

International Journal of Law and Information Technology  
Spring, 2007

**\*90 CYBER-TRESPASS AND 'UNAUTHORIZED ACCESS' AS LEGAL MECHANISMS OF ACCESS CONTROL: LESSONS FROM THE US EXPERIENCE**

Mary W. S. Wong [FN1]

Copyright © 2007 by Oxford University Press; Mary W. S. Wong

**Abstract**

The common law doctrine of trespass to chattels has recently been revived and applied by courts in the United States (US) to cover intrusions (in the form of electronic signals) to computer systems connected to the Internet. These cases represent judicial recognition of the need to protect certain unwanted intrusions in cyberspace, though the principles developed therewith are remarkably expansive. As such, they overlap with the concept of 'unauthorized access' under computer misuse legislation in the US and elsewhere. This overlap has yet to be judicially acknowledged. Since the US, the United Kingdom and other common law countries not only share a common law ancestry but also 'unauthorized access' principles as the primary trigger for computer misuse, this paper seeks to examine the consequences of developing a broad cyber-trespass doctrine beyond the US, and its corresponding implications for judicial interpretations of 'unauthorized access' in the common law world.

**\*91 1 Introduction**

In the realm of torts and what may conveniently be termed 'cyberlaw' [FN1], an interesting point of comparison (or perhaps more accurately, difference) between the United States (US) and English [FN2] common law can be found in the development of the cause of action in cyber-trespass in the former jurisdiction. Where the US courts have been faced with several cases concerning acts of unwanted interference with computer systems and networks that have been alleged to constitute trespasses to such systems and networks chattels, there has been little (if any) judicial activity on this front elsewhere. The US traces its common law ancestry to the United Kingdom, and there remain many shared as well as similar causes of actions and legal principles, including those pertaining to trespass to chattels. At the same time, the Internet (or more generally, 'cyberspace') is geographically borderless and operates along similar technical principles and social norms worldwide. The recent development of an action in cyber-trespass in the US, based on the 'ancient' [FN3] common law doctrine of trespass to chattels, is thus of interest to common lawyers worldwide, particularly given the comparative litigation silence elsewhere [FN4].

Besides academic interest in doctrinal development, however, a further point of interest arises in the context of cyber-trespass. The breadth of the US cyber-trespass action points to a possible overlap between the trespass cause of action and notions of 'unauthorized access' as the concept is utilized in computer misuse statutes. Given the fact that the UK has had a Computer Misuse Act for a number of years (as has other common law jurisdictions) and the increasing adoption of such statutes (and the corresponding foundation of liability on acts of 'unauthorized access' [FN5]) by other countries, the implications of a broader and developing common \*92 law

doctrine of cyber-trespass, beyond the boundaries (such as they are) of tort, necessitate further attention.

This article is thus broadly divided into two Parts. Part I highlights the reasons for the evolution of the cyber-trespass action in the US, noting salient differences between a trespass to chattels under US law and 'traditional' English common law. Part II notes the overlap between cyber-trespass (a civil action) and 'unauthorized access' (commonly a criminal act under several forms of computer misuse legislation [FN6]), with an eye toward analyzing how the comparatively more numerous US cases on this issue [FN7] might impact interpretation of the phrase in the UK and elsewhere, and vice versa.

## 2 The Development of Cyber-Trespass in the US and Its Implications for Other Common Law Jurisdictions

### 2.1 Back to the English Common Law: Brief Notes on the 'Traditional' Doctrine of Trespass to Chattels

It may first be useful to distinguish between various forms of, and usages of the word, 'trespass'. Legally speaking, trespass could mean the traditional forms of action dictated by the nature of the writ upon which the action lay: in English law, the distinction here lies between a 'writ of trespass' and a 'writ of trespass on the case' (or, more briefly and commonly, 'trespass' and 'case'.) The importance of this distinction to cyber-trespass lies in the fact that an action in trespass was actionable *per se* where trespass on the case required proof of damage; the implication of this will be further discussed below. The second distinction to be made with respect to the word 'trespass' as regards a person's property is that trespass can be of two different kinds; *viz.*, trespass to land (real property) or trespass to goods (chattels.) As will be seen in the discussion of recent US case law (below), this distinction, at least in terms of the damage requirement, seems less significant in the realm of trespass to goods in English law.

The law of cyber-trespass, as developed in the US courts, is basically an application of the general principles relating to trespass to chattels. While it would have been helpful to look to the English common law to see if these principles are similar, and hence could inform both the likelihood as well as the nature of the development of an action in cyber-trespass by \*93 common law courts outside of the US, there are few English case authorities, and (perhaps correspondingly) relatively sparse academic and textbook discussions of its scope and potential development [FN8]. For purposes of the present discussion, it would be helpful to set out some of the basic parameters and principles behind the English law of trespass to chattels.

A useful starting point is the question whether, under English law, an action in trespass to goods is actionable *per se* (i.e., without the need for any damage to have been caused by the act of trespass.) Although the current editors of *Salmond and Heuston on the Law of Torts* and *Winfield & Jolowicz on Tort* are of the opinion that, under English law, trespass to goods is actionable *per se* [FN9], other authors do not take such a clear stance [FN10]. *Winfield & Jolowicz* note, in addition, that where the interference is unintentional, actual damage may be required for policy reasons. Margaret Brazier argues in *Street on Torts* that, for consistency with most prior law and in accordance with general principles of trespass, a trespass to goods ought to be actionable *per se* [FN11].

The possibility that trespass to goods is actionable *per se* under English law can be traced back to the distinction between trespass and case, as highlighted earlier. An action in trespass, in contrast to an action on the case, was actionable *per se*, the only requirements for such an action were basically that the injury [FN12] com-

plained of was both 'forcible' - meaning physical interference with another's person or property - and 'direct' - meaning immediate and not merely consequential [FN13]. Thus, where damage is the 'gist' of the action in case, it was not so for trespass [FN14].

Although the paucity of English cases on trespass to goods has not compelled the resolution of the damage requirement under English law, in the US, the issue has not only raised some difficult questions, it can and \*94 has also served as a form of limitation on the type and number of cases that can be brought within the cyber-trespass doctrine. Absent such a requirement in English law, it could be that a potentially significant limiting factor would be lacking should the English law on trespass in cyber-space develop along similar lines as the US. Further, if trespass to goods is considered actionable *per se* under English law, the lack of a limiting factor (such as a damage requirement) could militate against the development of a broad doctrine of cyber-trespass outside of the US. In either case, the issue whether trespass to chattels requires damage (and proof thereof) in order to be actionable would, if it continues unresolved under English law but cases alleging cyber-trespass begin to make their way through the English and other common law courts, cause greater practical difficulty than it has hitherto. As a strictly common law development, the existence and scope of the tort of trespass to goods, as applicable to cyberspace, will fall to be determined in the courts. Given the recognition of such a claim by the US courts, the deliberations of an English (or other common law) court faced with such a claim should be closely watched by both US and non-US lawyers.

