OLIVE & OLIVE, P.A.
INTELLECTUAL PROPERTY LAW
Since 1957

500 MEMORIAL ST.
POST OFFICE BOX 2049
DURHAM, NORTH CAROLINA 27702-2049
(919) 683-5514

LIFE IN THE UNDERGROUND – DATA MINING

Data mining[1] from the websites of others is a common practice. Most of us search the Internet via Google, Yahoo, and other search engines; and when we find information that looks useful, we download it onto our own computers and use it. The use of this information is however protected; protected by copyright, trademark, trade secret, common, and even criminal law. Copyright law limits our ability to reproduce, distribute, and otherwise use what we have viewed. Trade secret law protects confidential data that has been appropriately safeguarded. But there's more, there are additional limitations which are not so well known. For example, there are limitations not only on the ability to use downloaded data, but whether the data even can be downloaded legally in the first place. Knowing these limitations and applying them, is critical as the Internet becomes an increasingly important part of our lives. In this article we are going to explore some of these other laws as well as causes of action–including criminal statutes–that the indiscriminate downloader can violate. At the same time, we will think about how websites should be structured so that the site owner may take advantage of available protection.

I. ARE YOU TRESPASSING?

Most people are familiar with the concept of trespass as it applies to land, and understand that entering a place without permission or a right to do so is unlawful. A similar doctrine of law exists with respect to personal and movable property, and is called "trespass to chattels." As discussed below, websites are treated as "chattels" and unauthorized entry onto a website can give rise to liability for trespass to chattels.

A website owner, or one who has posted web content, typically will have little trouble showing that they have the right to control entry onto the site. At the same time, one who has posted a website typically has–at least impliedly–invited the public to visit and use the website. How, under those circumstances, can a user become a trespasser? The key typically lies in whether the user has made some unlawful interference with the website or its contents or, as one

[1] Data mining, as used here, refers to entering the websites of others and removing useful information from those sites—a practice referred to as "harvesting" or "mining" data. The term first was used, and still commonly is used, to refer to making use of one's own data—collecting it in a usable format from one's own inhouse databases. Here, however, we are focused on mining data from third-party sites.

court has expressed the test for trespass to chattels, whether there has been "an unauthorized, unlawful interference or dispossession of the property."[2] Let's explore some examples.

In 1997 in the case of *Thrifty-Tel v. Bezenek*, teenage siblings secured the "access code" of a long distance telephone carrier from a boy in their neighborhood. The boys used the access code to get into the phone system and search for long-distance authorization codes. They performed multiple searches which in turn tied up the phone company's system, delaying the access of other users. Use of the long distance telephone carrier's website without authorization was held to constitute trespass and the parents were held liable for the boys' actions.

In another case, *CompuServe, Inc. v. Cyber Promotions, Inc.*, Cyber Promotions, a bulk e-mailer company, sent large volumes of unsolicited emails to Internet users, many of whom were CompuServe subscribers. CompuServe notified Cyber Promotions to stop spamming CompuServe's customers, but Cyber Promotions felt it was entitled to ignore those instructions. CyberPromotions argued that CompuServe had elected to join the Internet, so its mailboxes were open to all. They were wrong. The court found them liable and granted judgment in favor of CompuServe, reciting the general principles of trespass to chattels. The court stated:

> In the present case, any value CompuServe realizes from its computer equipment is wholly derived from the extent to which that equipment can serve its subscriber base. … To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve CompuServe. Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct.

CompuServe, Inc. v. Cyber Promotions, Inc. et al, 962 F.Supp. 1022 (S.D.Ohio 1997). The court further held**,**

> Defendants' intrusions into CompuServe's computer systems, insofar as they harm plaintiff's business reputation and goodwill with its customers, are actionable under Restatement Section 218(d).

