Educational Administration: Theory and Practice
2024, 30(5), 7923 - 7931
ISSN: 2148-2403
https://kuey.net/

Research Article

Cyber Torts: Unfolding Trends Of Common Law

Soniya Dhantole[1*], Dr. Sunil Kumar Pandey

[1*]Research Scholar (Law) School of Law and Legal Study Sanjeev Agrawal Global Educational University Bhopal (M.P.)
[2]Dean, School of Law and Legal Study, Sanjeev Agrawal Global Educational University Bhopal (M.P)

Citation: Soniya Dhantole , (2024), A Cyber Torts: Unfolding Trends Of Common Law, *Educational Administration: Theory and Practice*, *30*(5), 7923 – 7931
Doi: 10.53555/kuey.v30i5.4271

ARTICLE INFO

ABSTRACT

A tort is a negligent or intentional act is done by someone that injures someone else in some way. CyberTorts are simply a tort done over cyberspace. Cyber torts are very significant because they are on the rise and are still crimes that can have serious effects on society. Everyone should be exposed to the dangers and damages caused by cyber torts because technology is an important aspect in everyone's lives, especially now.

Online torts include trespass to chattels, conversion, cyber talking/harassment, and cyber defamation. Trespass to chattels includes all those spyware, spam emails, and scrapers you see some of the time. Conversion involves negligent or intentional stealing of other peoples domain names online. Cyber stalking/harassment happens a lot in social networks like Facebook and Whats App[1] where they have millions and millions of users. And cyber defamation also can happen a lot on social networks and forums. As you can see, these types of Online torts are serious issues that happens probably everyday that can result in serious harm to the public including us. This article is designed to cover all the contemporary issues of Online Torts.

Keywords- Cyber Torts, Cyber Crimes, Cyber Space, Unlawfull Acts, Contemporary Issues.

Introduction

A space without frontiers is known as cyber space and the law governing it is known as cyber law. The world of information and technology has surfaced within little time span, with the invention of computer and internet.

The unlawful acts committed by an individual or a group using computers as a tool and cyberspace as a medium is known as cyber torts. Internet provides a reasonable amount for criminal enterprises. The various acts and laws passed by Indian government have thrown light on the advancement and progress of cyber technology. With increasing circulation of electronic information and awareness, laws are in need. We have tried in our research to explore a less focused and under-viewed area of law. Online tort is an emerging area which requires a special attention. Cyber law encompasses electronic communication, freedom of expression, intellectual property rights, jurisdiction and choice of law, privacy rights etc. Nations and private organizations, all aim for better net policing as it looks increasingly daunting due to the fact of security measures and to avoid accidents, which have been quite frequent in the past and if not improvised- it can be a serious threat.

Many issues have been included under online torts, like cyber wrong and civil liability, defamation in cyber space, cyber squatting, litigations etc. many landmark cases are the sole proof of the importance of immediate tortious acts and law for better judicial satisfaction and betterment of natives.

The Internet has given rise to a new industry for the online publication and consumption of obscene materials. Millions of people around the world are visiting web-sites catering to this product. These Internet sites represent the largest growth sector of the digital economy. But as the use of internet is grown by the time, it is misused also and a large number of different types of crime are committed through this internet as hacking, cyber stalking, cyber defamation, cyber fraud, cyber forgery, cyber terrorism, IPR infringement etc. Cyber obscenity is one of them.

Obscenity is very sensitive issue all over the world yet there is no settled definition of the word 'obscenity' under any law. What is nude art or sexually explicit thing for one person may be obscene or porn for another.

Obscenity on the Internet is not a typical wrongdoing.. Internet has provided a medium for the facilitation of crimes like obscenity or pornography. Cyber obscenity is the trading of sexually expressive materials within cyber space. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression; it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as "offensive to modesty or decency; lewd, filthy, repulsive". It is very difficult to testify whether any pornographic material is illegal or not? One particular pornographic material may be illegal in Indiabut not in other countries. The test for obscenity was first laid down in the case of Regina v. Hicklin[2], as a tendency to deprave corrupts those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall."

