Our fast evolving world has graduated from analog devices such as telephones with cords, snail mail, and couriers to devices such as smart phones, email and other digital technology. Such innovative advances benefited businesses by increasing productivity and organization. While the positive side of a digital world is well appreciated, the potential legal traps facing employers are well articulated in *Smart Policies for Workplace Technologies*, by Lisa Guerin.¹

The book is a guide for employers on how to prevent issues involving various types of technology in the workplace. Among the risks are potential lawsuits resulting from privacy infringements, discipline, Internet and email use during company hours, and activity on social media. Attorney Guerin’s book emphasizes the importance of drafting technology policies at the office. Some of the major reasons for drafting technology policies are the protection of business assets, preservation of employee privacy rights, maintaining organizational efficiency and the management of electronic documents.

According to the author, digital technology poses a substantial and troubling risk because of employer liability for employee conduct. Currently, employers use technology to try and solve undesirable employee technology use, i.e. setting up spam filters, blocking non-work related

---

¹ Lisa Guerin, editor of Nolo, specializes in employment law. She has practiced employment law in both government and private sectors. She is a graduate of Boalt Hall School of Law at the University of California Berkeley.
websites and setting up email controls that prevent the sending of large files. However, the author cautions that most employees are savvy enough to implement work-arounds to employer controls. Therefore, an express handbook of policies is more desirable because it sets boundaries for the use of such digital technology and protects the employer and employee from legal injury.

The handbook should address protection of business assets, informing the employee of the scope and nature of the company’s trade secrets. In the event that an employee steals this type of intangible asset, the employer can show that it took initiative to protect this information by having the employee read and sign the handbook. The importance of an employer drafting technology policies is also important when a company needs to protect itself from former employees as well. The author makes this point by providing a real life story about a married couple who were both terminated from the same company and shortly thereafter were accused of using their former employer’s trade secrets and customer lists. The company prevailed in the suit mainly because it was able to provide evidence through a showing of its company policy that defined the defendants’ conduct as unauthorized.2

Customer and employee privacy is also a major concern. Most companies will house sensitive information about employees in the form of Social Security numbers or documents pertaining to medical history. The employer is obliged to exercise reasonable care for this information and the employee should know of its employer’s course of action should a leak of the employee’s information occur. A handbook of policies can also be a place to outline the basis of termination and discipline of employees. In the event of a lawsuit by the employee alleging wrongful termination or unfair treatment involving technology, the company could argue that their policies put the employee on notice and carefully followed steps of discipline set out in the

---

2 See Guerin, infra note 4, at 9 (noting defendants terminated for refusing to sign non-compete agreement therefore providing written policies as crucial for employer).
handbook. Furthermore, employees should be made aware that communication through the use of company issued devices or servers is not private. Privacy is based on what the employee reasonable expected. To this point, a handbook serves to notify the employee of what communication is private and that the company may read emails, check web browsing history or monitor phone calls. Maintaining business efficiency can be difficult if employees are using the Internet for purposes unrelated to work. This is not only a drain on time and employee productivity, but some Internet conduct such as watching streaming video and downloading media can consume large amounts of bandwidth thereby slowing down the company network. The employer should include policies for what type of Internet use is allowed. The author then discusses the creation of such policies in depth. Each chapter covers policies for certain types of technology: computer and software, email, Internet use, instant messaging, personal blog postings, social media and cell phones, portable devices and cameras.

The author notes that computers are the main way that employee work product is stored. Therefore, employers should include in their policies that company computers are the employer’s property which can be accessed at any time. This would mean that even if an employee has stored personal information on a company laptop, the employer still has a right to view such files making the physical location of the laptop irrelevant.\(^3\) Encryption and encoding company files may be a way that a savvy employee will try to protect their privacy. The employer should include a provision explicitly banning encoding unless directed by the employer.\(^4\) Software used on computers can also pose legal risks. The author cautions employers to recall that software was purchased with a license to use. Employees should know from reading the policy that they shall

\(^3\) See TBG Ins. Serv. Corp. v. Superior Court of Los Angeles County, 96 Cal. App. 4th 443 (Cal. App. 2nd District, 2002) (holding an employee’s computer was legally searched at his home because computer was company property).

