Vann Attorneys, PLLC | Attorneys at Law

THE LEGAL PAD

Practice of Excellence

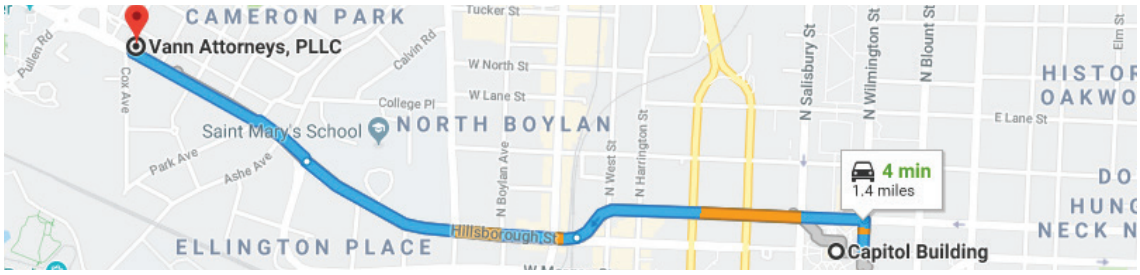
First Quarter 2019

A Newsletter of Current Business and Legal Matters

In This Issue:

Using GPS Tracking Devices in the Business Context | An Interesting Twist

By James R. Vann & Keith Boyette, Intern



While mostly always beneficial to our daily lives, the integration of new technology into everyday activity has also raised quite a number of legal concerns. Let's say a business competitor of yours places a GPS tracking device on the bottom of your vehicle and keeps track of your location as you travel from place to place. In 2015, the North Carolina Business Court addressed the very issue of whether such action resulted in the trespass of personal property and invasion of privacy under North Carolina law. The Court in that case determined that it did not.

Trespass of Personal Property

Under North Carolina tort law, the mere touching of personal property by another individual is insufficient to find trespass of personal property. Rather, the touching must actually interfere with the use of the property in some way or another. The Business Court determined that affixing a tracking device to the bottom of an individual's vehicle does not dispossess the owner of their property nor deprive the owner of their ability to use it. The ultimate determination of "interference" appears to rest on the underlying purpose of what is being interfered with. For example, the placement of a boot on a car's wheel is an interference with the car "because the main purpose of a car is transportation, and one cannot drive around with a boot attached to the wheel of one's car." According to this analysis and the Business Court, the placement of a GPS on the bottom of one's vehicle does not interfere with the use of the vehicle, does not impair the operation of the vehicle, nor does it damage the vehicle in any way.

Invasion of Privacy

The Business Court determined that there is no invasion of privacy where the information obtained is public, rather than private in nature. The underlying determination rests on the idea that a person traveling in a car on public roads has no reasonable expectation of privacy in movements from one place to another. Accordingly, the placement of a GPS device enabled to obtain information that could equally be obtained by observing the vehicle on the public roadways does not amount to invasion of privacy. Of course, the outcome could be different if the placement of the GPS successfully obtained information that would not otherwise be available to the public but for the intrusion into the place where an individual has a reasonable expectation of privacy.

Unfair and Deceptive Trade Practices Act (UDTPA)

Finally, for those of you in the business context, the Court determined that that attachment of the GPS tracking device did not amount to a violation of the UDTPA because the device was attached to the individual's private vehicle, and thus the surveillance was deemed not to be "in or affecting commerce."

So, how would this analysis change if it were a company vehicle or a company laptop? It is crucial to note that the ultimate determination depends on the specific situation at hand, so please contact us with any questions regarding your particular situation.

Who Owns Your Company's Social Media Presence?

By James R. Vann & Caitlyn Truelove, Attorney

In the classic nursery rhyme, "Hey Diddle Diddle," we find it amusing when the dish ran away with the spoon. Business owners, however, do not find it amusing when a former employee runs away with your business's username(s) and password(s) to its social media account(s) and/or the business's website. The creation of an online presence is necessary for success. An online presence not only makes it easier for customers to find your business, but it also helps you gain more customers, and thus, grow your business.