Id at 1023. The court disposed rapidly of the argument that just because desired customers are permitted to use the electronic facilities, all persons necessarily must permitted to do so:

> Defendants argue that plaintiff made the business decision to connect to the Internet and that therefore it cannot now successfully maintain an action for trespass to chattels. Their argument is analogous to the argument that because an establishment invites the public to enter its property for business purposes, it cannot later restrict or revoke access to

[2] *Fordham v. Eason*, 521 S.E. 2d 701 (N.C. 1999); *see also*, Restatement (Second) of Torts §218. In North Carolina, note that actual damages is not an essential element of the tort. *Hawkins v. Hawkins*, 101 N.C. App. 529 at 533, 400 S.E.2d 472 (1991).

> that property, a proposition which is erroneous… On or around October 1995, CompuServe notified defendants that it no longer consented to the use of its proprietary computer equipment. Defendants' continued use thereafter was a trespass.

Id at 1024.

More recently, in *eBay, Inc. v Bidder's Edge, Inc.*¸ the Internet auction site sued a company that collected and aggregated data about auctions. The court held that obtaining auction data from the eBay website, against the wishes of eBay, constituted a trespass to chattels:

> One who uses a chattel with the consent of another is subject to liability in trespass for any harm to the chattel which is caused by or occurs in the course of any use exceeding the consent, even though such use is not a conversion." …
>
> … Conduct that does not amount to a substantial interference with possession, but which consists of intermeddling with or use of another's personal property, is sufficient to establish a cause of action for trespass to chattel. …
>
> … A trespasser is liable when the trespass diminished the condition, quality or value of personal property. … The quality or value of personal property may be "diminished even though it is not physically damaged by defendant's conduct….
>
> … [I]t is undisputed that eBay's server and its capacity are personal property, and that BE's searches use a portion of this property Even if, as BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property. …

eBay, Inc. v Bidder's Edge, Inc.¸100 F.Supp.2d 1070-71 (N.D.CA. 2000).

Finally, in *Sotelo v. DirectRevenue, LLC*, the court found trespass to chattels was appropriately pled where adware was loaded onto a company's computer without the consent of the owner. The court noted that the interference need not be major, nor the harm substantial, to sustain a claim for trespass to chattels.

An award premised on trespass to chattels gives rise not only to the potential for nominal or actual damages, but also the potential for an award of punitive damages. There is no

requirement that special damages, such as loss of income, be proved in order to recover punitive damages.[3] The potential penalty paid by one who trespasses could, therefore, be quite large.

Lesson? Any use of a website that goes beyond the scope of that which the owner reasonably can be expected to have contemplated, should be undertaken with caution. Virtually all website use has at least some impact on the amount of resources available to serve others, and punitive damages can be a significant threat even where little specific harm can be itemized.

II. BREACH OF CONTRACT: THE ROLE OF "TERMS OF USE"

It is typical for users of websites to encounter "Terms of Use" posted on the website. Just as with shrink-wrap licenses, some people read them; some do not. At least when posted with sufficient prominence to attract attention, however, these Terms are generally held to constitute binding contracts, and it is perilous to ignore them.

A claim for breach of contract in the context of website use typically contains the following allegations: (1) the website owner created Terms of Use governing access to and use of its website and gave notice to the defendant of these terms, which constitute a contractual offer; (2) the defendant received notice of these terms; (3) defendants, after having been placed on notice of the existence of the Terms of Use and told that the Terms of Use would govern any use of data obtained from the website, elected to enter and use the website, thereby accepting the terms of the contract; (4) defendants then breached the contractual terms by using data obtained from the website in a manner that was expressly forbidden by the Terms of Use.

