Remote Work and Information Security

Protecting Valuable and Confidential Information During Quarantine©

An article by Robert J. McGee, Esq.

Business models permitting, many of our small business clients are encouraging and enabling employees to work remotely for the duration of the COVID-19 pandemic. This is a prudent step to take both in terms of employee safety and in terms of liability, as the company avoids unnecessarily exposing its workers to the virus.

However, if the company does not already have a robust set of policies and procedures in place for remote work, employees may inadvertently expose valuable company intellectual property to loss. Such risks can be reduced or mitigated with proper policy, so long as employees scrupulously observe these instructions. The following should be considered a brief, accessible summary of such considerations and some steps that can be taken to protect a company's confidential information during quarantine.

First and foremost, any company **Trade Secrets** must be stored securely by the workers. Trade secrets, meaning information which provides economic value so long as it is not generally known, are protected by federal statute, state statute in most states (including Arizona, home of the Law Offices of Donald W. Hudspeth), and by contract provisions with individual employees. However, trade secret law will not generally protect a company against innocent disclosure to the general public. Employee personal computers may operate on a shared network with every other device in their home, or may be transmitted via unsecured wireless network. It may be stored on portable media such as a USB drive which could be inadvertently be used for other purposes by a family member. Once a trade secret is out, it's out forever; one cannot un-ring the bell. Monetary remedies are generally inadequate – a competitor with access to an inadvertently disclosed secret may immediately move to undercut your company's rates.

Ideally, all trade secrets will be accessible only remotely via VPN or other secure means, and workers will not keep copies of such information on their personal computers or in hard copy at home. Workers should be aware that they may not create local copies, even to avoid network lag or to continue working when the company server is under maintenance. Even little details matter – employees should even be asked to prevent family and roommates from reading their work screen over their shoulder. If needed, employees should work with your IT provider to properly secure their home wireless network and restrict access to such information from other devices on their home network.

If a remote worker's spouse receives and views trade secrets, that is not always a disaster. Spouses benefit from a presumption of martial confidentiality. However, unless the non-worker spouse is aware that the information must be kept secret, that person may innocently disclose the information further, or carry unsecured data unknowingly on a USB drive or wireless device where it may escape into the world. It is best to prevent such disclosures in the first place. And of course, children do not benefit from any presumption of confidentiality.

It can be difficult to separate information which is secret from that which is not, so as a general rule, data protection policies should apply to all work, or at least to as much work as is practical. These policies should be communicated to employees in writing, and the writing itself should be preserved: evidence of practical steps taken to preserve a trade secret is valuable in any related litigation.

In summary:

- A "trade secret" is any kind of information which is valuable in part because it is not generally known.
- Generally, once a trade secret enters public knowledge, it is gone forever.
- Remote workers should avoid keeping off-site copies of company trade secrets and should avoid the risk that family members and housemates will see them.
- Companies should provide remote workers with adequate data security such as a secure VPN and assistance in setting up secure wireless, if needed.
- Companies should provide clear written guidelines of all procedures to remote workers.

Confidential Customer Information requires similar considerations to trade secrets. The economic concern here is different in nature, being a liability rather than a risk of lost profits, but the concerns are the same. Take all reasonable steps to prevent confidential information from reaching third parties, including family, or from ending up on unsecure storage media or anywhere it could be misplaced. This is of particular concern for medical providers, law firms, and accountants, who tend to handle their clients' most sensitive information and are bound by very strict standards of confidentiality.

Notably, confidential client and customer information must be kept from one's spouse with as much rigor as a complete stranger. While all trade secrets and patentable subject matter should be kept from those who do not need them, including spouses, it is sometimes possible to rely on the presumption of marital confidentiality to prevent loss of such IP. This is not the case for confidential client information. For example, an attorney who discloses confidential client information to a spouse is already in violation of his duties even if she is completely discrete. Companies should be flexible with remote workers living in close quarter with family to avoid accidental disclosure.

In summary:

- "Confidential customer information" must be protected to avoid liability.
- The measures taken to protect such information is similar to that for trade secrets.
- There is no failsafe option for accidental disclosure to a spouse.

For material subject to **Patent Protection**, including matter not yet the subject of a patent, the most stringent protections are required. This is because patentable matter is subject to becoming part of the public domain after public disclosure. In nearly all circumstances, once patentable matter has first been disclosed to parties not subject to confidentiality requirements, the inventor will have only one year to apply for patent protection; after that, the information is considered public domain.[1] The economic benefits of a patent's years-long monopoly on "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof" is then lost forever. While there is

[1] There are exceptions and nuances to this rule, but as a practical matter, broad, simple guidelines are best for ensuring secrecy, whereas trying to brush against the very edge of a gray-area rule invites litigation at best and outright loss of patentable matter at worst.

precedent for preserving patentability of matter incidentally disclosed in places like the home where one is entitled to a presumption of privacy and seclusion (see *Moleculon Research Corp. v. CBS, Inc.*, 793 F.2d 1261, 1265, 229 USPQ 805, 809 (Fed. Cir. 1986)), the general rule is that any disclosure to the public starts the countdown. A famous example, *Egbert v. Lippmann*, 104 U.S. 333, 336 (1881), resulted in a ruling that the public use of corset rings were sufficient to render them unpatentable, even though the rings were disclosed only to close friends and the "public use" was under layers of clothing. Consequently, work on patent should be performed in conditions of privacy similar to those recommended for confidential client information. Where work on patentable matter involves work on tangible prototypes, such work should be temporarily halted if at all possible; where that is impossible, work should continue to be performed on-site under condition which will enable proper sanitation and social distancing.

In summary:

- Patentable subject matter includes any new and useful process, machine, manufacture, or composition of matter."
- Patentable subject matter generally becomes ineligible for patent one year after its first public disclosure.
- "Public disclosure" of patentable matter may include even discrete use by a single close friend without the knowledge of any other party.
- Remote work on patentable subject matter requires similar protections to trade secrets.
- Patentable subject matter that cannot be developed remotely will require the company to either suspend development or enable sanitary and safe working conditions.

As always, the key is to set down clear policies for employees, communicate those policies in writing, and then provide working conditions conducive to following policy. This last point will require some effort by employers; expecting employees to work remotely requires a connection free of lag and inconvenient interruptions. Expecting an employee to keep secure any material at home, particularly hard copies or USB drives, may require providing a portable means of secure storage. Above all, listen to your employees' feedback about the expectations placed upon them.