue paper examines the issue from a fleet's perspective to help you determine the right path for your mobile workforce.

Evolution of Mobility Options: BYOD and COPE

Historically, fleets have opted for fleet managed or "Corporate Owned, Corporately Enabled" devices, which offers little to no choice to users but maintains control for the fleet. The company owns the communication device and does not allow incorporation of personal applications on it. As a result, this model provides the highest levels of support, security and compliance.

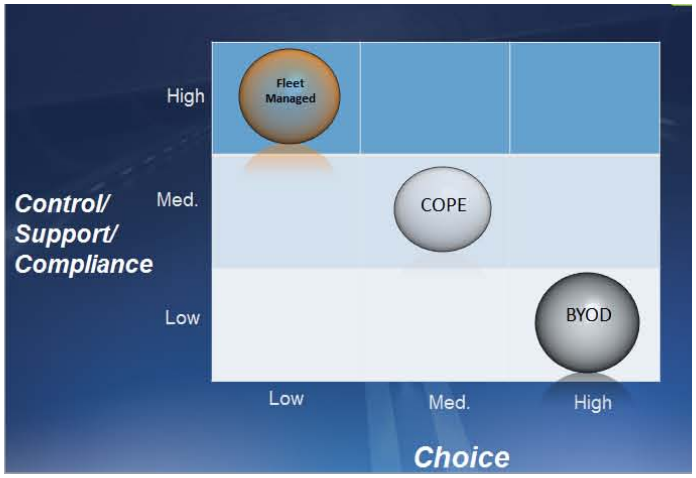
BYOD (Bring Your Own Device) refers to employees bringing their own computing devices—smartphones, laptops, tablets, and other PDAs—to the workplace for use and connectivity on the corporate network. BYOD affords end-users their choice of devices, programs, and services that best meet their personal and business needs.

The continuous stream of innovative consumer devices and services make BYOD attractive to end-users. The company IT department provides device support and security. While IT departments initially buoyed the concept to shift the burden and expense of hardware ownership (and replacement) to their internal customers, IT has come to appreciate how onerous it can be to deal with an infinite variety of platforms and profiles, hardware and security issues (See Management Perspectives). It is the classic tradeoff between choice and complexity. How far should companies and fleets go?

As a result, IT is rethinking BYOD and reshaping it with COPE (Corporate Owned, Personally Enabled) policies. Instead of making corporate functions work on personal devices, COPE sets up a framework to support and allow personal uses of company devices. The company selects preferred devices, buys and owns them, but the employee is allowed, within reason, to install the applications they want on the device. The company also establishes usage and cost thresholds for employees.

Most important, in a COPE environment, the company reserves the right to disconnect devices on the corporate network when necessary (as in the case of a security breach) to keep their networks and information secure, one of the biggest issues associated with BYOD programs.

COPE Vs. BYOD Tradeoffs



Issues to consider

Data Security and Privacy

Security is the most critical issue facing IT when personally owned smartphones and mobile devices are connected to the company network under BYOD. If employees are allowed to use their own mobile devices at work, the network is exposed to security risks that include but are not limited to:

- Confidentiality of proprietary information: Multiple unauthorized individuals (family, friends, strangers who find a phone left at a truck stop) may use employee-owned devices, exposing information to breaches that the company will never even learn about until the data on them has been misused.
- Customer liability due to loss or improper use of personally identifiable information found in email, documents, phone calls, text messages.
- Data and network integrity risks due to malware and jail-broken devices
- Human Resources issues (surfing inappropriate websites within the enterprise campus or cab)
- Erosion of public image, market status
- Risk and cost of non-compliance

How does the company secure information on a device that it doesn't own since the law may limit what a company can do to help itself? A well-defined security policy should clearly outline the company's position and governance to help IT better manage these devices to mitigate network compromise, including:

- Detailed security requirements for each type of personal device used in the workplace and connected to the corporate network
- Configuration passwords
- Approved applications
- Encryption requirements for all data on the device
- Activity limits at work (e.g. email usage only on corporate accounts)
- Periodic IT audits to ensure devices comply with BYOD security policy
- Data storage and access to data in a cloud-based virtual desktop or profile
- An employee-signed agreement that allows the company to disconnect the device when policy is violated or when suspicious activity is detected

Costs
Under BYOD, employees buy and expense the mobile devices and services they need. The employer may choose to reimburse all or a portion of these costs (at retail prices). With technology advancing at a frenetic pace, BYOD could be onerous for employees since they would be expected to have devices that support EOBR advancements and a growing number of sophisticated applications. In addition, wireless carriers are reversing their position on deep discounts for cell phones. Additionally, BYOD has significant cost risks for employees that may end up going into data overages driven by their personal applications, company applications or a combination of both. Sorting out the root cause of these overages can be nearly impossible.