One such case involved an online computer game.[4] A company called Blizzard developed and launched Battle.net, a free program that allows games purchased from Blizzard to be played over the Internet. Now consider this: There were twelve million users, racking up 2.1 million online hours/day. Blizzard wasn't at first prepared to handle the volume of gamers, and Battle.net users immediately became frustrated with the amount of downtime. Some of those frustrated users thought it would be a good idea to come up with an alternative, so they reverse-engineered Battle.net and created a game platform that used the same protocol. While game players thought that was pretty clever and were happy, Blizzard wasn't so pleased, and sued. Even though reverse engineering of the gameware might otherwise have been legal, Blizzard pointed out that in the Terms of Use that came up at the first login of Battle.net, reverse

[3] The subject of punitive damages, and constitutional limitations on the amount of such damages, is beyond the scope of this article. Some states have statutory limits on punitive damages. For example, in all cases except those where the harm was caused by driving while impaired, North Carolina sets a punitive damages cap of $250,000 or three times the amount of compensatory damages, whichever is greater. Even where there are not statutes, there are constitutional limitations. The United States Supreme Court has said that punitive damages must be reasonable in amount, and that excessive awards violate the due process clause of the U.S. Constitution. At the same time, the Court has recognized that punitive damages are constitutional. The extent to which there must be any nexus between provable special or general damages awards and punitive damages, and if so, the extent of the nexus, remains in flux. Challenging the amount of an award would be expensive, even if ultimately successful; and success cannot be assured.

[4] *Davidson & Associates v. Jung*, 422 F.3d 630 (8th Cir. 2005)

engineering was clearly prohibited. The Eighth Circuit Court of Appeals agreed, and held the Terms of Use posted on the Battle.net website were enforceable.

In another case centering on Terms of Use, Verio accessed the website Register.com (a domain registrar), downloaded domain owner names, contacted the customers and sought their business.[5] Registrar.com's posted Terms of Use however forbade use of the website data for marketing purposes. Verio argued that it had not agreed to the Terms of Use. The court, however, found that by proceeding to submit a WHOIS query, Verio manifested its assent to be bound, forming a contract that it subsequently breached. Thus, the court found in favor of Registrar.com.

In addition to the expected damages for breach of contract, it is important to be aware that the Terms of Use may themselves address the issues of damages and attorneys' fees (although, if the terms are too onerous there may be defenses in the nature of "contract of adhesion" and, as well, the court will look at the degree of notice provided to the user with an even more than usually jaundiced eye).

Lesson? Terms of Use are important. If one is going to make use of data from a website, read the Terms first. Even nominal use that might otherwise be considered a reasonable business risk can escalate in cost once attorneys' fees are factored in. On the other hand, if you are a website owner, "post your property!" Website owners should post Terms of Use, that include prominent statements imposing conditions on use of the site such as: "you may access and use our site…if you and your company will abide by these terms…". The website also should include an express instruction, prominently posted, that "IF YOU DO NOT AGREE WITH THESE TERMS, DO NOT USE OR FURTHER ACCESS ANY PART OF THIS WEBSITE."

III. CRIMINAL STATUTES (& THEIR CIVIL OFFSHOOTS)

Not only can data mining give rise to civil liability, but it also can be a crime. Many states now have criminal statutes directly addressing various forms of computer crime including unauthorized data mining. North Carolina, for example, has an entire article (Article 60) devoted to "Computer Crime." The Federal government also has laws that criminalize a wide variety of activities in the data mining and computer fields, providing criminal penalties for everything from spam, to unauthorized use of computers, to copyright infringement.

While we could expand on this topic at great length, the statutes are fairly explicit. Thus, we will outline and briefly discuss the North Carolina statutes, which are fairly typical of the state trends, and point out the leading Federal statute. If one is charged with a crime, however, one should not try to figure out whether the charges are justified but should instead immediately contact an attorney. Penalties can be severe, including not only substantial fines but also lengthy prison terms.

[5] *Register.com v Verio*, 126 F.Supp.2d 238 (S.D.N.Y. 2000), *affirmed*, 356 F.3d 393 (2nd Cir. 2004)

A. North Carolina Statutes

Two North Carolina statutes, typical of those found in other states, are particularly applicable to data mining, and one of them provides a civil remedy as well as criminal penalties.