Another noteworthy point for purposes of the current discussion is that under English law, various acts in relation to goods have now been 'folded' into the concept of 'wrongful interference' under the Torts (Interference with Goods) Act 1977. Although the Act does not change the substantive English law on the various torts relating to interference with goods and interests therein [FN15], and thus prior case law on conversion, trespass and other such actions continue to be relevant, it does attempt to rationalize the various remedies available in such causes of action [FN16]. Section 3 of the Act provides for remedies that consist either of delivery of the goods (or payment with reference to the value thereof) and consequential damages, or for damages. This confirms the prevailing notion, up to recently at least, that trespass to and other interferences with goods (chattels) concerned physical (tangible) goods and actual physical movement, dispossession or other similar activities relating thereto. The idea that such interference could occur in cyberspace - through the sending of electronic signals to computers - was probably so remote as to be nonexistent at the time (1977.) In just twenty years, however, a US court would be faced with precisely that issue, and have to consider whether or not such an act could amount to trespass to chattels under US common \*95 law principles [FN17]. It will therefore be interesting to observe how an English court will deal with the issue whether or not electronic interferences can be considered sufficiently tangible (physical) so as to qualify as a trespass to a chattel (e.g., a computer.)

## 2.2 *Trespass to Chattels in the US: the Road to Cyber-trespass*

Under § 217 of the Restatement (Second) of Torts [FN18], a trespass to chattels is committed where a person intentionally dispossesses another person of the chattel, or uses or intermeddles [FN19] with a chattel in the other's possession. Liability arises, however, only if (a) the other person has in fact been dispossessed of the chattel, or (b) the intermeddling caused harm to the other's 'materially valuable interest' in the physical condition, value or quality of the chattel, or (c) the possessor is deprived of the use of the chattel for a substantial time, or (d) bodily harm is caused to the possessor, or to some person or thing in which the possessor has a legally protected interest [FN20]. In other words, an interference with a chattel that does not cause harm may technically be a form of trespass, but does not give rise to a legally recoverable claim even if the act was done intentionally. In

this sense, trespass to chattels under US law has evolved so as to be distinct from conversion (which historically required that intangible interests be reflected in something tangible), as well as from a trespass to land (which is actionable *per se*) [FN21]. As such, the tort deals, first, with interferences that are 'not sufficiently important to be classed as conversion [which would] compel the defendant to pay the full value of the thing with which he has interfered. Trespass to chattels survives today, in other words, largely as a little brother of conversion.' [FN22] Secondly, a harmless trespass to chattel under the US law does not give rise to a claim for nominal damages. Instead, according to the Restatement, '[s]ufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference.' [FN23] These statements of principle seem to entrench and reinforce the conceptual distinction (and differing requirements of liability) among conversion, trespass to land and trespass to chattel.

**\*96** The first major US case to apply the traditional doctrine of trespass to chattels to cyberspace activity was the 1997 decision by the Southern District Court of Ohio in *CompuServe, Inc. v Cyber-Promotions, Inc.* [FN24] The court relied on the earlier (1996) California Court of Appeals case of *Thrifty-Tel v Bezenek* [FN25], where the Court held that unauthorized use of long-distance telephone services could constitute a trespass to chattels; the electronic signals that were generated by a practice that came to be known as 'phreaking' [FN26] were thought 'sufficiently tangible to support a trespass cause of action'. The *CompuServe* case saw an Internet service provider (CompuServe) argue successfully that a trespass to chattels action lay against a defendant who had transmitted 'spam' [FN27] to users of CompuServe's network and services. The electronic signals thus transmitted constituted the 'intermeddling' (to CompuServe's computer system) required by the law, and though no actual dispossession had occurred, it was not necessary as long as there was an impairment to the value of the chattel in question [FN28]. In addition, the loss of customer goodwill was a form of damage in that it constituted a thing in which CompuServe had a 'legally protected interest.'

There have been many commentaries on the *CompuServe* case, and the subsequent US cases that essentially adopted its reasoning (including *eBay, Inc. v Bidder's Edge, Inc.* [FN29], *Register.com, Inc., v Verio, Inc.* [FN30], and *Intel Corp. v Hamidi* [FN31]), [FN32] and it is not proposed to rehash them here, although some of the more significant implications of these decisions for the **\*97** purpose of the present discussion will be noted. Essentially, most commentators agree that this line of decisions - culminating in the *Intel* case (discussed below) - heralded not just an unexpected judicial recognition of the utility to the Internet age of an old form of action, it also demonstrated the flexibility and breadth of the trespass to chattels claim [FN33]. Certainly, by applying *Thrifty-Tel* and allowing recovery where there was no physical damage to the chattel in question, the *CompuServe* decision opened the door to wider claims for cyber-trespass than was probably and previously thought possible under traditional trespass rules. This development has taken place in parallel with the ability of website, database and other information possessors to limit access through contracts and other legal mechanisms, such that there seems to be a growing number and scope of legal tools for access control in cyberspace.

It must, however, be stated that there are several policy reasons in favor of allowing recovery under a trespass to chattels claim by the plaintiffs in most of the cases decided in the US so far. These reasons revolve largely around two factors: (a) the commercial risks and realities of Internet-related businesses, and (b) the lack of an adequate legal remedy for unfair competition in this realm. For example, in *eBay v Bidder's Edge*, it may be argued that a website provider such as eBay ought to have legal recourse to exclude unwanted activity from its website, at least where such activity can in some objective way be viewed as socially inappropriate. In eBay's case, a palpable sense of 'free riding' and hence unfair competition will almost inevitably arise if Bidder's Edge (or similar aggregators or competitors) were permitted to continue spidering, scraping and otherwise gathering information that would lead to a decrease in the utility of eBay's site and services (since the information on cur-

rent bid prices, available items and so on would now be available on non-eBay sites) and the overall value of the user experience (since the excitement and anticipation of checking on current information would not depend solely, or even primarily, on accessing eBay.) As a matter of fact, it can be said that the user experience on websites such as eBay's is almost inextricably tied to the 'real time' anxiety and challenge of bidding, outbidding, timing and strategy. As such, where information crucial to this experience is readily available on more than one unrelated website, it can be argued that the user experience is in some way thus diluted. This would be aside from, though related to, any direct (including, in some potential competitive situations, financial) and legitimately detrimental effects on \*98 eBay's services or business (such as network slowdown or capacity issues, whether actual or potential, as acknowledged in the *eBay* case itself.)

In addition, where the plaintiff may have first attempted to rely on 'self-help' mechanisms (such as technological blocks and tracing of the alleged trespassory acts, as in *CompuServe* and *eBay*, or the attempts by Intel's employees to block Hamidi's email messages in *Intel*), the plaintiff can be said to have turned to litigation only because such 'self-help' failed [FN34]. Similarly, the plaintiff may be said to have used good faith attempts to craft a solution without resorting to the absolutism of asserting her property rights, such as where a negotiated contractual solution to the alleged trespassory activity was attempted (as in *eBay*.) In such instances, it may be difficult to accuse the plaintiffs of attempting to overly monopolize or aggressively control their respective 'corners' of cyberspace. Further, where the plaintiff has a legitimate online business model (whether that be providing Internet communications services (*CompuServe*), an online auction community (*eBay*), or domain name services (*Register.com*), it may be justifiable to rely on whatever legal doctrines are available and applicable, as control mechanisms over access to its website and information in ways not necessarily hostile to the growth or usage of the Internet, in that these control mechanisms represent only a choice by such entities to exclude certain actors and acts, but do not dictate the choices open to other entities, who may elect not to assert their property rights in the same way [FN35].