A Broad Classification of Online Tort:

1. **Cyber Stalking-** Cyber stalking occurs when a person is followed and persuaded online. In other words, their privacy is invaded. It is a form of harassment, and can disrupt the life of the victim leaving them feeling afraid and threatened. The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantlybombarding the victim with emails etc.
2. **Cyber Breach of Privacy-** With the advent of multi channel televisions all over the world, and fast spreadinginternet network, the privacy of an ordinary man is increasingly under threat. Breach of privacy is a kind ofcyber tort which affects a common man.
3. **Cyber Obscenity-** Cyber space offers a very wide range of pornography, and makes children and women vulnerable of trafficking. This also includes child pornography and internet rape. The term 'Cyber Space' was first used by William Gibson in his novel 'Neuromancer' 1982. The word Cyber or Cyber Space denotes a virtual environment within which networked computers' activity takes place and Obscenity is any statement or act which strongly offends the prevalent morality of the time. Obscenity is a legal term that applies to anything offensive to morals and is often equated with the term 'Pornography'. Obscenity is derived from the Latin word obscaena. In R v. Hicklin3, the word obscene was clearly defined as "Any matter which has the tendency to deprave or corrupt those whose minds are open to immoral influence.

"The Hicklin's test states that a governing body may prohibit anything that "depraves and corrupts those whose minds are open to such immoral influences and into whose hands a publication of this sort might fall.
Cyber-obscenity is the trading of sexually expressive materials within cyber space. The cyber pornography or obscenity debate is very complex because pornography is not necessarily illegal. The test is the United Kingdom and other jurisdictions is whether or not the materials are obscene and deprave its viewers, but there are considerable legal and moral differences regarding the criteria that enable law enforcers to establish obscenity and depravation. In Britain, for example, individuals daily view risqué images though the various facets of the mass media. These same images might be legally obscene in some Islamic societies, yet they are deemed perfectly acceptable in more permissive countries.
According observation of Supreme Court of India given in the case of Chandrakant Kalyandas Kakodar v. The State of Maharashtra And Ors[4] "the concept of obscenity would differ from country to country depending on the standards of morals of contemporary society." And that obscenity has a tendency to deprave and corruptthose whose minds are open to such immoral influences.

4. **Cyber Defamation-** Due to expansiveness of the internet for a, defamation is quite possible. Cyber defamation is statements that are unflattering, annoying, irksome, embarrassing or hurt one's feelings are not actionable. It is an act of imputing any person with intent to lower the person in the estimation of the right-thinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium. E.g. hacking of a mail account and sending mails from his account to some other with intent to defame him.
5. **Harassment via e-mails-** Harassment through e-mails is not a new concept. It is very similar to harassing through letters. Eg. Sending mails constantly, sometimes emotionally blackmailing or threatening a person.This is a very common type of harassment via e-mails.
6. **Dissemination of obscene material/ Indecent exposure/ Pornography (basically child pornography) / Polluting through indecent exposure-** Pornography on the net may take various forms. It may include the hosting of web site containing these prohibited materials. Use of computers for producing these obscene materials, downloading obscene material through the Internet. These obscene matters may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind. The well known case of pornography is the Bombay case[5] wherein two Swiss couple used to force the slum children for obscene photographs. The Mumbai police later arrested them.
7. **Unauthorized control/access over computer system:-**This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking" to prevent confusion as the term used in the Indian Information Technology Act of 2000 (hereinafter referred as "the Act") is much wider

than hacking.

8. **E mail spoofing**-A spoofed e-mail may be said to be one, which misrepresents its origin. It shows its originto be different from which actually it originates.
9. **Computer vandalism:-**Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.
10. **Intellectual Property crimes / Distribution of pirated software:** Intellectual property consists of a bundle ofrights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc.
11. **Cyber terrorism against the government organization:-**At this juncture a necessity may be felt that what is the need to distinguish between cyber terrorism and cyber torts. Both are dangerous acts. However there is a compelling need to distinguish between both these acts. A cyber tort is generally a domestic issue, whichmay have international consequences, however cyber terrorism is a global concern, which has domestic as well as international consequences. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc. Technology savvy terrorists are using 512-bit encryption, which is next to impossible to decrypt.

Cyber terrorism may be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives"
Another definition may be attempted to cover within its ambit every act of cyber terrorism. A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of services or means of communications essential to the community or in damaging property with the view to:

a. Putting the public or any section of the public in fear; or
b. Affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or
c. Coercing or overawing the government established by law; or
d. Endangering the sovereignty and integrity of the nation and a cyber terrorist is the person who uses the computer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof is an act of cyber terrorism.