1. Accessing computers (N.C.G.S. § 14-454).

(a) It is unlawful to willfully, directly or indirectly, access or cause to be accessed any computer, computer program, computer system, computer network, or any part thereof, for the purpose of:

(1) Devising or executing any scheme or artifice to defraud, unless the object of the scheme or artifice is to obtain educational testing material, a false educational testing score, or a false academic or vocational grade, or

(2) Obtaining property or services other than educational testing material, a false educational testing score, or a false academic or vocational grade for a person, by means of false or fraudulent pretenses, representations or promises.

A violation of this subsection is a Class G felony if the fraudulent scheme or artifice results in damage of more than one thousand dollars ($1,000), or if the property or services obtained are worth more than one thousand dollars ($1,000). Any other violation of this subsection is a Class 1 misdemeanor.

(b) Any person who willfully and without authorization, directly or indirectly, accesses or causes to be accessed any computer, computer program, computer system, or computer network for any purpose other than those set forth in subsection (a) above, is guilty of a Class 1 misdemeanor.

(c) For the purpose of this section, the phrase "access or cause to be accessed" includes introducing, directly or indirectly, a computer program (including a self-replicating or a self-propagating computer program) into a computer, computer program, computer system, or computer network.

While some initially thought that the last section of this statute might limit its applicability to situations in which viruses are introduced into the computers of others, that is not the case. *State v. Johnston* (N.C.App. 2005) held (among other things), in the context of a related statute, that introducing viruses is a separate offense, not an element of the preceding sections. In other words, subsections (a) and (b)—which criminalize accessing computers of others without authorization—are crimes whether or not computer viruses are introduced into the computer that was accessed.

When one accesses a website, agrees to Terms of Use, and then uses data from the site in violation of the "representations or promises" that were made to access the site, the plain language of N.C.G.S. §14-454(a)(2) seems to apply.[6] In other words, that breach of contract is no longer just a civil violation; it has become a crime. And even on a website that doesn't have Terms of Use, accessing portions of the website that aren't generally intended to be open to the public can be a violation. For computer-related crimes, "authorization" is defined as "having the consent or permission of the owner, or of the person licensed or authorized by the owner to grant consent or permission to access a computer, computer system, or computer network *in a manner not exceeding the consent or permission.*" See *State v. Johnston, noted above.*

It is worth noting that the law provides analogous penalties for those who intentionally damage or alter computer systems or programs, whether by introducing viruses or otherwise. Typical data miners, however, are more likely to face liability for unlawful access than for unlawful damage.

> **2. Computer trespass; penalty (N.C.G.S. §14-458).**
>
> (a) Except as otherwise made unlawful by this Article, it shall be unlawful for any person to use a computer or computer network without authority and with the intent to do any of the following:
>
> (1) Temporarily or permanently remove, halt, or otherwise disable any computer data, computer programs, or computer software from a computer or computer network.
>
> (2) Cause a computer to malfunction, regardless of how long the malfunction persists.
>
> (3) Alter or erase any computer data, computer programs, or computer software.
>
> (4) Cause physical injury to the property of another.
>
> (5) Make or cause to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software

[6] N.C.G.S. 14-453 spells out "exceptions" to the coverage of these criminal statutes. One exception states that these statutes do not "apply to or prohibit" "any terms or conditions in a contract or license related to a computer, … database, …". It remains to be seen whether this will be interpreted to prevent application of the computer crime statutes to cases where access was in violation of Terms of Use, or whether instead Terms of Use will be used to define the scope of authorization that the user had, so as to determine whether he or she exceeded that authorization and hence is guilty. "'Authorization' means having the consent or permission of the owner, or of the person licensed or authorized by the owner to grant consent or permission to access a computer, computer system, or computer network in a manner not exceeding the consent or permission." N.C.G.S. §14-452(a)(1). These apparently conflicting directives have not yet been resolved.

residing in, communicated by, or produced by a computer or computer network.

(6) Falsely identify with the intent to deceive or defraud the recipient or forge commercial electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk commercial electronic mail through or into the computer network of an electronic mail service provider or its subscribers.