On the other hand, it can also be argued that it would be unfair to deprive other legitimate online businesses of opportunities to compete freely, where this is the price of allowing others to assert their property rights in cyberspace [FN36]. For example, Bidder's Edge was arguably not the archetypal 'free rider', first because it did attempt to negotiate a license with eBay, and secondly because its form of business (providing convenient consumer services and information through collecting, aggregating and organizing a huge mass of consumer-relevant online data) can be said to be just as legitimate and useful to the growth and usage of the Internet as eBay's. From this perspective, it may be difficult to distinguish between a company like Bidder's Edge and other online service providers such as search engines, or even online activities such as linking [FN37]. This \*99 argument would, however, favor a different outcome only in the *eBay* case, probably not *CompuServe*, and possibly not *Register.com*. In *CompuServe*, the defendant was engaged in 'spamming', arguably a socially undesirable and doubtless a 'free riding' activity. In *Register.com*, although Verio's main business was undoubtedly legitimate [FN38], its access and use of the WHOIS database could arguably be said to be somewhat opportunistic and perhaps even marginally deceptive to the recipients of their emails (such emails could themselves constitute a mild form of 'spam'.)

Further, it can be argued that allowing parties such as *CompuServe* and *eBay* (however desirable corporate 'netizens' they may be) to succeed on a trespass claim represents a setback for proponents of open access to information on the Internet and dampens legitimate (and desired) competition in terms of electronic commerce, including increasing transaction costs [FN39]. In other words, extending trespass to chattels in the way that the US courts have done results in 'over-propertization' of the Internet, which is largely a public communications resource, the growth and success of which lies substantially in its open nature and the 'network effects' thus cre-

ated [FN40]. Thus one important question is whether encouraging (and protecting) Internet-based business activities through propertization is worth the 'cost' and risk of such property (chattels) owners 'fencing off' their own 'corners' of cyberspace, based as it is on a cause of action that historically was developed to protect physical property. This concern is exacerbated by the fear that such 'fencing off' will perpetuate a fragmentary, even 'anti-commons', approach to the Internet. This question raises implications beyond the law of trespass, particularly as regards the fact that the relatively easy extension of trespass notions to cyberspace can be traced, in part, to the fairly lax use by the US courts of the term 'trespass' and the different types of property associated with it. This judicial casualness has fanned academic discussion of the possibility that cyber-trespass developed in the way it did in part because of a perception of 'cyberspace-as-place' [FN41]. The full implications of such a view are beyond \*100 the scope of this paper, but it must be noted as a relevant consideration in any instance where a court (or for that matter a legislature) is called upon to determine the applicability and extent of private property rights in cyberspace. In such a case, the need to balance such private rights with the public interest in open access must surely be a relevant policy factor. Whether couched in terms of real or personal property rights, one risk of a pro-'propertization' stance is that the balance is tipped in favor of those who control the means to communicate and the content available in cyberspace. While this may be an overly-simplistic statement of the problem and its implications, it is not difficult to hypothesize that a person who is inclined to view cyberspace as a distinct 'place' (and by association, acts and things within that space) may also find it easier to use real property analogies and metaphors in any argument or decision emanating from a cyberspace problem. Such a tendency would not, by itself, dictate the legal outcome of a case, just as it would not necessarily cloud that person's analytical framework or reasoning; it is only when it leads to 'tunnel vision' that the 'cyberspace-as-place' perception can be 'outcome-determinative' without taking into account other perspectives and possibilities [FN42].

Another relevant policy factor in some of the cyber-trespass cases is that the trespassory acts (such as in *eBay* and *Register.com*) were directed against publicly-available information and databases. This fact may make a difference from the perspective of determining whether or not it is permissible for 'owners' to 'fence off' cyberspace; it also raises the question, discussed further below, as to the actual 'property' that was trespassed against and consequently harmed, and whether the trespass claim can succeed in protecting these interests where other property rights fail to do so. Finally, there is at least one US case that considered the 'taking of factual information from a public source ... not a trespass' [FN43], though unfortunately the court's analysis of the trespass doctrine was fairly sparse, and the argument failed ultimately because the plaintiff failed to prove the requisite harm to the chattel in question (a website from which the defendant extracted factual information about forthcoming events through the use of spiders.)

Without revisiting the 'cyberspace-as-place' metaphor, the notion that trespass to chattels could apply - without much need for adaptation - to \*101 cyberspace, based entirely on the fact that a chattel belonging to the plaintiff was involved at some point during the defendant's activities, is at first blush somewhat discomfiting. It is true that the defendant's act of trespass cannot take place in the absence of the chattel; however, even though the presence of the chattel may be a necessary pre-condition to the doing of the act complained of, this fact gives rise to two problems: first, the chattel (and damage thereto) seems only incidental to the intention behind the act (i.e., the act was not necessarily directed at or against the chattel, which was merely the means to achieve a particular purpose.) Secondly, the real damage that is caused by the act generally is not to the chattel or any possessory interest of the plaintiff's therein, inasmuch as it lies in the defendant being able to, e.g., compete effectively with the plaintiff, or acquire commercially valuable data or information, thus injuring some (usually) commercial interest of the plaintiff's.

The question of intention may not, however, be a major problem within the scope of the action of trespass to

chattels. Under the US law of trespass to chattels, the requisite 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. 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.' [FN44] It can be argued that a 'spammer' or other 'intruder' onto a website or into a computer network does that act at least with 'knowledge that ... intermeddling will, to a substantial certainty, result' therefrom. Despite academic doubt about the presence of the requisite intention in the US cyber-trespass cases [FN45], it is arguable that the Restatement comments are wide enough to accommodate situations where the defendant may not have intended (whether solely or even primarily) to 'intermeddle' with the plaintiff's chattel, so long as she committed the trespassory act with the knowledge that some interference with the chattel in question will take place, and such interference is deemed by the law to be sufficient to constitute a trespass. Under English law, there has not been exhaustive judicial or academic discussion over the definition of 'intention' in the realm of torts, in recent times probably because of the rapid growth of the law of negligence, overlaid on top of the fact that historically it was the forms of action that dictated the nature of a claim. It has been suggested, however, that recklessness as to the effect of one's \*102 actions, being sufficient for a trespass to land, should apply to all the forms of trespass [FN46], although whether this will constitute yet another divergence from the US law in this area could be an issue, since the US law requires 'substantial certainty' that intermeddling will result from the act [FN47], which seems to set a higher standard. Regardless, however, of these issues and differences, the general point remains that it seems odd to include the kind of activity that more resembles some kind of unfair competition (whether or not actionable under this heading) in a tort that emphasizes possession and ownership of a physical thing.

