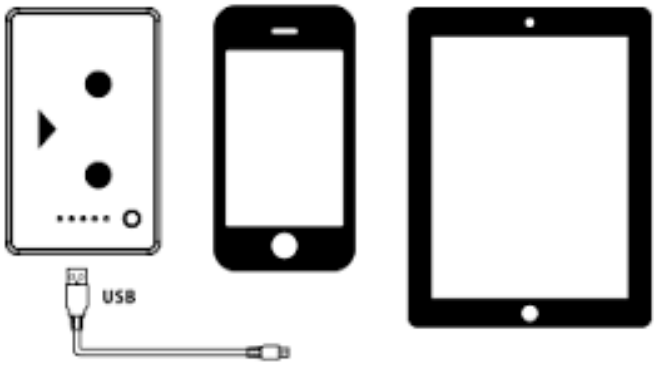
Bring Your Own Device (BYOD)

Legal Issues Surrounding the Use of Personal Electronic Devices for Work



Gary Eisenstat
Figari & Davenport, LLP
gary.eisenstat@figdav.com

TABLE OF CONTENTS

I. INTRODUCTION

Recent innovations in cloud and mobile computing technology have created unprecedented efficiencies in the work place. Employees can now communicate and work remotely, collaborate on projects from various locations, and use multiple electronic devices to access the same materials, all with just a cell phone or wireless internet connection. These technological advancements allow unprecedented work flexibilities and cost savings, and have helped increase profitability. However, they also create new practical and legal problems. The lines between personal and company time and property are increasingly blurred, often pitting individual and corporate rights directly against one another.

While not meant to address every issue that might arise from these technological changes, this paper will identify potential problem areas to consider and monitor. It will also suggest best practices for drafting policies and enforcing work rules regarding the use of personal devices for work, and highlight some of the legal and practical concerns that arise when employees can remotely access company information remotely or from multiple devices.

II. PROTECTING COMPANY AND CUSTOMER INFORMATION

Operating in a digital environment, today's companies face increased challenges in guarding both their confidential and trade secret information and securing their customer data from unauthorized access, use, or disclosure, by both current and departing employees and outsiders. A variety of typical scenarios can quickly spell disaster.

A. Lost or Stolen Devices. A current employee routinely uses her personal smart phone, tablet, or laptop for work emails and projects or to access company or customer information. The device is lost or stolen but is not password protected. Equally plausible, a family member innocently uses or loses the personal device,

which is now subject to unauthorized access. In either case, the company's data and customer information are now at risk. The data could be accessed illegally and then used for improper purposes. Company computer systems could also be hacked, causing massive damages, triggering reporting obligations, and resulting in a financial or public relations disaster.

B. **Terminated Employees.** Just as likely, a disgruntled employee quits or is fired, but not before accessing the company's network or information through a personal device. Absent an agreement with (or prompt action by) the company, a court order, or voluntary compliance by the terminated employee, an employer may have little opportunity to determine what items the terminated employee may accessed or copied onto their device or another storage device. Often, the only way to determine what has been accessed or copied is through a forensic examination of the phone, computer, or tablet. Company or customer information could have been copied and stored onto an external drive or a cloud account, such as a Google drive, an iCloud account, or a Dropbox account. Although a digital "fingerprint" likely exists, getting access to it could become a huge and expensive challenge.

C. **Wiping the Device.** If the company has the technical ability to do so, it might elect to remotely wipe the device and restore it to the original factory settings. However, doing so can create a conflict between the employee and the

Title search: Bring Your Own Device (BYOD): Legal Issues Surrounding the Use of Personal Electronic Devices for Work

First appeared as part of the conference materials for the
37th Annual Corporate Counsel Institute session
"Bring Your Own Device (BYOD): Enhancing Employee Productivity or Inviting Problems?"