How the business's online presence is created, whether through the formation of a website and/or social media account(s), is at the discretion of the business owners. Creating an online presence for your company through a social media site such as Facebook, Twitter or LinkedIn, or creating your own website effectively advertises your business before a large audience. As such, your social media account(s) are assets potentially bringing more of business to your company. At least one bankruptcy court in Texas classified a social media account as an asset .
So, what happens when your ex-employee, who created the social media account(s), leaves your employment with the username(s) and password(s)? Are the username(s) and password(s) of the account(s) made for your company your property, or the former employee? What about if the account taken was an employee's work profile? This does not seem like a big issue, right? After all, even though your employee made the account(s), username(s) and password(s); it is your company's name on the account. Therefore, the account is company property, right? Maybe not. The answer is not that easy, nor is it straightforward, especially if it was the former employee who created the website and/or social media account(s).

This issue can become a massive headache and nightmare for business owners. The company's social media account(s) represents your company. Quite often today, this account is the first impression a potential customer gets of your company. The mere notion of a vindictive employee holding your website and/or account(s) hostage and doing who knows what to it is frightening.

Although this issue has been litigated in some federal courts, there is no case law in North Carolina on the issue. The federal court decisions, however, may give North Carolina business owners some tips and guidance on how to possibly avoid this headache.

The cases of PhoneDog v. Kravitz and Eagle v. Morgan have demonstrated that costly and long litigation may be avoided if the business owner had included a social media policy clause in the employment contract. In the case of PhoneDog, Mr. Kravitz left his former employer, PhoneDog, with the Twitter account that had been created for the company. This case was later settled allowing Mr. Kravitz's to retain his Twitter account and followers; however, this issue could have been avoided if PhoneDog had the former employee sign a modification to his employment agreement with a social media clause supported by new consideration.

In the case of Eagle, Dr. Linda Eagle was the president of Edcomm until she was fired. Almost immediately after she was fired, her LinkedIn account was accessed by Edcomm, whereupon, Edcomm changed her password, and replaced her photo and name with that of the new president of Edcomm. Dr. Eagle sued under several claims, including: unauthorized use of name, invasion of privacy by misappropriation of identity, and misappropriation of identity. While she was able to prove the elements of each of the claims listed above, she could prove no monetary damages.

The bright-side is that there are some steps that your company can take now to possibly avoid some of the issues in PhoneDog and Eagle. The most important step is to create a clause in a written agreement, such as an employment agreement and/or a work product agreement, clarifying ownership of social media accounts. This clause should clearly state that the company owns the social media account and, in the event the employee is terminated, all usernames and passwords must be surrendered to the company. This clause should cover any business and personal accounts you require your employees to create. As we can see from the case of Ardis Health, LLC v. Nankivell , this approach to avoiding long and costly litigation really does work. In the case of Ardis Health, the court ordered the defendant, who was hired as a video and social media producer, to return any login information, including passwords, required for the plaintiff's websites and social media accounts. Here, there was a signed work product agreement, which stated any websites and social media accounts were the property of the plaintiff. You must remember; however, that your employees have a contract between the individual and the social media site he/she uses.

Another possible step companies should consider is registering social media accounts in the company's name and providing approved usernames and passwords to employees for these accounts. The company should actively maintain and monitor the employee's social media accounts, which were created and distributed by the employer. These usernames and passwords should be available to more than one person within the company. The common-sense reason behind this is that creation, active monitoring, and maintenance may be useful in demonstrating ownership if one of the situations listed above occurs, however, continual access to these accounts is necessary for this to occur. It would be prudent to have both the owner of the company and someone else, in a position of authority at the company, or better yet, the person who monitors all employee social media accounts, to have a written copy of all the passwords and usernames. If only one person had the list, the employer would be in a bind when that employee left with all the social media access information or demanded a promotion or pay raise holding this access information hostage. The same is not true if more than one person has access.

We hope this article has helped you. If you have any questions, the attorneys at Vann Attorneys will be more than happy to answer your questions and assist you with the creation of such policies and contracts as your business requires.