On the issue of damage, although the chattel at issue in the cases under discussion could have been damaged in some way (whether as to its physical condition, quality or value), any such damage was not in any way done to the chattel as a thing, in and of itself. This was a point made by the California Supreme Court in *Intel v Hamidi*, and as such will be discussed further below [FN48]. For now, it will suffice to note that the tort of trespass to chattels revolves around an act done to the chattel itself, or more generally, the possessory interest in the chattel, such that the damage requirement (to the extent it exists in a particular jurisdiction) ought logically to be found in damage to the chattel or possession thereof. To loosen these 'connectors' would risk confusing the acts done, and/or damage caused, to the chattel (the subject of the tort) with acts done, and/or damage caused, to other 'things' - in the cases under discussion, largely intangibles - associated with the chattel (for example, intangible information in the form of computerized data is embodied in the form of code and programs residing on a computer.)

In this regard, a distinction can be made between 'cyberspace-as-place' [FN49] and 'information-as-thing', which the courts for the most part seem not to have done clearly. The fact is that the interferences in the cases in question were ultimately directed toward intangibles, i.e., the data or information (auction listings, database entries, email addresses) residing within or on a tangible computer server. In other words, it might be more theoretically plausible - if not necessarily easier - to view the databases and information being spidered, crawled and gathered, as the requisite chattel, rather than hinge the tort on the 'real' (i.e., tangible) chattel, viz., the computers they were stored on. This analysis would set the 'spam' cases apart from the automated search cases, but there seems little policy reason for not doing so, particularly given the increasing \*103 occurrence and costs incurred by 'spam'. The result in these two categories of cases might not be dissimilar, in any case, and even by a different reasoning process (though ultimately still within the same tort) as the 'spam' cases would fit more easily (especially as regards the damage caused and the link between the interference complained of and the damage) within the doctrinal rubric of trespass to chattels.

It seems, however, as if the US courts in the cases to date have preferred the alternative route of borrowing from cases and principles governing real property trespasses, rather than identifying and declaring that personal property principles apply to 'information-as-thing.' The fact that it seems natural and human to consider 'cyberspace-as-place' could explain the courts' effortless borrowings of real property principles in this way [FN50] such that there is little conceptual difficulty with allowing recovery under trespass to chattels when the interference was non-physical in nature (at least, not to a significantly substantial extent) [FN51], and where the damage to the chattel was either incidental, or unrelated to its principal physical characteristics or functions (a point emphasized by the Court in *Intel.*) Regardless, therefore, of whether the courts have been so deeply mired in the metaphor of 'cyberspace-as-place' so as to conflate real and personal property in cyberspace [FN52], the dominance of a 'property' motif in the cyber-trespass cases shows in the relative alacrity with which courts have granted injunctions restraining further trespassory activity against the plaintiff's 'property', where the 'property' motif at play centered on tangible property in the form of computers and associated equipment. Where the requisite damage has been found in injury to a broadly generalized 'value' [FN53] of the chattel rather than in an impairment to its physical condition or quality, it would seem as though the interests that the courts are protecting are somewhat distant from the relatively narrow basis of the tort, which essentially concerns intentional dis-possession or interference \*104 with a physical thing such that the owner's possession or use of the thing is impaired in a way sufficiently significant as to warrant legal protection.

A related point is the fact that, in the cyber-trespass cases, the intangibles toward which the interferences were directed tended to be data, databases, information and listings that, while commercially valuable, are un-protected (and in many cases unprotectable) under intellectual property and related laws. Unlike the United Kingdom (UK) and the rest of the European Union (EU), the US has no generic database protection law. Under general copyright principles, data and factual information cannot be protected by copyright law. Where such information is commercially valuable, legal rights are conferred only by means of trade secret and related laws (such as any protection provided by the action in breach of confidence in the UK.) Although it was not necessarily the case that any of the plaintiffs in the cyber-trespass cases were relying on trespass as a last resort, it must be said that the effect of extending trespass to these cases could - even inadvertently - amount to granting legal protection over intangibles that would otherwise not be protected. It is true that the legal protections so conferred exist only insofar as the intangible resides on a tangible thing that is interfered with, and as such are conceptually and in scope different from obtaining actual rights in the intangible itself. The net practical effect, however, is fairly similar, in that the owner (or at least person in control) of the intangible is able to control the means, extent and duration of access to, and use of, that intangible, and by whom. In light of the existence of database protection in the UK, it could be that courts there and in other countries with similar protection would resist the extension of a trespass to chattels claim.

One fundamental question that can be asked in this regard is whether or not trespass to chattel is, in fact, the correct legal principle to base recovery on, in respect of unauthorized access and intrusive activity to intangibles on the Internet. Various commentators have proposed other legal rules that, for various reasons, might be more appropriate, such as trespass to property (land) [FN54], or even the doctrine of nuisance [FN55]. In the comparative US/UK context, one commentator [FN56] has suggested that the US cyber-trespass cases could more properly have been framed as an \*105 action on the case (following the old forms of action discussed above), which permitted recovery for consequential damage caused by trespassory acts that did not 'rise' to the level of an actionable trespass. What this diversity of academic opinion shows is the clear need for the law to deal with an increasing amount and different kinds of intrusive activity in cyberspace, *viz.*, whether for general policy, doctrinal and economic reasons, a claim and recovery ought to be allowed, and if so, what branch or principle of law

would be the most appropriate medium for recovery. The trespass to chattel claim as developed by the US courts has so far seemed more of a 'gap-filler' than a logical and complete solution [FN57].

Another relevant factor to consider in extending trespass to chattels to cyberspace is the ability of an owner/possessor/controller of information to augment or restrict another's access to and use of that information by the mechanism of contract. A contract can represent a set of mutually-agreed rights of and limits to access and use of information, and several of the cyber-trespass cases illustrate this. For instance, eBay and Bidder's Edge had actually entered into negotiations for a license, while Register.com had sought to impose restrictions on the use of its customer database. This issue raises considerations that reach into the realm of general contract law as applied to different types of electronic and online contracts [FN58]; in the present context, the point to note is that, assuming \*106 there are no difficulties with the substantive requirements of contract law (such as offer, acceptance, notice and certainty), the owner of the sort of chattels at issue in the cyber-trespass cases (and the information and other property residing in and on them) may allow, extend, limit or prohibit access to such information, chattels and property by way of contract [FN59]. This point is further discussed below, in the context of the meaning and scope of 'unauthorized access.'

The line of US cases beginning with *CompuServe* can thus be said to have effectively created a new (or at least broader and certainly updated) cause of action for cyber-trespass, which not only liberalizes the traditional requirements for a trespass to chattels claim, but also positions it as a form of property right that is (1) aside and different from any known species of intellectual property; (2) separate from and in addition to contract (which can impose restrictions on access by mutual agreement); and (3) without the conventional limitations developed by these areas of law [FN60]. Given that, in the appropriate case, intellectual property [FN61] rights might be available to protect an intangible that is of some value to the owner, and that in many cases, owners of information, databases and other intangibles can and do draw 'fences' around access to their 'property' by way of contract, the growth of cyber-trespass as an alternative or additional legal means to protect intangibles is significant. Taken together, these and other mechanisms [FN62] that can be used to control access to information and content can collectively give to the owner/possessor/controller of intangibles a series of different but effective legal rights by which to control access to these intangibles.