12. **Trafficking:** Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms weapons etc. These forms of trafficking are going unchecked because they are carried on under pseudonyms.
13. **Fraud & Cheating:** Online fraud and cheating is one of the most lucrative businesses that are growing todayin the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that havecome to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc.

The distinction between Cyber Crime and Cyber Tort

There is specific distinction between cyber crime and cyber torts which has to be cleared when we arediscussing cyber torts.
The cyber crime includes hacking/cracking, Possession of unauthorised information , cyber terrorism against government organisations,distribution of pirated software, harassment through emails, cyber stalking, dissemination of obscene material on the internet, defamation, hacking/cracking, indecent exposure, computer vandalism, transmitting virus, internet intrusion, unauthorised control over computers, pornography, exposing the youth to indecent material, Trafficking.
Online torts include cyber stalking, breach of privacy, cyber obscenity and cyber defamation. So there may be some elements which may be common in both but there are several differences between the two.

Liability of intermediaries and the author under Indian law

The Internet has made it simpler than any time in recent memory to spread a tremendous sum and assortment of data around the world. Any individual can write any statement, including the defamatory one, allalone or a third individual's virtual profile.In this scenario, the question which naturally arises is: who can be sued by the person against whom such defamatory statement has been made.
Under the operative Indian law, the person who made such statement as well as its distributor and publishers can be sued. Apart from the author of such statement, intermediaries, the website holder, the internetservice providers, as well as the other users on whose profiles defamatory statements have been written by the author, can be sued in their capacity as a publisher of defamatory statements and can be held liable for such statements. It is to be noted that such intermediaries may not be aware of such defamatory statements by the author on their own virtual profile.The Information Technology Act, 2000 gives immunity to network service

providers. According to Section 79 of the Act, a 'network service provider' (defined as a person who on behalf of another person receives, stores or transmits the electronic messages) shall not be liable under the Act, or Rules or Regulations made thereunder, for any third party information or data made available by him if he proves that the offence or contravention was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence or contravention. However, the Information Technology Amendment Act, 2008 provides limited immunity to the intermediaries such as internet service providers and other interactive web service providers. The amendment bears a certain degree of similarity to the prevailing law in the United States of America. In USA, intermediaries are exempted from liability under defamation if (i) they prove that they have no control over the statement or content and (ii) they remove such statement or content from their website or network immediately upon receiving the notice from the plaintiff.
The amended Section 79 of this Amendment Act provides the mechanism equivalent to the law of USA. Following are the relevant provisions of the Information Technology Act (after the said amendment comes intoforce). This section runs as follows:
(1) Notwithstanding anything contained in any other law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available by him.
(2) The provisions of sub-section (1) shall apply if—
(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored; or
(b) the intermediary does not—
(i) initiate the transmission,
(ii) select the receiver of the transmission, and
(iii) select or modify the information contained in the transmission.
(3) The provisions of sub-section (1) shall not apply if—
(a) the intermediary has conspired or abetted in the commission of the unlawful act;
(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that anyinformation, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disableaccess to that material on that resource without vitiating the evidence in any manner.
(4) Intermediary shall observe such other guidelines as the Central Government may prescribe in this behalf. Explanation.--For the purpose of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary.
Further the Act defines the term 'intermediary' in section 2(w). It says that, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes, but does not include body corporate referred to in section 43A.

Analysis of the Statutory Provisions

The Information Technology Act 2000 was undoubtedly a welcome step at a time when there was no legislation on this specialised field. The Act has however during its application has proved to be inadequate to acertain extent. The various loopholes in the Act are:

1. The rush in which the enactment was passed, without adequate open civil argument, did not by any stretch of the imagination fill the coveted need Experts are of the supposition that one reason for the deficiency of the enactment has been the rush in which it was passed by the parliament and it is likewise a reality that adequate time was not given for open level headed discussion.
2. "Cyber laws, in their very preamble and aim, state that they are targeted at aiding e-commerce, and are not meant to regulate online torts. The main intention of the legislators has been to provide for a law to regulate the e-commerce. It is one of the reasons for its inadequacy to deal with cases of online crime. The reason being that the preamble of the Act clearly state that the Act aims at legalizing e-commerce. However it does not stop here. It further amends the I.P.C., Evidence Act, Banker's Book Evidence and RBI Act as well. The Act aims to deal with all matters connected therewith or incidental thereto. It is a cardinal rule of interpretation that "text should be read as a whole to gather the meaning". The preamble, if read as a whole, makes it very clear that the Act equally aims at legalizing e-commerce and to curb any offences arising there from.
3. Some Online torts are not covered by the Act: The recent cases including Cyber stalking cyber harassment, cyber nuisance, and cyber defamation have shown that the I.T. Act 2000 has not dealt with those offences. Further it is also contended that in future new forms of online torts will emerge which even need to be taken care of. However the I.T. Act, 2000 (as amended) read with the Penal Code is capable of dealing with these felonies.
4. Online crime in the Act is neither comprehensive nor exhaustive: We need dedicated legislation on online crime that can supplement the Indian Penal Code. The IT Act, 2000 is not comprehensive enough and doesn't even define the term 'cyber crime. India, as a nation, has to cope with an urgent need to regulate

and punish those committing cyber torts, but with no specific provisions to do so. Supporters of the Indian Penal Code School vehemently argue that IPC has stood the test of time and that it is not necessary to incorporate any special laws on cyber crime. This is because it is debated by them that the IPC alone is sufficient for all kinds of crime. However, in practical terms, the argument does not have appropriate backing. It has to be distinctly understood that cyber crime and cyberspace are completely new whelms, where numerous new possibilities and opportunities emerge by the day in the form of new kinds of crimes.

5. Ambiguity in the definitions: The definition of hacking provided in section 66 of the Act is very wide and capable of misapplication. There is every possibility of this section being misapplied and in fact the Further section 67 is also vague to certain extent. It is difficult to define the term lascivious information or obscene pornographic information.
6. Uniform law: The need of the hour is a worldwide uniform cyber law to combat online torts. Online torts are a global phenomenon and therefore the initiative to fight it should come from the same level.
7. Lack of awareness: One important reason that the Act of 2000 is not achieving complete success is the lack of awareness among the s about their rights. Further most of the cases are going unreported. If the people are vigilant about their rights the law definitely protects their right
8. Jurisdiction issues: Jurisdiction is also one of the debatable issues in the cases of online crime due to the very universal nature of cyber space. With the ever-growing arms of cyber space the territorial concept seems to vanish. New methods of dispute resolution should give way to the conventional methods. The Act of 2000 (as amended) is very silent on these issues.
9. Extra territorial application: Though Section 75 of the Act provides for extra-territorial operations of this law, but they could be meaningful only when backed with provisions recognizing orders and warrants for Information issued by competent authorities outside their jurisdiction and measure for cooperation for exchange of material and evidence of computer crimes between law enforcement agencies.
10. Raising a Cyber army: By using the word 'Cyber army' by no means is an idea of virtual army. It is required to establish a well equipped task force to deal with the new trends of hi tech crime. The government has taken a leap in this direction by constituting online crime cells in all metropolitan and other important cities. Further the establishment of the Cyber Crime Investigation Cell (CCIC) of the Central Bureau of Investigation (CBI) is definitely a welcome step in this direction. There are many cases in which the C.B.I has achieved success. The present position of cases of cyber crime is –
11. Cyber savvy bench:- Cyber savvy judges are the need of the day. Judiciary plays a vital role in shaping the enactment according to the order of the day. One such stage, which needs appreciation, is the P.I.L., which the Kerela High Court has accepted through an email. The role of the judges in today's word may be gathered by the statement- judges carve 'law is' to 'law ought to be'. Recently the Law Commission has highlighted the requirements for introducing e-courts in India. There is one area of Governance where IT can make a huge difference to Indian public is in the Judicial System.
12. Dynamic form of online crime: Even though the capability to fight online intrusions has been improved, the problem is growing even faster and we are falling further behind." The creativity of human mind cannot be checked by any law. Thus the only way out is the liberal construction while applying the statutory provisions to online crime cases.
13. Hesitation to report offences: As stated above one of the fatal drawbacks of the Act has been the cases going unreported. One obvious reason is the non-cooperative police force.