1 In re CTLI, LLC, No. 14-33564, mem. Opinion (Bankr. S.D. Tex., Apr. 3, 2015).
2 PhoneDog LLC v. Kravitz, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal., Nov. 8, 2011).
3 Eagle v. Morgan, 2013 U.S. Dist. LEXIS 34220 (E.D. Pa. March 12, 2013).

Who Owns Your Company Website?

By James R. Vann & Caitlyn Truelove, Attorney

It is essential for the commercial success of your business to create an online presence. This article will be discussing some issues arising from having an employee or a website designer create and register a domain name and website.

Imagine if you commissioned the creation of a website and domain name perfect for your business. Suddenly, the employee or web designer who created the website and registered the domain name is: fired, quits, or disappears. Now, your website is down, and you do not have the username(s) and password(s) necessary to gain access to the account. You thought you owned the website and domain name. To your horror, however, you discover that you do not actually own the website and domain name for which you paid a considerable amount of money to create and upkeep. This nightmare situation has happened to others before. Don't let it happen to you too.
Merck KGaA may demonstrate a real-life example of the value of such property. In the case on Merck KGaA, "Merck [KGaA] entered into an agreement with Facebook for the exclusive use of the Web page www.facebook.com/merck." Less than two years later, Merck "found that: a) it no longer had administrative rights to the Web page [despite the agreement]; and b) that the Web page had content that appeared to be created by, and is related to its competitor Merck & Co." Merck KGaA filed in a New York state court against Facebook to try to determine how it was that Merck's Web page was misappropriated by its competitor. This Web page for Merck KGaA represented one of its very valuable marketing devices. Facebook apologized for the inconvenience after the court filing. However, this apology was hollow as Facebook essentially said that they were going to make the web page unavailable until both Merck's can agree to who actually owns the web page despite the existing agreement. Unfortunately, as you can see from Merck's case, an agreement may not be enough to protect you from such aggravation and frustration.

It hardly needs mentioning that a website is one of a small business's greatest intangible assets; so it is important to protect it. One step that you can use to protect yourself is to require whoever is to create the website to sign a work for hire/work product agreement. This agreement in essence states that the business owns anything that that person makes. This step was implemented by Ardis Health in the case of Ardis Health, LLC v. Nankivell, The companies had a signed work product agreement, which stated any websites and social media accounts created by the defendant ("employee") were the property of the plaintiffs ("companies"). The employee took the passwords and usernames with her when she left and refused to give them back. The companies sued for the return of the access information and intangible assets. In that case, the court ordered the employee, who was hired as a video and social media producer, to return any login information, including passwords, required for the plaintiffs' websites and social media accounts. If the companies had not possessed such an agreement the court would likely have held the employee as the author, and thus owner, of the website. The companies would then have to pay another person to create another website that does not infringe on the defendant's website. This is a painful lesson which may be avoided by the creation of a work product/ work for hire agreement. Furthermore, if your employee also created a website, you should create a work for hire or similar agreement stating that both the graphic work and the software coding work of the website belongs to the business. The reason for this suggestion is that there are different parts of your website that may be protected as different copyrights under copyright law. By making it clear that the company owns the entire work, legal arguments from the employee or website designer claiming legal ownership of one of the website's copyrightable parts may be avoided.

The business should make sure that more than one person has access to the account and that the access information is written down. The common-sense reason behind this advice is that in order to actively monitor and maintain the website and domain name. It would be prudent to have both the owner of the company and someone else, preferably, someone in a position of authority at the company, to have a written copy of all the passwords and usernames for the website and domain name. If only one person had the list, the employer would be in a bind when that employee left with all the website and domain name access information or demanded a promotion or pay raise holding this access information hostage. The same is not true if more than one person has access.

We hope that this article has been helpful to you. This is not a full and comprehensive list of the issues you and your business may face in such a situation as the facts differ from case to case. If you have any questions or would like help with implementing steps to help protect such intangible assets as your company's domain name and website the attorneys at Vann Attorneys would be happy to assist you.