Before moving on to examine briefly the California Supreme Court's decision in *Intel v Hamidi*, one final point may be made on issues raised so far by the present discussion. As alluded to previously, a deeper consideration for the policy and competition concerns underlying the cyber-trespass cases may in some instances point toward a different treatment of and outcome for 'spam' cases such as *CompuServe*. 'Spammers' can be distinguished from legitimate competitors, in that their methods and aims tend to demonstrate socially undesirable, 'free riding' and (sometimes) distasteful behavior. In addition, it is not difficult to imagine that 'spam' and 'spamming', if unchecked, could lead to the kinds of server and network overloads and slowdowns feared by the *eBay* court in respect of spiders. Similarly, in non-'spamming' cases where the defendant's actions may be considered illegitimate in some way and can or will cause obvious harm to \*107 a plaintiff's commercial or other legitimate interest, a trespass to chattels claim may well be a useful, perhaps even the only, legal means available to restrain further activity (e.g., through the award of an injunction.) [FN63] In many jurisdictions, some such practices have begun to be regulated by anti-'spamming' legislation [FN64]. As such, the need for a common law solution to 'spamming' may well be much less pressing. Ironically, then, it would still be the cases which do not concern 'spam' (including mass emailing cases that do not amount to 'spam', such as *Intel v Hamidi*), that remain in need of a legal remedy. The California Supreme Court's judgment in *Intel* should be considered in the context of this existing need.

### 2.3 *The State of Play After 2003 and the Aftermath of Intel v Hamidi*

In June 2003, the California Supreme Court issued its decision on the appeal in the *Intel* case. While accepting the applicability of trespass to chattels to cyberspace, in that the Court did not question either the doctrine or the prior case law, the majority's decision had the effect of reining in some of the potentially broader implications of the action, primarily as regards the kinds of damage that would be actionable thereunder. As such, the Court's decision is significant also for providing a potential glimpse into how future cases of cyber-trespass could be treated by the US courts.

The Court emphasized the need to show damage in order to succeed in such an action, and distinguished the case before it from *CompuServe*, *eBay* and other precedent cases on that basis. In this respect, the Court contrasted the scant evidence of damage presented by Intel [FN65] with the damage shown in the prior cases. Because the emails sent by Hamidi did not rise to the volume of 'spam' (as was the case in *CompuServe*), and because Intel could not show that its computer systems had in any way been, or could potentially be, burdened or impaired in their 'intended function' by Hamidi's actions (as in *eBay*, however minimally or potentially), the Court concluded that Intel's real complaint was about the contents of Hamidi's email communications, and not the effect of his sending them on its personal property.

**\*108** The emphasis which the Court placed on the damage requirement shows (as mentioned previously) a potentially large divergence between the US and English common law of trespass to chattels. Interestingly, the Court highlighted the fact that the origin of the tort differed in the US from England, based as it was in the latter on the historical procedures of the forms of action, and distinguished it also from trespass to land. The majority of the *Intel* Court therefore seemed to be aware that US law on this point differs in a significant respect from the English; it also showed no sign of confusing cyber-trespass with acts of interference with real property. On the contrary, the Court expressly rejected the possibility of applying real property concepts of inviolability to what is clearly personal property, seeing no policy reason to adopt a 'rash' and 'rigid' rule of this nature in such cases [FN66]. The majority also warned against over-extending the scope of the tort to protect interests beyond that which it was originally designed to protect, *viz.*, possession of a chattel, particularly if the extension was by way of stretching the damage requirement such that almost any unwanted act of intrusion (such as an unsolicited telephone call) could constitute an actionable trespass.

Although the *Intel* Court's ruling on the general requirements of a trespass to chattel claim in cyberspace will doubtless have a large impact on future cases, the specific circumstances of the case justify a comparison of its result with that of the other, prior, cases. As mentioned in the earlier analysis of the pre-*Intel* cases, the trespass to chattels claim seems to have been pressed into service in order to restrain activity which the courts considered sufficiently illegitimate to require legal intervention, but which other existing causes of action (e.g., under intellectual property or contract laws) could not cover. Even though these cases concerned mainly commercial interests that could only, at a stretch, be related directly to the chattel in question and the plaintiff's possessory interest thereto, it is difficult to disagree with the courts' conclusions on the facts of cases such as *CompuServe*, *eBay* and *Register.com*. In *Intel*, however, an additional factor that could have underlay the Court's analysis was the issue of free speech. Even though the First Amendment issues raised by Hamidi were not, ultimately, the main basis for the majority's decision and thus constituted *dicta* in the case, the majority decision displays a concern for free speech considerations. This factor, going toward Hamidi's intent and motives, and Intel's inability to show that Hamidi's actions damaged the kind of interests which previous courts have considered legitimate to protect, places the *Intel* case in a category somewhat apart from those other cases [FN67].

Nonetheless, the remarks made by the Court in *Intel* emphasizing the basis for and the nature of the trespass to chattels action (*viz.*, as a species \*109 of personal and not real property), and the consequence that the requisite damage should be linked causally as well as conceptually as such, are welcome reminders to future courts that, even if trespass remains the doctrine of choice to restrain certain kinds of unwanted activity, its precepts ought not to be conflated with other forms of property, nor should damage be founded on doctrinally suspect grounds. Courts tasked with deciding future cyber-trespass cases should thus bear in mind this 'anchoring ... [of] a doctrine that had drifted loose of its traditional moorings.' [FN68]

Where non-US case law development is concerned, the *Intel* Court's comments ought thus to be just as welcome and useful. In particular, if non-US courts are to apply the English law conception of trespass to chattels doctrine to cyberspace, the fact that the claim would be actionable *per se* means that the potentially-limiting factor of damage would be absent. In such a case, the need to bear in mind the fundamental basis of a trespass to chattels claim would be even more acute.

#### 2.4 How Significant would the Differences between the US and English Law on Trespass to Chattels Be?

As highlighted above, where the US law requires either some form of damage, whether actual or threatened, to the 'physical condition, quality or value' of the chattel, or to the relevant possessory interest in it, the traditional English view seems to be that trespass to chattels would be actionable even in the absence of damage. Thus a lawsuit for nominal damages would be recognized under English law, where in the US the possessor of a chattel that had not suffered any damage would have no legal remedy other than the right to use 'reasonable force' to protect the inviolability of the chattel. For the most part, this distinction is likely to be more theoretical than practical, as it is highly unlikely that anyone would sue, even under the English doctrine, unless they had suffered some damage worth the expense, trouble and process of a lawsuit. In the US cyber-trespass cases, the plaintiffs all either suffered, or were concerned they would suffer, sufficiently significant financial, business or other losses if the defendants' activity continued unchecked. Thus, even though the US courts may have adopted a fairly liberal - possibly even doctrinally awkward - interpretation of what is sufficient to constitute the necessary damage, the outcome of each of the cases discussed above has been to protect the plaintiff's interests (largely commercial) which the courts considered legitimate as against the defendants' intentional intrusive conduct. In the two cases where the plaintiffs failed to win a remedy (*Ticketmaster* and *Intel*), the court in question was either not sufficiently convinced of the actual or potential damage suffered \*110 by the plaintiff, particularly where the defendant's acts were not considered to constitute illegitimate competition (*Ticketmaster*), or was unwilling to extend the trespass doctrine to non-commercial cases with a free speech element (*Intel*.) The real theoretical concern, therefore, is whether or not trespass to chattels is the appropriate doctrine to apply to those cases where the courts consider the plaintiff's interests worth protecting.