Capacity of human mind is immeasurable. It is not possible to eliminate cyber crime or either cyber torts from the cyber space. It is quite possible to check them. No legislation has succeeded in totally eliminating crime from the globe. The only possible step is to make people aware of their rights and duties(to report crime as a collective duty towards the society) and further making the application of the laws more stringent to keep a check. Undoubtedly the Act is a historical step in the cyber world. A word of caution for the pro-legislation school that it should be kept in mind that the provisions of the cyber law arenot made so stringent that it may retard the growth of the industry and prove to be counter-productive andat the same time a vigil check should be kept on its misappropriation and further consequences.

Application of Classic Principles of torts

Trespass to movables is a tort whereby the encroaching party has purposefully meddled with someone else's lawful possession of a mobile individual property. The interference can be any physical contact with the chattel in a quantifiable way or any dispossession of the chattel whether by taking it, destroying it, or barring the owner's access to it. As opposed to the greater wrong of conversion, trespass to chattels is argued to be actionable per se.

The origin of the concept comes from the original writ of trespass *de bonis asportatis*. As in most otherforms of trespass, remedy can only be obtained once it is proven that there was direct interference regardless of damage being done, and the infringing party has failed to disprove either negligence or intent.

In some common law countries like the United States and Canada, a remedy for trespass to chattels canonly be obtained if the direct interference was sufficiently substantial to amount to dispossession, or alternatively where there had been an injury proximately related to the chattel.[6]

Features of the claim

1. Lack of consent- A vendor can attempt to dispute a trespass claim on the grounds that the user consented to the terms of the contract. Even if consent was given for certain access, a user may still have a valid trespass to chattels complaint if the vendor has exceeded the contractual terms, if the contract is found to misrepresent the actual functioning of the product, or if the consent has been withdrawn. A vendor can be held liable for "any use exceeding the consent" given.[7]

2. Actual harm- The precise criteria for ascertaining actual harm vary among states. In California, for instance, an electronic message can be deemed a trespass where the message interferes with the target computer's operation, as long as a plaintiff can demonstrate either actual hardware damage or actual impaired functioning.[8] But the general concept of requiring impaired computer functioning has been adopted consistently and in showing impaired computer functioning, courts have usually emphasized system unavailability.

3. Intentionality- In clarifying the meaning of intentionality in the context of a trespass to chattels claim, "intention is present when an act is done for the purpose of using or otherwise intermeddling with a chattel or with knowledge that such an intermeddling will, to a substantial certainty, result from the act, and it is not necessary that the actor should know or have reason to know that such intermeddling is a violation of the possessory rights of another." [9]

Trespass to chattels in the electronic age

The antiquated common law tort of trespass to chattels has been invoked in the modern context of electronic communications to combat the proliferation of unsolicited bulk email, commonly known as spam.[10]

What's more, a few organizations have effectively utilized the tort to block certain individuals, typically competitors, from getting to their servers. Though courts initially endorsed a broad application of this legal theory in the electronic context, more recently other jurists have narrowed its scope. As trespass to chattels is extended further to computer networks, some fear that plaintiffs are using this cause of action to quash fair competition and to deter the exercise of free speech; consequently, critics call for the limitation of the tort to instances where the plaintiff can demonstrate actual damages.

Rules for Application of Trespass to chattels to Electronic Wrongs

The trespass to chattels tort punishes anyone who substantially interferes with the use of another's personal property, or chattels. Plaintiffs must show that the offender had intentional physical contact with the chattel and that the contact caused some substantial interference or damage. The courts that imported this common law precept into the advanced world contemplated that electrical signs bridging systems and through exclusive servers may constitute the contact important to bolster a trespass guarantee. Applying this common law action to computer networks, plaintiffs must first prove that they received some type of electronic communication viz. typically bulk e-mail or spam, that the defendant intentionally sent to interfere with the plaintiff's interest in his or her property and second that this communication caused a quantifiable harm to their tangible property, such as impaired functioning of the computer, network or server.[11]