1 Merck KGaA v. Facebook Inc., N.Y. State Supreme Court, New York County, No. 113215/2011 (Nov. 21, 2011).
2 Ardis Health v. Nankivell, 2011 U.S. Dist. LEXIS 120738 (S.D. N.Y., Oct. 19, 2011).

Which Minority Interest Provides Better Protection?

By James R. Vann & Caitlyn Truelove, Attorney

Here's the scenario, Adam and Bill hold interest in two different business entities. Adam is an LLC member holding a minority interest. Bill is a minority shareholder in a close corporation with a similar interest to Adam. Recently revealed information shows that the majority interest holders of both organizations have been dishonest, making decisions that benefit themselves at the expense of the business's interest. The question is whose interest is better protected from the misconduct of their respective majority interest holders? Is it Adam, whose interest lies in an LLC; or is it Bill, whose interest lies in a close corporation, that is better protected?

The power balance in an LLC and a close corporation are not always equal. These business entities often have minority shareholders or members. The minority interest holder in a business can be easily disadvantaged by the actions of the majority whether in an LLC or a close corporation. While the minority interest has little to no decision-making power in the business; there are ways for the minority interest holder to protect him/herself. However, those minority shareholders and members may be limited in how they are able to protect themselves from the wrongdoing of the majority and company or corporation.

The case of Norman v. Nash Johnson & Sons' Farms, Inc., reiterated that close corporations are often characterized in the state of North Carolina as incorporated partnerships where the partners are often the shareholders. In a close corporation the minority shareholders may be left with few remedies if the majority acts against them because he does not have the "way out" which is open to minority shareholders of a publicly held corporation. This "way out" is the opportunity to sell his shares on the public market at market value. While there is great risk of the majority exploiting the precarious position of the minority and forcing him to sell his interest at mere pennies on the dollar; there is a bright side for the minority in such situations. The bright side: the minority may proceed against the offending shareholders and corporation in a direct action, so long as he meets the standing requirements for raising such a claim. Otherwise, it would be ludicrous for the courts to require the minority to file a derivative action on behalf of the close corporation when the monetary award would just go into the hands of the wrongdoing majority. Also, the derivative actions burdensome procedural requirements are not required for filing a direct action. The LLC's answer to the troublesome procedural requirements for a derivative action, such as a pre-litigation demand: eliminate them. So, both close corporations and LLC's have ways of getting around the derivative actions onerous procedural requirements.

According to Fiske v. Kieffer, the state of North Carolina treats a member of an LLC like a corporate shareholder. Like shareholders, these members owe no fiduciary duty to each other; however, a fiduciary duty is owed to the minority when a majority member exercises control over the LLC. Nevertheless, the court has yet to recognize a fiduciary duty when multiple minority members act in concert due to the ability of the minority members of the LLC to contract for protection not available to shareholders of a close corporation in a written operating agreement. The content of the operating agreement, if there is one, would likely be the deciding factor in whether a close corporation or an LLC grants its minority interest holders greater protection from the majority.

There is no clear-cut answer to this question. As stated in Blythe v. Bell, this question must be decided on a case-by-case basis based on the particular facts of each case. The deciding factor may be the operating agreement. The operation agreement allows the LLC to contract for greater protections for the minority members. Thus, the decision as to who is better whether Adam or Bill holds the better protected minority interest may come down to the content of the LLC's operating agreement, if one exists in writing.

We hope this article has been helpful to you. If you have questions, please feel free to contact us.

1 Norman v. Nash Johnson & Sons' Farms, Inc., 140 N.C. App. 390, 404, 537 S.E.2d 248, 258 (2000).
2 Fiske v. Kieffer, 2016 NCBC LEXIS 22.

VANN ATTORNEYS
ATTORNEYS AT LAW
Practice of Excellence

1720 Hillsborough Street | Suite 200 | Raleigh, NC 27605
Phone: 919-510-8585 | Fax: 919-510-8570

1200 East Morehead Street | Suite 251 | Charlotte, NC 28204
Phone: 704-496-7495 | Fax: 704-496-7480
www.vannattorneys.com