What's more, the total cost of ownership rises with each mishap—when a phone is lost, stolen or breaks. COPE not only helps companies keep their corporate discounts, but also alleviates their employees' financial commitment.

In addition to lowering device acquisition cost, COPE helps companies score better deals on EOBR application fees and data plan costs for mobile devices for more cost-effective usage. From a savings perspective, BYOD may save on capital expenditures (computers, phones, tablets), but COPE saves far more in operational expenditures (IT, training, support, etc.). The cost of administration between BYOD and COPE is reflected in keeping track of a plethora of BYOD devices vs. a few under COPE. Under BYOD, a company could be forced to engage third-party support vendors, which could erode security.

Certification/Standards/Upgrades
With so many cell phones on the market and the typical phone life cycle being 9-12 months, managing and updating the procurement list of certified consumer phones that meet company standards is an endless, time-consuming task under BYOD. What's more, the constant stream of new models makes it extremely difficult for the fleet to create a road map for evolving and upgrading its technological capabilities.

When a driver loses a smartphone or it breaks, the latest model will likely be the most attractive since models are typically not supported after 12 months. Timing is everything and if the latest/greatest model has just come out, it is likely that the company may have not have had enough time to certify that the model meets company standards. What if the EOBR provider hasn't certified the latest model? In this scenario, the company's policy may delay the driver's purchase, which would impede his/her productivity as well as cause information gaps in workflow. Also, when on the road without a smartphone, a driver won't be happy about reverting to paper logs in order to comply with HOS regulations.

Personal Control
Users may prefer BYOD because they have the power to choose their device, and they own it. Therefore, the business can no longer simply wipe anything (and everything) from the device since there are laws protecting the employee from that sort of thing. Ownership and control empower users. They have not been forced to use a specific device and have a choice about how they engage with technology in order to conduct their job function.

This choice has a downside. If a driver powers down a mobile device (intentionally or unintentionally), they put a plug in the workflow, such as getting them to a hot load or requesting an HOS update for dispatch? The desire to control technology devices is especially prevalent among GenY-ers. How can IT co-exist with this attitude? The PE (personally enabled) aspect of COPE can allow employees to choose their company-owned devices from a predetermined list and allow them to use those devices both professionally and personally.

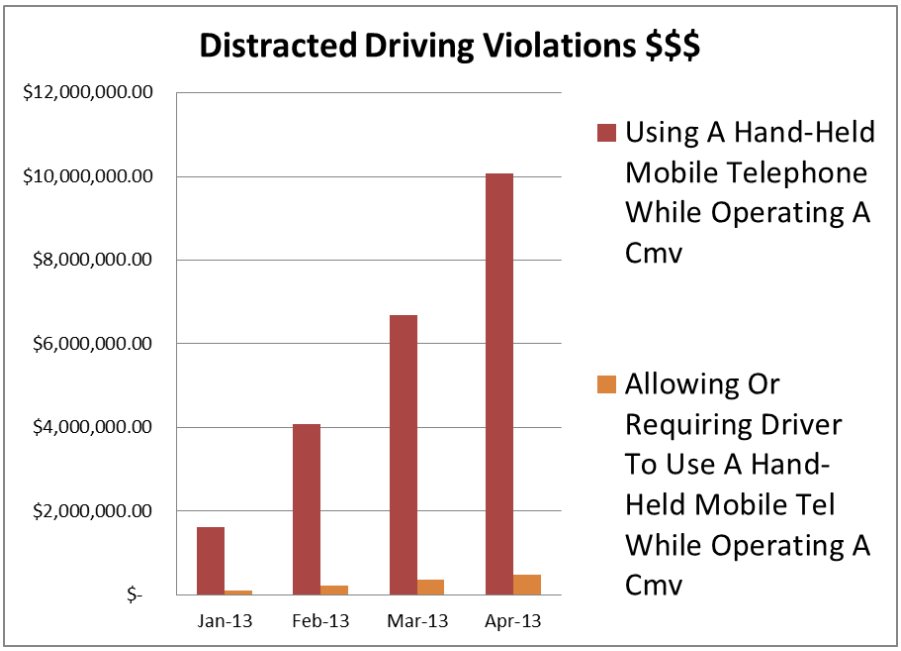
Safety
Consideration for employee safety and the many others who share our roadways always plays a big part in making this type of decision. Not only do you have to look at the device itself and the ease of use, but also what the driver will be using it for while the vehicle is moving.

Considering the number of accidents related to distracted driving while using a handheld mobile phone and the recent ban on cell phones nationwide for commercial drivers, a company must review the possibility of the additional risk and exposure to liability. Fixed mounted devices that can be configured to the functionality they have while the vehicle is moving has positives for company and driver alike. There is currently no ban on this type of technology. Furthermore, the COPE model allows for more extensive control on distracted driving tools while BYOD creates a barrier to mandating these types of tools.