Early applications of trespass to chattels to computer networks

In the late 1990s, when the World Wide Web was in its infancy, courts were more receptive to extending the trespass to chattels tort to the electronic context. In CompuServe Inc. v. Cyber Promotions, Inc., a 1997 case that was the first to extend the trespass theory to computer networks, the court held that a marketing company's mass mailing of a high volume of unsolicited advertisement emails to CompuServe subscribers constituted an actionable trespass to chattels.[12] CompuServe customers repeatedly received unwanted advertisements from Cyber Promotions, a company that specialized in sending marketing email in bulk.Cyber Promotions also modified its equipment and falsified other information to circumvent CompuServe's anti-spam measures. Due to the high volume of email, CompuServe claimed damage to its servers as well as money lost dealing with customer complaints and dissatisfaction. CompuServe also extended its damages claim to its subscribers who spent time deleting unwanted email. The court held that Cyber Promotions' intentional use of CompuServe's proprietary server was an actionable trespass to chattels and granted a preliminary injunction enjoining the spammer from sending unsolicited advertisements to any email address maintained by CompuServe. Cyber Promotions' persistence in sending email to CompuServe's servers after receiving notification that CompuServe no longer consented to the use weighed heavily in favor of a finding of trespass.

In 1998, a case in the Eastern District of Virginia involving America Online more firmly established the use of the trespass to chattels tort as a spam-fighting tool. In America Online, Inc. v. IMS, the court held that the owner of a marketing company committed trespass to chattels against an Internet service provider's (ISP) computer network by sending 60 million unauthorized email advertisements to the ISP's subscribers after being notified that the spam was unauthorized.[13] The court found that the defendant, intentionally and without authorization, caused contact with the plaintiff's computer network by sending the bulk email messages. Such contact injured the plaintiff's business goodwill and diminished the functioning of its computer network.

Similarly, in America Online, Inc. v. LCGM, Inc., a company engaging in pornographic website advertising sent a deluge of spam to America Online's customers, and, in doing so, also forged the America Online's domain name in an effort to trick customers into opening the emails.[14] The court once again held that a website operators' transmission of unsolicited bulk emails to customers of an Internet service provider, using the provider's computers and computer network, constituted trespass to chattels.

In America Online, Inc. v. Prime Data Systems, Inc., the defendants sent millions of spam emails to America Online's subscribers advertising computer software programs designed to facilitate bulk emailing by allowing users to harvest email addresses from the plaintiff's member directories, chat rooms, and electronic bulletin boards.[15] The defendants also used technology designed to avoid America Online's spam filtering mechanisms. The defendants frequently used false and deceptive "headers" in email messages to make it appear as if America Online had sent the messages. The increased demand on America Online's servers resulting from the spam caused substantial delays of up to 24 hours in the delivery of all email to America Online members, forcing America Online to temporarily stop accepting any new messages. As the spam problem grew worse, America Online had to purchase millions of dollars worth of additional equipment to increase the capacity of its

servers to handle the volume of email. The court held that this activity constituted a trespass to chattels and awarded injunctive relief, reasonable attorneys' fees and costs, as well as damages.

Screen Scraping and Data Harvesting

Since the early spam cases, courts have extended the electronic trespass to chattels theory even further to encompass screen-scraping and other data "harvesting." Screen-scraping is the practice of taking information from another website, generally through the use of search agent software, and "harvesting" the data for one's own commercial use. For example, travel websites frequently use this tactic to offer a host of options and prices gleaned from various airlines' sites. Because the courts have entertained such litigation, some companies have specifically banned the conduct in their terms and conditions statements.[16]

In eBay v. Bidder's Edge (2000), eBay successfully used the trespass to chattels tort to prevent Bidder's Edge from employing spiders to cull information about its auctions to display on its own website.[17] Although Bidder's Edge's robots only consumed a small percentage of eBay's computer resources, the court noted that the plaintiff need not demonstrate current substantial interference as conduct which constituted a use of another'sproperty is enough to sustain a trespass to chattels claim. In light of this, the court found that eBay had demonstrated a sufficient likelihood of future injury to warrant granting a permanent injunction: "If the court were to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers."[18]

Register.com, Inc. v. Verio, Inc.[19] (2000) is a further example of this temporary trend in which plaintiffs did nothave to demonstrate any real interference. Register.com, a domain name registry service, sued competitor Veriofor using Register.com's proprietary WHOIS look-up service to find potential leads among its customer base. The court found that, by continuing to access Register.com's online customer database after being told to stop, Verio was trespassing on Register.com's WHOIS server. Register.com had specifically withdrawn its consent to Verio's use of search robots to review Register.com's customer list. The court held that Verio caused harm toRegister.com's files through the use of these search robots and that the searches improperly taxed Register.com's server capacity.

