DOES BRING YOUR OWN DEVICE DESTROY YOUR TRADE SECRET/CONFIDENTIALITY/AND NON-SOLICITATION PROTECTIONS?

By
Bob Gregg
Boardman & Clark Law Firm
P.O. Box 927
Madison, WI 53701-0927
608-283-1751
rgregg@boardmanlawfirm.com

BYOD means Bring Your Own (Electronic) Device (I-phone, laptops, tablets, etc.) to work, and then use it for the organization's business purposes. These uses include standard internal and external business calls, texts, emails, and social networking with clients, vendors, professional associations as part of the organization's public presence and promotional efforts.

More and more organizations are not only allowing this. Many are encouraging it, and a growing number are requiring it – preferring to save money on equipment, and reimburse employees for their own device use.

In surveys some 78% of employees state that they use their own devices for their organization's business purposes.

This obviously creates security, confidentiality, privacy and electronic retrieval issues (especially regarding former employees). However, one of the major Intellectual Property issues raised is trade secrets. Does allowing use of BYOD jeopardize trade secret or confidential information protection? Do we need to have additional policies or agreements on this issue? Can any policy or agreement give adequate protection?

Employers devote great effort to protection of trade secrets, confidential information, customer contacts, and non-compete/non-solicitation policies and agreements. Once the employment ends, all information is supposed to be returned, not revealed, and no customers contacted. Can the employer really expect this when the information is now on the former employee's personal device, personal cloud storage, personal hard drive? The device is the former employee's personal property. It may be hard to claim that the electronic contents are also not now that employee's property.

The Uniform Trade Secrets Act prohibits "misappropriation" of trade secrets. It generally defines a violation as use or disclosure by "improper means." Once we give employees access to secrets on their personal devices, then have they obtained this by "improper means?" The company allowed – encouraged – the employee to store the information on their personal devices, personal servers, personal cloud.

The employer required the employee to create a presence on various social media sites. Does the employee's profile belong to the company – or is it personal? Do former employees violate the non-compete – non-solicitation agreement when they update their personal social media profile, on their personal devices, letting everyone know what competitor they went to and what they have to offer?

It may be difficult to claim that the former employee's social media customer contacts were "purely business", and not of a social/friendship nature. Purely business contacts can more easily be protected even on the employee's personal device. However, content of a personal social nature blurs the issue and creates a serious problem in protecting or prohibiting future customer or vender contacts. Personal communication on one's BYOD can possibly gut an employer's claim of trade secret/confidential information violations.

Most companies actively encourage sales people and others to "connect" with customers and "build relationships." This routinely involves personal communication – not just business. The sales people "connect" over family issues, sports interest, vacation details, etc. A customer sends out a new baby announcement. Most companies expect their sales people to goo-goo (excessively) over the new arrival, and all the personal details. Personal connection cements the customer, and sells. However if your sales person gives the "purely business" response to the new baby message with, "Nice! We are now offering a 10% discount on all orders over $10,000! What would you like to order?" Which sales person will make the future sales?

In post-employment you cannot prohibit the employee from using the contact information to stay in touch with "personal friends".

If the communications are on the organization's own electronic devices, then all contents, and contacts are property of the organization. The organization can control usage, prohibit any transfer or retention of information, and enforce its ownership regarding later post-employment usage. The organization has the right to monitor usage, enforce security and seize the device at any time. Not so with BYOD.

If you are concerned with protection of information, trade secrets, intellectual property, and non-competition, then BYOD may be an unwise practice. You should be consulting with your IT professionals and legal counsel. This article only addresses the narrow issue of trade secrets, confidential information and non-solicitation areas of concern. There are many more possible areas of concern.

If you have any level of BYOD in your organization you should be consulting with these same people about developing policies and specific BYOD use agreements which give you as much protection and post-employment enforcement and protection as possible. Clear policies and agreements are becoming a major issue.