Any conflation by the US courts of real and personal property concepts in this context is thus unfortunate, not least for obscuring the real problem. The costs and implications of using trespass to chattels to protect the plaintiff's commercial or other interests include the risk of reducing open access and affording an alternative avenue of protection to 'property' that would not otherwise be protected by other means; in both of these situations, the fact that the plaintiff's 'property' is connected to the Internet and consists of publicly-available information presents a difficult interest-balancing issue. On the other hand, the US cases have shown that 'self-help' measures that might conceptually fall within the 'reasonable force' allowance usually are not sufficient to protect the plaintiff and her property against further intrusion by the defendant.

Such questions and conflicting interests will be the same in the UK and elsewhere, as has been the case in the US. The courts that may be faced with such difficulties may thus find themselves wrestling less with the problem of whether damage is necessary (or if so, proven) - a conceptual issue - than with the more commercially important problems of balancing different private and public interests. This does not, of course, render the conceptual issue unimportant (except, perhaps, from the business and practical perspectives of the parties to the suit and other, similarly-sited persons.) Where US and non-US courts continue (or begin) to confront these theoretical issues, one added concern should perhaps be the potential overlap between an expanding doctrine of cyber-trespass and the concept of 'unauthorized access.'

### **3 Equating Cyber-Trespass in the Common Law with 'Unauthorized Access' in Computer Misuse Legislation**

In the US, several fairly recent cases seemed to indicate that a mere act of unwanted 'intrusion' into another's computer systems, where the act was done without the consent of the other person, could fall not only within the scope of the doctrine of trespass to chattels, but also run foul of statutory restrictions on computer access, such as those found in the federal Computer Fraud and Abuse Act [FN69] (CFAA.) In both types of situations, the \*111 courts had to determine what (if any) the extent of the permission given by the plaintiff to the defendant had been, as that fact was directly relevant to the issue whether or not there had been a trespass or an unauthorized access to the plaintiff's computers, network or systems. In other words, what was the limit of, and what in fact constituted, the plaintiff's 'consent' (or lack thereof) to the defendant's activity. These questions are important for at least three reasons: (1) it raises the possibility that chattel owners could have more than one legal remedy to guard against unwanted activity on their websites, databases, networks and equipment; (2) intrusions can be made unwelcome by unilaterally-imposed contractual restrictions on consent; and (3) similar questions, legal issues and principles can arise in non-US jurisdictions that have computer misuse legislation. [FN70] Given the breadth of a civil claim in cyber-trespass (as discussed above) and the discovery that unauthorized access seems to be a very broad and undefined concept in computer misuse legislation (discussed below), these questions take on an even larger significance.

#### *3.1 When does an 'Unwanted Intrusion' become Actionable as an Act of Cyber-trespass, or of Unauthorized Access, for Lack of Consent?*

As described previously, it is possible under general contract formation rules to limit a person's access to and use of a website, database, software and other intangible (if valuable) information, through contract (including electronic forms such as 'clickwrap' contracts and possibly 'browsewraps'.) [FN71] Whether or not a person (or for that matter, technology such \*112 as a robot, crawler, spider or other automated search and data-gathering device) is permitted to view, download, edit or otherwise do anything in relation to a webpage, data, computer program or other information thus depends in large part on whether there is a contract (express or implied) with the website/database operator/owner, and the extent of the relevant permission granted thereunder. It would seem that the US courts are fairly liberal in determining when a plaintiff owner/operator is considered to have denied or withdrawn the relevant permission, at least in relation to the question whether or not the user's access was authorized.

In *EF Cultural Travel BV v Zefer Corporation & Explorica, Inc.* [FN72], the issue was whether the defendant's use of a 'scraper' to obtain information off a website 'exceeded [his] authorized access' to the website under the Computer Fraud and Abuse Act (18 U.S.C. §1030(a)(4).) The US Court of Appeals for the First Circuit

confirmed that a lack of authorization could be shown if the website explicitly barred access (subject to any public policy limitations.) A lack of authorization could also be implicit rather than explicit (e.g., through the requirement of passwords, which would constitute an implicit restriction through technological means.) However, the Court considered that it would not be 'prudentially sound' or within the statutory mechanism to base a finding of lack of authorization on a 'reasonable expectations' test, which the Court considered 'highly imprecise' and 'litigation-spawning'. The Court hastened to add that the 'reasonable expectations' test was not being rejected based on a presumption of open access; rather, the shortcomings of such a test contrasted baldly with the ease with which website providers could spell out clearly the restrictions they wish to place on access.

Prior to *EF Cultural Travel v Zefer*, US courts had already upheld explicit prohibitions unilaterally imposed on users by website providers as sufficient to justify a finding of lack of authorization; specifically, through express restrictions stated on the website provider's Terms of Service (TOS.) This was the case in *America Online, Inc. v LCGM* [FN73], where the Eastern District of Virginia, in a brief opinion, considered that the defendant's 'spamming' of other AOL subscribers violated AOL's TOS and 'as such' were unauthorized. The court also found that the elements of a state trespass to chattels claim (following cases such as *CompuServe*) were made out. Similarly, in *America Online, Inc. v National Health Care Discount* [FN74] (NHCD), the Northern District of Iowa held that violation of AOL's TOS by 'spamming' 'exceeded authorized access' under the CFAA. Interestingly, while the NHCD court noted that the evidence might not have been sufficient to prove whether or not access had been 'without \*113 authorization' (presumably given that the messages were sent as emails through the AOL network), the court in *LCGM* did not seem to distinguish between an act of access 'without authorization' and an act 'exceeding authorized access', nor did it appear to consider the need to do so, holding only that the relevant CFAA requirements were met by the defendant's unauthorized acts. Perhaps unfortunately, the NHCD court did not comment further on the distinction between acting 'without authorization' and an act 'exceeding authorized access', as the evidence allowed it to rule that the latter had been shown. The implications of the *LCGM* court's interchangeable use of similar terms relating to unauthorized access is discussed further, below.