These holdings gave the court license to expand the applicability of trespass to chattels to computer networks even further. In Oyster Software v. Forms Processing (2001), the Northern District of California determined that a plaintiff need not demonstrate any physical interference with a server at all to sustain a trespass to chattels claim and consequently denied the defendant's motion for summary judgment, even though there was no evidence of damage to the plaintiff's computer system.[20] Although Oyster conceded that there was no evidence that the defendant's activities had interfered in any way with the functioning of Oyster's computer system, the court nonetheless denied FPI's motion for summary judgment. According to the court, following thedecision in eBay, plaintiffs only need to demonstrate that the defendant's actions "amounted to a 'use' of Plaintiff's computer," and the court determined that copying the metatags amounted to a use.[21]

These cases indicate that, at least in California, a plaintiff did not have to demonstrate any kind of actual interference with the computer system to successfully claim trespass to chattels.

The Criticism against the Tort's Expansion

However, some courts subsequently limited tort claims for electronic trespasses, in that a complaining party may be unable to recover for lack of real harm if the party did not suffer any tangible damage to their property.

The Supreme Court of California reversed the trend exemplified by Oyster in the seminal case Intel v. Hamidi,[22] reaffirming the need for a demonstration either of actual interference with the physical functionality of the computer system or of the likelihood that this would happen in the future. Although Intel conceded that Hamidi's emails caused neither physical damage nor any disruption to their computer system, they alleged that the economic productivity lost due to the disruption caused by the emails could sustain a trespass claim. The Supreme Court of California disagreed, holding that the tort does not extend to claims in

which the electronic communication involved "neither damages the recipient computer system nor impairs its function."[23] In reaching this conclusion, the court criticized the understanding of eBay advanced in Oyster, explaining that previous cases in which courts have found trespass to chattels in the electronic setting have involved either "actual or threatened interference with the computers' function."[24] To that effect, the court in Oyster misconstrued the holding in eBay; trespass requires more than use a use--it requires an actual or threatened interference with the physical functionality of the system.

Although the vast majority of states have yet to determine the applicability of the trespass to chattels theory, the courts that have addressed the issue have applied Intel and required that the plaintiff demonstrate damage to the computer system. A supreme court in New York in School of Visual Arts v. Kuprewicz[25] denied the defendant's motion to dismiss for failure to state a claim on the trespass to chattels claim because the plaintiff had alleged actual damage to the functionality of the computer system, which Intel requires; the defendant had sent enough e-mails that it reduced the computer system's functionality and drained the hard drive's memory. The Fourth Circuit in Omega World Travel v. Mummagraphics, Inc.[26] also followed Intel, although this resulted in granting a motion for summary judgment for the defendant because the plaintiff did not allege any actual damage on its computer system. The court clarified that Oklahoma courts have yet to recognize the validity of a trespass to chattels claim based on an electronic intrusion to a computer system, but if it were to recognize it, the plaintiff would need to allege more than nominal damages, which in this case it had not.

Conclusion

Although a number of commentators have expressed enthusiasm over the increasing application of intellectual property to intangible property and the extension of the trespass to chattels doctrine to computer networks,[27] a number of detractors have expressed concern over the consequences of extending the theory to protect electronic communications that do not actually damage the computers in question but only cause nominal damage due to their content.[28] Primarily, these critics worry that extending trespass to chattels in this fashion would stifle free speech on the internet because any unwelcome email might constitute a trespass and may subject the sender not only to civil liability under the trespass theory but to criminal liability as well.[29] This would presumably reduce people's willingness to communicate freely on the Internet and curtail the Internet's ability to function as an open, democratic forum.30 Particularly in situations where the electronic communication is an email that contains speech that is of importance to the public and the communications do not hamper the functionality of the recipient's computer system, First Amendment free speech protections ought to outweigh the property right in the unharmed computer system.[31] Similarly, critics have also expressed concerns that plaintiffs have employed the doctrine to stifle legitimate competition.[32] For example, the screen-scraping cases indicate that courts might interpret trespass to chattels in such a way that allows major corporations to prevent price comparison sites from employing harmless bots to aggregate information that users want in a readily accessible format since it might encourage consumers to look elsewhere.[33]