\(^4\) See Lisa Guerin, Smart Policies for Workplace Technologies (2010) (stating companies may demand encoding to protect customer information from unauthorized access by third parties).
not duplicate such software thereby exposing the employer to possible copyright infringements alleged by the owner of the software.5

The author next addresses policies for email use. Employees should be aware of how the email system should be used. The author suggests allowing minimal personal use of email as long as productivity and resources are not harmed. Next, the author recommends that employees are notified that emails are subject to access by the employer. In the event of a breach of this provision of the handbook, the author suggests mentioning that discipline will take place. The employer might have to get specific about what can be sent through the company email system. For example, if a company has had issues with email, those should be expressly stated in the policy. The author suggests that the employer assess its own needs with respect to email; to provide express statements prohibiting conduct that it has experienced in the past. For example, if an employer has had issues with email content, the employer should explicitly prohibit problematic conduct. A provision in the handbook could say that emails shall not contain harassing or discriminatory content. If the employer experienced issues involving the company’s good will, a provision should explicitly state that to protect good will, email shall not be a vehicle for supporting another organization’s business practices. Finally, the author includes provisions guiding employees to check their emails before they are sent. Tools such as spell-check and other practices for proofreading should take place in order to maintain professionalism as emails can circulate to higher-ups in the organization.

Attorney Guerin next addresses Internet use, which is a broad area of concern as far as productivity is goes.6 Personal use of the Internet should be expressly acknowledged in the written employment policy manual. Here the employer can direct how often, if at all, the Internet

---

5 See Guerin, supra note 4, at 37 (providing an example of company policy involving computer and software use).
6 See Guerin, supra note 4, at 69 (stating 60% of employees admitted to spending 3 hours weekly on personal sites at work).
may be used by employees before becoming subject to discipline. It is also advised that the employer expressly direct browsing activity. For example, an employer can direct which types of activities (live streaming, downloading) is permissible, and what types of websites an employee should not access (adult material, personal shopping, online auctions). The employer should include a statement that if in doubt the employee should ask the employer before proceeding to browse particular material.

As far as social networking and blogs are concerned, employers should know that because they are liable for the employee’s actions through the doctrine of respondeat superior, they must provide a policy for personal postings using computer resources. The author notes a specific circumstance where an employee’s public opinion could be construed as being the employer’s opinion. This can result in liability under the Federal Trade Commission (FTC) which “requires any endorser of a product—including those who post online reviews or discuss products on online discussion boards—to reveal their relationship to the product’s maker, if applicable.” Employees who post opinions about products that their company sells would be considered an endorser. Therefore, the author suggests that a provision prohibit using the company’s equipment to post personal opinions to a blog or other online forum.

The author cautions about privacy with respect to employee Internet browsing. She explores various scenarios that force an employer to investigate into employee browsing activity. To this point, she recommends that employers expressly allow themselves this privilege despite what the employee might allege to be private activity. According to a survey, 75% of

---

7 Guerin, supra note 4, at 75.
8 See Guerin, supra note 4, at 77 (outlining undesirable employee browsing activity requiring employer investigation).
employers use monitoring software that tracks browsing activity and the employee should be aware of this.\(^9\)

Other than web browsing, personal email that can be accessed through the Internet can also pose risks to employers. The author states that even the best employees can make mistakes by contacting clients through their personal email address. This would make sensitive company information vulnerable to many viruses or exposure to third parties.\(^10\) The author notes that it is critical to fit these policies around your company’s culture. For example, the author states that most companies are not comfortable with outright banning of personal email access.\(^11\) Therefore, she recommends that these policies be written in accordance with company culture and needs. The author strongly cautions however that reading personal email even though company property was used to access it, could cause legal problems. She refers to case law that held that employers are liable for viewing this type of content and the employer should consult with an attorney on how to draft limitations on use of personal email at work.\(^12\)

Another communication feature that co-workers use frequently is instant messaging (IMing). IMing allows people to type messages to each other in real time. The author begins by listing benefits to such a feature. For example, co-workers IM while working on their computers as the software doesn’t interfere with other programs; this quick, non-interfering communication increases productivity.\(^13\) However, the author does not let the downsides of allowing IMing to slip. Among likely problems are co-workers talking about subject matter outside the scope of their employment and the vulnerability of IM software to viruses. To this point, the author

\(^9\) *Id.* (noting that purpose of monitoring software is also to prevent employee from browsing illicit material).

\(^10\) *See Guerin, supra* note 4, at 79 (highlighting benefits of company email servers as being secure unlike personal web accounts).

\(^11\) *See Guerin, supra* note 4, at 81 (translating survey results of 50% of companies with no policy as indicating hesitancy).

\(^12\) *See Guerin, supra* note 4, at 83 (providing example provisions informing employees about monitoring software making email passwords exposed).