Where the relevant restriction (e.g., an express bar on screen scraping or spidering) is contained in the TOS, its validity would fall to be determined by contract law. Most TOS tend to be in the form of a 'browsewrap' contract, where the user is not required to click on a button or other icon to indicate assent to the terms (as would be the case in a 'clickwrap'); rather, the TOS can be found only if the user follows (by clicking on) a hyperlink, which is generally in smallish font and commonly placed at the bottom of the website homepage, displayed alongside similarly-sized hyperlinks to other webpages relating to the website provider's user policies. Many TOS also contain a provision which states that by using the website or its services, the user is thereby assenting to the terms governing her user thereof. The obvious question is thus whether or not the user can be said to have assented to the actual terms, such that a legally binding contract can be said to have been formed between her and the website provider [FN75]. Where a plaintiff claims that restrictions on access or use were contained in its website TOS, therefore, in determining whether the defendant user had the requisite permission to do whatever she was seeking to do on the website, the court would first have to undertake a contract law enquiry [FN76].

Where the relevant restriction is not found in a website TOS, the situation can be far more difficult, given that it would not even be clear in such cases whether or not the restriction would have any legal effect at all, and thus serve to bind the defendant user (or not.) In such cases, however, it is possible that the plaintiff might be in an even stronger position vis-à-vis the defendant on this point, as it may be possible to argue that, far from being a contractual question, it is a simple matter of fact, viz., by placing the restriction on its website, the plaintiff is expressly withholding her consent to the act complained of. Since the question is outside \*114 the realm of con-

tract, it is also irrelevant whether or not the defendant saw or could reasonably have seen (and thus be taken to have assented to) the restriction; what matters is that the plaintiff has explicitly indicated her lack of consent. As such, by flouting the restriction, the defendant is either trespassing or otherwise acting without authorization. In either case, one of the elements of either cause of action (i.e., trespass or unauthorized access) may quite easily be made out.

A look at several of the cyber-trespass cases would seem to bear out this possibility. In *CompuServe*, *eBay*, *Register.com* and *Intel*, all the plaintiffs had, in one way or another, effectively notified the defendants of the plaintiffs' objections to the defendants' acts, viz., through technological filtering or blocking attempts (*CompuServe* and *eBay*), or actual (*Intel*) or constructive (*Register.com*) notice. At the latest, either a cease-and-desist letter or (perhaps a rather extreme view though this was the court's view in *Register.com*) actually bringing a lawsuit could serve as proof of lack of consent on the plaintiff's part. This is troubling in the context of cyber-trespass because of the liberal approach the US courts have taken toward the concept of intermeddling or interference; in computer misuse cases based on unauthorized access, the same concern arises because of a lack of clarity and rigidity in the definition of the term, which could thus be read to encompass the kinds of acts constituting lack of consent in the cyber-trespass cases.

If the fact that courts are willing to allow such a broad interpretation of what authorization, permission or consent means is viewed in the context of the development of a broad doctrine of cyber-trespass, then the fact that neither courts nor legislatures have clearly defined the meaning of 'unauthorized access' for purposes of computer misuse must be cause for further concern. It is telling that none of the cyber-trespass cases has delved deeply into the overlap between a trespassory act in cyberspace and an act of 'unauthorized access', and that *EF Cultural Travel v Explorica* was decided as a case of exceeding authorized access within the scope of the CFAA, rather than trespass. Given the acts complained of by the plaintiffs in the CFAA cases and the trespass cases, there is a substantial overlap in the various activities in both 'categories', whether that be screen scraping (as in *Explorica*), spidering (as in *eBay* and *Register.com v Verio*) and bulk emailing (as in *Hamidi*.) In all of these cases (including *Explorica*), the defendant(s) used some form of software tool, and/or the Internet, to access the plaintiff's Internet-related network or systems (e.g., a website, a server, or a database), without the plaintiff's permission. With the liberal approach toward consent and trespass, it is therefore possible that a website owner, database operator or other possessor of a chattel connected in cyberspace could also investigate the further option of proceeding under computer misuse legislation. The defendant's behavior in many of these instances has been variously determined to possibly constitute either a trespass to chattels or an act of unauthorized access. \*115 The *AOL v LCGM* case, in fact, is an illustration of this. This means that an action can conceivably be brought under either 'unauthorized access' principles within the relevant computer misuse statute, or cyber-trespass, whether within or outside of the US, if a similar trend is observed in judicial interpretation of both sets of legal principles. The next section will examine the notion of 'unauthorized access' under other major non-US legislation, as a gauge of how likely this overlapping scenario will be.

### 3.2 US Law on Unauthorized Access: The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) is the main federal statute dealing with various aspects of computer crime in the US. First passed in 1984, it has since been amended several times, for our purposes most significantly in 1986 and 1996 [FN77]. Dealing in part with both criminal prosecutions and civil lawsuits for various computer-related activities involving 'unauthorized access', it employs a fairly dizzying number of terms to describe the various possible offences, thus creating a rather complex and involved statute. For the most part, it

employs two threshold tests that are directly relevant to the question of an overlap with cyber-trespass, *viz.*, the requirements of 'unauthorized access' and of intention. For the former, various subsections utilize (and presumably distinguish between) differing aspects of 'unauthorized access', e.g., as acts of access either 'without authorization' or of 'exceeding authorized access.' [FN78] On the issue of intention, different subsections seem to underscore a potentially-significant distinction between doing an act 'intentionally' and doing it 'knowingly.' A third requirement that merits mention in this respect is \*116 the need for damage to have been caused, and 'damage' is largely crafted in monetary terms and values.

The following are examples of the varying aspects of 'unauthorized access' used in the relevant parts of the CFAA, and shows also the significance of the distinction between acting 'intentionally' and acting 'knowingly.' First, 'knowingly access[ing] a computer without authorization or exceeding authorized access' to obtain information protected for national security reasons and then disclosing it to unauthorized personnel is an offence under § 1030(a)(1.) Secondly, 'intentionally access[ing] a computer without authorization or exceed[ing] authorized access' to obtain either certain financial information, information from a US government agency, or information from a 'protected computer' [FN79] where the conduct involved an interstate or foreign communication, is an offence under § 1030(a)(2)(A), (B) and (C) respectively. Thirdly, accessing 'intentionally [and] without [the requisite] authorization to access any nonpublic computer of a department or agency of the United States' can be an offence under § 1030(a)(3.) Fourthly, furthering a fraud by 'knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access' thereto, is an offence under § 1030(a)(4.) Fifthly (and perhaps most generally applicable to civil cases also resembling cyber-trespass), whoever '(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' commits an offence under § 1030(a)(5)(A) if, additionally, the damage requirement is met [FN80].

The requisite damage for any unauthorized acts under § 1030(a)(5)(A) is listed under § 1030(a)(5)(B) as any of the following: '(i) loss to 1 or more persons during any 1-year period ... aggregating at least \$5,000 in value; (ii) the modification or impairment, or potential modification or impairment, \*117 of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (iii) physical injury to any person; (iv) a threat to public health or safety; or (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.' For most of the kinds of cases under discussion, the relevant head of damage will be that under § 1030(a)(5)(B)(i), which damages, if claimed as the sole injury, are limited expressly to 'economic damages' [FN81]. Damages are also intended to be 'compensatory', though injunctive or other 'equitable relief' is also available as a remedy [FN82].

