The Dangers of Pirated Software and the Risks for Employers

Omar Obeidat - Partner, Head of Competition and Intellectual Property - Intellectual Property / Competition

o.obeidat@tamimi.com - Dubai International Financial Centre

Mariam Sabet - Senior Counsel - Intellectual Property / Competition

m.sabet@tamimi.com - Dubai International Financial Centre

Broadly, copyright law protects the value of a creative work. When making an unauthorized copy of the creative work, copyright infringement occurs. We often see digital copyright warnings in our personal lives, such as before watching a movie, or when accepting a user agreement before downloading software or an application.

Digital piracy in the UAE may constitute copyright infringement under Article 7 of Federal Law No. 7 of 2002 Concerning Copyrights and Neighboring Rights. In a broad context digital piracy is a form of online piracy and includes the unauthorized online distribution of electronic copies of copyrighted material such as software. Violation of local copyright law amounts to a crime, and is subject to criminal prosecution in the UAE. Additionally, unauthorised use of software may be deemed to be an aggravating factor under Article 46 of the Federal Decree Law No. 5 of 2012 On Combating Cybercrimes, as technological means are used to further a crime against the copyright holder. Damages often include paying the price of the illegally-downloaded licenses, and may also lead to serious personal sanctions, such as imprisonment, fines, and even deportation for a company's top officials.

In respectof commercial software, an end user license agreement is included to protect the software program from copyright infringement. Typically, such licenses state that the user can install the original copy of software bought on one computer and allow a backup copy in case the original is lost or damaged. The user agrees to the licensing agreement in the following forms: (i) once the software package is opened usually referred to as a shrink wrap license; and (ii) when the user installs the software. One of the biggest problems faced by software developers and companies is that their software is often cracked and made available online thereby allowing users to freely download and use an unauthorised version of the software; typically this involves downloading illegal software from peer-to-peer network.

Oftentimes, the risks of infringing digital copyright in software are overlooked by employers whose staff regularly uses the internet. In this regard employees illegally download software on company computers without the knowledge of their employer. Over time, this can lead to serious legal disputes, financial repercussions and major disruptions to day-to-day business operations. In fact, according to a study conducted in 2013 by the IDC (International Data Corporation) it was determined that a third of the PC Software in the world is counterfeit. Through its study, the IDC encountered tracking cookies and spywares 78% of the time when downloading software from the internet and Trojans and other malicious adware 36% of the time. Given these rates, where pirated software is downloaded from the internet, there is a one in three chance that dangerous malware will be contained. It is important to point out that some malware are capable of remotely turning on an infected computer's microphone and video camera, potentially giving a cybercriminal eyes and ears into a victim's home or business. Furthermore the risks associated to malware are serious, not only is there risk of loss data and identity theft but there is also serious risks associated to copyright infringement.

In the UAE, as in most jurisdictions, employers may be liable for the actions of its employees. For the employer to be liable, the employee need only show he or she was acting in the scope of their official duties. This is often a fairly low bar. Whether or not the employer is immediately aware of its employees'

actions is generally irrelevant. As such, when employees illegally download software on company property, especially if used in the course of their jobs, the employers may be found guilty of copyright infringement.

Detecting software piracy is no longer reserved for sophisticated intelligence agencies and cyber police and can easily be traceable. Software companies are able to monitor “cracked” versions of their software thorough what is described as a “phone home” technology. In brief, the “phone home” technology scans the internet for illegal downloads of its software, and provides detailed information about the infringer, including its IP and Machine Access Control (“MAC”) address. These details are linked to the employer through open source methods such as whois.com. Serial keys of illegally downloaded software will often not match the authorized keys known by the copyright holder; thus exposing that the program has been cracked. Hence, when a cracked version of software is downloaded and is being used, the “phone home” technology which is embedded in the software technology, much like a heartbeat, sends signals to the server and provides information which can identify the infringer.

Once this information is known, copyright holders can take swift legal action against infringing companies. This includes filing a complaint with the police and the local courts. Employers should be aware that deleting illegal software can also be tracked, and is often seen by the courts as the company acknowledging its own wrong-doing and possibly tampering with evidence.

In order to minimize the risk of liability for software violations, employers can take various steps to safeguards their rights and minimize the risk of exposing themselves to copyright infringement. For one, the employer can conduct regular audits of employee software usage which includes tracking all software downloads on company property. Secondly, the employer can maintain a well-organized library of software licenses, and make sure they are up to date. Lastly, it is important to educate staff by both ensuring that employee policies are clear about the risks and penalties of software piracy and via regular training to employees about copyright and similar legal issues.