The financial exposure to a serious commercial vehicle accident is at an all-time high. Even though the industry is experiencing the lowest fatality rate in 20 years, the cost associated with a fatal collision has doubled over the last five years to over $7.2 million per incident. This dramatic increase is due primarily to punitive damages when it is proven that the driver, carrier or both were negligent. This could include the choice of technology by the carrier and what the driver was doing with the device at the time of the accident.

In addition to the safety concern, it is now illegal to use a cell phone while moving in a commercial vehicle unless it can be done with a single touch and hands free. The violations being issued for this can cost a driver up to $2,750.00, and repeated offenses can result in the loss of their license. Carriers can also be found in violation by "requiring or allowing" their drivers to use a cell phone. This type of violation can cost a carrier up to $11,000.00 per occurrence. In 2012 almost 7,000 driver violations were issued and 168 to carriers. 2013 is currently exceeding that pace through first quarter. In fact driver use violation is now ranked 20th in driver violations issued to drivers during inspections. This violation and speeding are generally the reason a driver gets pulled over for an inspection in the first place. Under CSA, the cell phone violation carries the maximum point value of 10, ranked equal to a reckless driving violation.

These and many others safety-related facts must be weighed in this very important decision process. They are also integral to building a culture of safety that carrier and driver can be proud of.



Source for all safety-related charts: Federal Motor Carrier Safety Administration

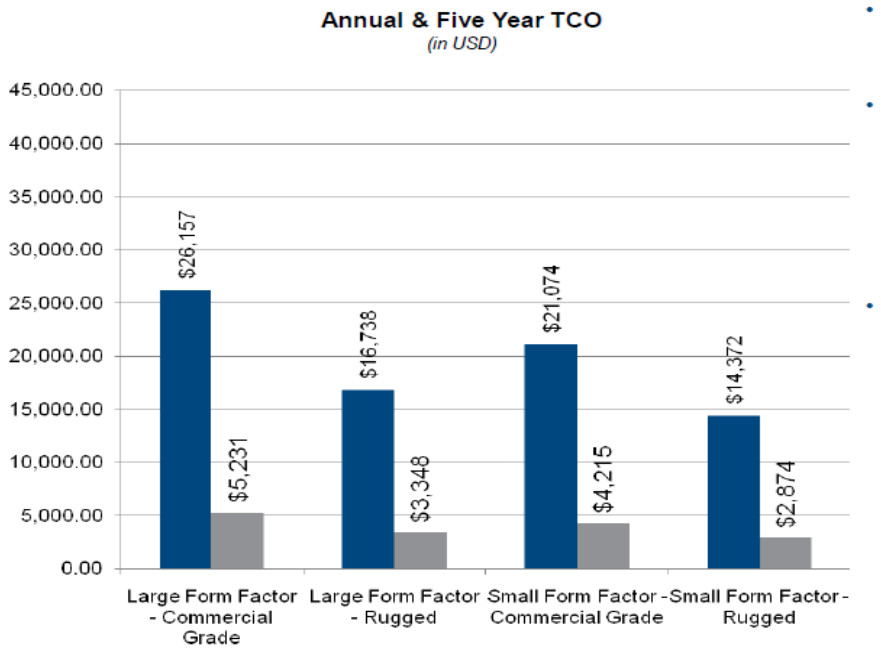
In the first four months of 2013 alone, carriers and drivers have been fined more than 10 million dollars for using a handheld mobile telephone while operating a vehicle or requiring/allowing drivers to do the same. Fines include 43 carrier violations and 3,662 driver violations.

Support
Consumer-grade mobile phone releases occur on average every six months, making a BYOD model extremely difficult and costly to keep up and requiring the additional costs of driver training and technical support. The issue is compounded for fleets in which multiple makes and models of phones are being used. Updating each with the company's latest software code would be an onerous task.

In addition to updates, the fleet would have to continually update an approved list of devices that the company has certified to run their applications. With hundreds of different phones and models and tablet devices on the market today, keeping the certified list current is a time-consuming proposition.

Another potentially time-consuming area to consider is obtaining outside support for problems. Consumer-grade mobile devices without an operating system lack important enterprise tools for streamlined support. Instead of having "one neck to grab" in the case of a single provider of network, software and hardware, the issue may require multiple contacts. For instance, if an application doesn't work, do you call the software or hardware vendor? Support issues have the potential to escalate into a frustrating finger-pointing duel.

Durability
Anyone who has ridden in the cab of a truck knows better and understands that in-cab devices need to withstand the harsh environment inside the cab as well as external elements. It's a gamble to assume that phones will survive plummets to the cab floor, the ground, a puddle, or snow. Studies have shown a significant reduction in total cost of ownership through the use of rugged devices vs. commercial grade devices. This difference goes up further with consumer grade devices in the trucking environment.