Critics of the theory's extension to computer networks also note greater theoretical problems with the applicability of a real property theory to intellectual property. In order to explain why real property theories might extend to the Internet, proponents equate "cyberspace" with real land, arguing that owners of computer servers should have the same right of inviolability as owners of land receive to promote greater efficiency in transactions.[34] However, even if some aspects of cyberspace resemble real space, detractors contend that cyberspace is not like real land at all because "the 'placeness' of cyberspace is a matter of ongoing social construction."[35] Furthermore, even if granting property rights might help to avoid problems of inefficiency and under-cultivation in the context of real property, critics note that nothing suggests that the same principles would also be effective in the context of computer networks—especially because the problem of under-cultivation does not tend to occur online.[36]

Damages from a trespass claim are limited to the actual harm sustained by the plaintiff which can include economic loss consequent on the trespass - e.g. loss of profit on a damaged chattel. In cases of dispossession, the plaintiff is always entitled to damages if they can prove the dispossession occurred, even if no quantifiable harm can be proven.

A related tort is conversion, which involves an exercise of control over another's chattel justifying restitution of the chattel's full value. Some actions constitute trespass and conversion; in these cases, a plaintiff must choose which claim to make based on what amount of damages they seek to recover.

References

1. An application used for instant messaging service in smartphones.
2. [1868] LR 3 QB 360
3. [1868] LR 3 QB 360
4. 1970 AIR 1390, 1970 SCR (2) 80
5. TNN | Nov 15, 2002, 12.09AM IST
6. See Restatement (Second) of Torts, 1965.

7. Ibid, S. 256.
8. Intel Corp. v. Hamidi, 30 Cal.4th 1342 (2003).
9. Section 217 of the Restatement (Second) of Torts
10. Marjorie A. Shields, Applicability of Common-Law Trespass Actions to Electronic Communications, 107 A.L.R.5th 549.
11. eBay v. Bidder's Edge, 100 F.Supp.2d 1058 (N.D. Cal. 2000).
12. CompuServe Inc. v. Cyber Promotions, Inc., 962 F.Supp. 1015 (S.D.Ohio 1997).
13. America Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998).
14. America Online, Inc. v. LCGM, Inc., 46 F.Supp.2d 444 (E.D. Va. 1998).
15. America Online, Inc. v. Prime Data Systems, Inc., 1998 WL 34016692 (E.D. Va. 1998).
16. Wawa's website terms and conditions, which forbids users to employ screen scraping programs.
17. eBay v. Bidder's Edge, 100 F.Supp.2d 1058 (N.D. Cal. 2000).
18. eBay v. Bidder's Edge, 100 F.Supp.2d 1058 (N.D. Cal. 2000).
19. Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000).
20. Oyster Software v. Forms Processing, 2001 WL 1736382 (N.D.Cal. 2001). **21.**Oyster Software v. Forms Processing, 2001 WL 1736382 (N.D.Cal. 2001). **22.**Intel v. Hamidi, 30 Cal.4th 1342 (Cal. 2003).
21. Ibid.
22. Ibid.
23. School of Visual Arts v. Kuprewicz, 771 N.Y.S.2d 804 (N.Y. Sup. 2003).
24. Omega World Travel v. Mummagraphics, Inc., 469 F.3d 348 (4th. Cir. 2006).
25. See, e.g., David M. Fritch, “Click Here For Lawsuit – Trespass to Chattels in Cyberspace,” 9 J. Tech. L. & Pol'y 31 (June 2004).
26. Electronic Frontier Foundation, Amicus Brief in Intel v. Hamidi (Jan. 18 2000) Laura Quilter, The Continuing Expansion of Cyberspace Trespass to Chattels, 17 Berkeley Tech. L.J. 421 (2002). Shyamkrishna Balganesh, “Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass,” 12 Mich. Telecomm. & Tech. L. Rev. 265 (Spring 2006).
27. Amicus Brief in Intel v. Hamidi at 6.
28. Id.
29. Id. at 28-29.
30. EFF Analysis of Trespass to Chattels Legal Theory.
31. Law Professors' Amicus Brief in eBay v. Bidder's Edge at 14.
32. Lastowka, “Decoding Cyberproperty” at 46
33. Id. at 45.
34. Id. at 55.