For purposes of this subsection, a person is "without authority" when (i) the person has no right or permission of the owner to use a computer, or the person uses a computer in a manner exceeding the right or permission, or (ii) the person uses a computer or computer network, or the computer services of an electronic mail service provider to transmit unsolicited bulk commercial electronic mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider.

(b) Any person who violates this section shall be guilty of computer trespass, which offense shall be punishable as a Class 3 misdemeanor. If there is damage to the property of another and the damage is valued at less than two thousand five hundred dollars ($2,500) caused by the person's act in violation of this section, the offense shall be punished as a Class 1 misdemeanor. If there is damage to the property of another valued at two thousand five hundred dollars ($2,500) or more caused by the person's act in violation of this section, the offense shall be punished as a Class I felony.

(c) Any person whose property or person is injured by reason of a violation of this section may sue for and recover any damages sustained and the costs of the suit pursuant to G.S. 1-539.2A.

This statute was initially aimed at spammers but was expanded and now is in many respects a statutory codification of the common law action for trespass to chattels, providing a civil remedy in addition to criminal penalties. However, it seems to be more limited in many respects, because of its requirements that the defendant must have "disabled" a computer, caused it to "malfunction," caused "physical injury" to it, etc.[7] (Those of us who practice copyright law see a pre-emption issue with respect to subsection (a)(5), and doubt it will survive challenge.)[8]

[7] Many practitioners, for this reason, advise suing for trespass to chattels rather than under this statute if the defendant made unconsented use of resources, causing an immeasurable slow-down in service, and did no other harm to the computers or website.

[8] That is, N.C.G.S. 14-458(a)(5) sets out a cause of action that forbids using a computer with the intent to "make or cause to be made an unauthorized copy…" The Copyright Act provides that "all legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright . . . are governed exclusively by this

C. Federal Statutes

Chief amongst the Federal statutes that can affect data miners is one titled "Fraud and Related Activity in Connection with Computers" (18 U.S.C. §1030). Among other things, it provides that:

> (a) whoever,
>
> ….
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> ….
>
> (C) information from any protected computer if the conduct involved an interstate or foreign communication;
>
> ….
>
> (4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
>
> (5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
>
> (ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
>
> (iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
>
> (B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--
>
> (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
>
> ….

---

title." 17 U.S.C. § 301(a)Since use of the computer is a necessary step in making or causing to be made an unauthorized copy of programs residing on that computer, it seems the statute adds nothing to the Copyright Act's prohibition against willful infringement and hence would be pre-empted by the federal statute and rendered unenforceable.

shall be punished as provided in subsection (c) of this section.

(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

This federal statute broadly defines actionable damage ("(8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information;" and "(11) the term 'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service;"). It also provides a civil remedy for violations, limited to economic damages.

There are additional criminal penalties in the Copyright Act. A good collection of the federal statutes relating to computer crime, as well as reports of recent cases, can be found at the Department of Justice website maintained by the Computer Crime and Intellectual Property Section: http://www.usdoj.gov/criminal/cybercrime

Lesson? There's more at stake than money. These criminal statutes provide up to ten years' imprisonment in addition to hefty fines and the attached civil remedies.[9] If you find yourself thinking, "acceptable business risk," think twice, and consider talking to your lawyer.

IV. CONCLUSION

The ease of Internet access can be misleading. Although the Internet is indeed much like a highway, most websites are not public parks along the way but instead are akin to the stores that line our streets. Just as merchants are entitled to place parts of their premises "off limits" and to charge money for goods taken or movies viewed, website owners have the right to control the use of their sites and the charges (if any) for access and use. As traffic increases, website owners are becoming more savvy about Terms of Use and more concerned about unauthorized access. There are remedies to prevent unauthorized use, and there are penalties for unauthorized use. The wise business owner, and the wise Internet user, must keep these in mind.

[9] In addition to the civil remedies expressly mentioned in the statutes, remember that multiple criminal acts likely will trigger criminal and civil liability under the federal Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §1961 et seq., as well as civil liability under N.C.G.S. §75-1.1 *et seq.*, commonly referred to as the Unfair and Deceptive Trade Practices Act.