Source: VDC Research

The Dope on COPE
Outsourcing wireless mobility management (WMM) helps IT departments seamlessly roll out a COPE program. COPE offers the feel of a BYOD policy, and actually gives employees the opportunity to customize their device selection and data plan (to accommodate personal use) within the IT budget. The added perk for employees is the support system and help from their IT departments and mobile device management (MDM) or WMM representatives (if a company contracts one).

By embracing COPE, IT can reassert the control that it must have to keep data and work processes secure, while still giving employees the shiny toys they so desperately want. Plus, employers have greater control over costs and preferences that lead to productivity gain for employees.

Finally, COPE provides management a proactive, organized approach for planning the adoption of technology vs. a reactive, at hoc approach that thrusts the company into technology whether or not it's prepared for the latest advancement.

Getting to COPE
The company determines a list of acceptable devices for users to select from, and buys the chosen devices. The company's usage policy may include limits for personal usage. The device remains the property of the business throughout its use cycle, which is determined by the company.

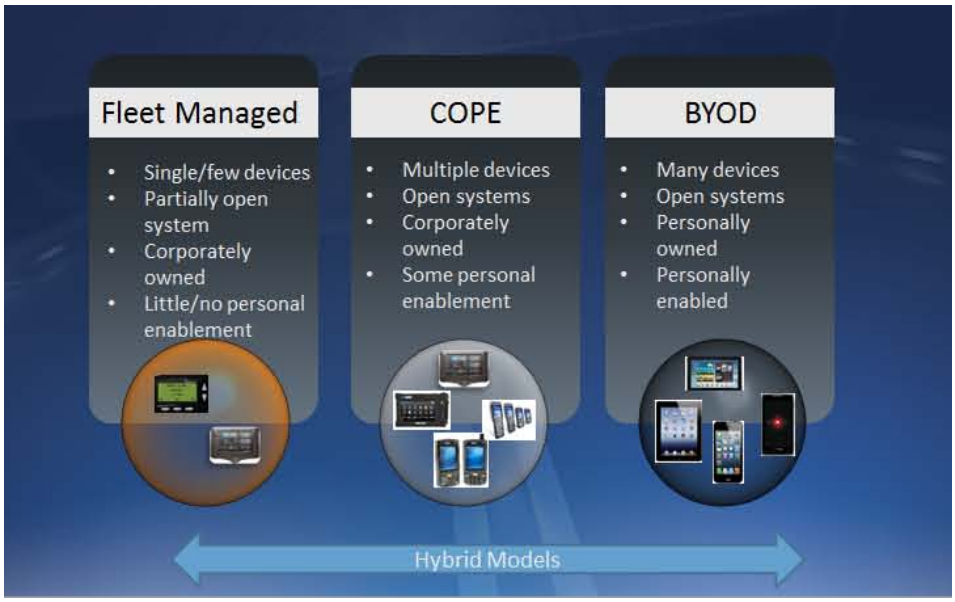
Personal usage can be as simple as email or can lead to more extensive use such as web browsing or personal applications. While users may select applications for personal use, these apps should not be allowed to interact with corporate data. Should the app be found to fly in the face of security or usage policies, the company has the right to remove the app.

Driver Privacy
BYOD may be a moot issue for fleets. When a fleet provides drivers mobile communications devices, drivers may want to carry an additional smartphone for personal use. First of all, not everybody wants to use their personal telephone number for business purposes due to privacy. Secondly, drivers will most likely want to retain their personal telephone number and information should they leave the company. Since the telephone number in the company-owned device belongs to the company, the driver would have to notify their contact base of a number change.

Management Perspectives
Mobile communication is the lifeline between drivers and operations. Without device reliability and durability, the flow of real-time information throughout the operation is at risk. While it might be tempting to use consumer mobile devices for keeping your organization connected, fleets must keep in mind that there is a chasm between consumer and commercial devices and industry-specific applications. Lightweight, portable phones and tablets are not practical alternatives to commercial-grade fleet mobility solutions offered in a COPE model.

Another practical solution to the device ownership dilemma is a hybrid model. This approach combines a BYOD regarding the driver's personal applications with COPE for fleet managed, compliance- and mission-critical applications. This hybrid model would eliminate security risk associated with inadvertent deletion of a fleet's proprietary data from a personally owned smart device. It also allows fleets to control their flow of critical information (dispatch, regulatory) to and from drivers without risks noted above in a BYOD model.

Mobility Options Summary



In Summary
Selection and ownership of mobile communications devices is a balancing act in which your mobile workforce's business and personal needs should be considered along with company objectives for efficient, cost-effective management. Understanding all the issues and their ramifications is critical for creating a model that works for your fleet.

Published by:
PeopleNet
4400 Baker Road
Minnetonka, MN 55343
888-346-3486

www.peoplenetonline.com
info@peoplenetonline.com