\(^13\) *See Guerin, supra* note 4, at 93 (noting results of survey proving use of IM productive).
suggests that like email, employers inform employees that IM messaging may not be private, especially on the company’s servers and that the employer specifically draft for how IM can be used by employees. Blogs and personal postings on the internet are another major area of concern for employer liability, especially when employees use these avenues to express themselves with regard to colleagues, bosses and clients. This is because employers can be responsible for employees’ actions. First, the author strongly cautions the employer against accessing postings that are password protected as this could lead to liability. The author suggests that employers educate themselves on laws that protect employee privacy. According to the author, the best approach is for employers to expressly prohibit postings created through company resources and to inform the employees of consequences for doing so. Social networking sites are also addressed in this book. According to the author, employers should not connect with subordinates through social networks like Facebook. She claims that by virtue of viewing personal posts and pictures, potential evidence for legal claims like discrimination are available.

Computer hardware and software are not the only ways employers can get involved in litigation. Cell phones and other handheld devices are growing in number as our world becomes more mobile and as the hours we are expected to work increase. Among the author’s major concerns are their use at work, wage and hour issues and safety. The simplest form of protection from losing productivity is to outright ban cell phone use for personal concerns at work, however

14 See Guerin, supra note 4, at 114 (showing high number of people who blog).
15 See Guerin, supra note 4, at 115 (discussing cases that held employer liable for claims infringing privacy rights). The Ninth Circuit Court of Appeals held that an employer violated the Stored Communications Act when employer accessed a private MySpace page belonging to the employee. Konop v. Hawaiian Airlines, 302 F.3d 968 (9th Cir. 2002).
16 See Guerin, supra note 4, at 116 (listing privacy protections for off-duty expression, political views, whistlebloggers, retaliation and concerted activity).
17 See Guerin, supra note 4, at 127 (noting how viewing pictures of boss at gay pride event could prevent a promotion caused by discrimination on the basis of sexual orientation).
this is not likely reasonable as valid reasons to take a brief call occur. Therefore, the author recommends that the employer draft a provision including this permission. In terms of safety, if the cell phone or handheld is work-issued, the employee should use care not to lose or damage the phone.

While employees working all the time can increase productivity, the downside is that employees entitled to overtime might work offsite resulting in hours not being recorded for wage purposes. There could be implications for the employer under the Fair Labor Standards Act (FLSA).\(^\text{18}\) The author recommends that the company have a policy that prevents employees from using their personal cell phone and other portable devices for work related calls and texts. Otherwise, this could result in a breach of security granted to clients if their contact information is stolen.

Additionally, employers should consider that cell phone use during driving is a large hazard, especially if the employee is traveling within the scope of employment. The employer may be liable for any accidents. Therefore, it’s best to include a provision that bans talking on a cell phone while driving during work hours. The author stresses the importance of the fact that portable devices are vulnerable to theft and damage that can result in a loss of company and client information.\(^\text{19}\) Provisions for proper steps to take in the event of loss or damage should be created as a guideline for the employee.

Lastly, the author addresses something that most people fail to consider: cameras. Today, cameras are a feature in most handheld devices and laptop computers. The author warns that the small size of these cameras and their portability make the workplace a danger if photos are taken

---

\(^\text{18}\) See Guerin, *supra* note 4, at 170 (stating Fair Labor Standards Act requires employers to pay qualifying employees overtime if more than 40 hours of work accumulate in a week).

\(^\text{19}\) See Guerin, *supra* note 4, at 188 (explaining how employee sued The Gap because company laptop theft resulted in security breach of employee personal information).
in a sneaky manner. Taking pictures of co-workers without their knowledge can be a violation of privacy. In addition, if pictures are taken of company documents or processes, this could be exposing trade secrets that a company strives to protect. The author suggests a few alternatives that employers can choose from. One option is for the employer to completely ban use of cameras in whatever form at work. A second option is to allow employees to bring such devices but with express limitations on their use. The author then recommends that the type of option an employer chooses depends on the nature of their company. A government agency for example would likely choose an outright ban, while an advertising agency may allow more leeway as far as camera use is concerned.

*Smart Policies for Workplace Technologies* is a very informative guide for employers that first raises their awareness about how technology involving the workplace can negatively impact their relationship to employees from a legal standpoint and also provides specific guidelines on how to draft policies that seek to inform and prevent potential legal liability. In addition, the book provides real life stories to put all of Attorney Guerin’s advice in context. The book is simple to understand but manages to retain its objective of tying legal implications arising from certain conduct. If an employer would speak to attorney regarding specific concerns at the workplace, I strongly suggest that the employer read this guide first in order to set the employer’s compass in the right direction, thereby decreasing prospective legal fees that go beyond the scope of a company’s concerns.