Several commentators have noted that much computer misuse legislation, including the CFAA, is premised on property notions (and hence property-rule protections) [FN83] and that, outside the US, many jurisdictions have also adopted similar statutes relating to unauthorized access to computers [FN84]. Given the thoughtful and extensive analysis already provided by other authors [FN85] of the US cases of 'unauthorized access', it seems timely, therefore, to examine some non-US legislation and case law in this area, to determine if the approach in non-US jurisdictions on the issue of 'unauthorized access' is similar to that displayed by US courts so far, and what significance, if any, should be attributed to the differing wordings or aspects to 'unauthorized access' captured by these in comparison to the US statutes.

### 3.3 Computer Misuse Legislation in the UK and Singapore

Like their US federal counterpart, the UK and Singapore [FN86] computer misuse statutes also reveal a property-based notion of computer crime, as \*118 well as a lack of clarity or definition as to the concept of 'unauthorized access.' Given that these two statutes were drafted within three years of each other [FN87], it is perhaps not surprising to find these similarities between the two, as well as substantially similar types of offences. For example, with respect to the more general concept of when an act of unauthorized access might constitute a criminal offence, both the Singapore and UK statutes subtitle their respective sections, 'Unauthorised Access to Computer Material.' Section 3 of the Singapore Computer Misuse Act (SCMA) [FN88] states that a person who 'knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer' commits an offence, while section 1 of the UK Computer Misuse Act (UKCMA) states that a person commits an offence if '(a) [he] causes a computer to perform any function with intent to secure access to any program or data held in any computer; (b) the access he intends to secure is unauthorised; and (c) he knows at the time when he causes the computer to perform the function that that is the case.' There are interesting minor variations in language and, possibly, consequential scope, between the two sections. For example, where the Singapore statute uses the phrase 'without authority', the UK equivalent uses the word 'unauthorised.' It would appear that the UK usage is more consistent, at least internally within the statute, as the word 'unauthorised' is used throughout the statute to condition access. In the SCMA, the phrase 'unauthorised access' is used as well as 'access without authority.' It is therefore not surprising that, while the definition of 'unauthorised access' is identical in both statutes, the Singapore statute has an additional phrase, in that its definition does not just encompass when an act is considered to be unauthorised, it applies also to an act that is 'done without authority'. While this might be a trivial point for practical purposes, in principle it seems somewhat unnecessary, and adds avoidable complexity, to have two usages and phrases to describe the one concept.

Another difference in the 'unauthorised access' sections of both statutes is the placement of the knowledge (i.e., intent) requirement. Under section 3 of the SCMA, it is not entirely clear whether the word 'knowingly' is intended to qualify both the causing of a computer to perform a particular function as well as the purpose of securing unauthorised access. In the UKCMA, this point seems clearer, in that the placement and usage of the word 'knows' (in section 1(c)) seems intended to mean the accused knows that the access he is intending to secure is unauthorised. It would thus seem as though there is a higher standard (in there \*119 being more-to prove) for knowledge under the SCMA compared to the UKCMA.

More to the point of the present discussion, however, is the actual definition in both statutes as to what constitutes 'unauthorised access', which, though somewhat unhelpfully limited in some ways [FN89], suggests useful indications of how the UK and Singapore courts would approach Professor Kerr's description of the US problem of what 'access' means [FN90]. Under the SCMA (Section 2(5)) and the UKCMA (Section 17(5)), access is unauthorised if the person in question 'is not himself entitled to control access *of the kind in question* to the program or data, and he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled' (emphasis added.) It ought, however, to be noted that both the SCMA and the UKCMA speak expressly of access 'to any program or data held in any computer' [FN91]. Notwithstanding such an apparent limitation on the concept of access, it is submitted that the principle that access means 'access of the kind in question' ought equally to apply to any other types of access, without any descriptive limits as to whether it is a particular aspect, portion or function of a computer, system or network that is being accessed. There seems no reason in policy or principle to use such a meaning of access only when access is to program or data held in a computer.

At least one UK case has shed some authoritative light as to the interpretation of the phrase 'access of the kind in question.' In *Regina v Bow Street Magistrates Court and Allison (A.P.) ex parte Government of the United States of America* [FN92], the House of Lords clarified unanimously that as a 'plain meaning subsidiary' to the other substantive provisions of the Act (including Section (1)), 'the authority must relate not simply to the data or programme but also to the actual kind of access secured. [T]he word 'control' [does not mean] a physical sense of the ability to operate or manipulate the computer. It does not introduce any concept that authority to access one piece of data should be treated as authority to access other pieces of data 'of the same kind' notwithstanding that the relevant person did not in fact have authority to access that piece of data. Section 1 refers to the intent to secure unauthorised access to any programme or \*120 data. These plain words leave no room for any suggestion that the relevant person may say: 'Yes, I know that I was not authorised to access that data but I was authorised to access other data of the same kind'.' As such, in the *Allison* case, a credit analyst who obtained confidential data from a part of her employer's database that she did not have the authority to access (although she had the ability to do so) was held to have secured 'unauthorised access' to such data within the meaning of Section 1 of the UKCMA [FN93].

This ruling by the House of Lords thus laid to rest some doubts that had been created by a wider reading of Section 17(2) and the concept of 'unauthorised access' in an earlier case, *D.P.P. v Bignell* [FN94]. While being careful to say that the Divisional Court in *Bignell* might well have reached a correct conclusion on the facts, the House of Lords in *Allison* stated firmly that the court had erred in its interpretation of Section 17(5) (and thus, Section 1) by misreading the language of Section 17 and glossing over certain concepts under the UKCMA, including reading access to mean 'access to data of the kind in question' rather than, more generally, 'access of the kind in question' to the relevant data. [FN95] The House of Lords cited the Working Party Paper and Report of the Law Commission that led to the passage of the UKCMA, noting that it had considered problems of insider misuse of computers and systems to be as significant as 'hacking' by outsiders. The narrower *Bignell* interpretation of the language and purpose of the UKCMA would have limited the mischief the Act was meant to deal with.

The House of Lords' insistence on the 'plain meaning' and clarity of Sections 1 and 17 of the UKCMA is to be welcomed, as is its acknowledgment of the correctness of the court's decision on the facts in *Bignell*, despite that court's misinterpretations of the law. The fact that the *Allison* and *Bignell* decisions ultimately went the opposite way on the facts is not problematic, as they each illustrate the proper reach and application of Section 1, read with Section 17. Where the employee in *Allison* who was alleged to have conspired with Mr. Allison had the ability to access the entire database but had authority only to access certain data records within it, her access of those records she was not supposed to access must surely be illegitimate. The House of Lords held that those acts fell 'squarely' within the ambit of Section 1. In contrast, the police employee in *Bignell* who obtained confidential data for the two police officers \*121 charged under Section 1 had both the ability and the authority to access the entire database and the data within it. He only provided the data to the two officers because they misrepresented the purpose of their request to him. In both cases, therefore, it can be said that each court reached the correct decision on the facts, as to whether 'access of the kind in question' was authorized or not.

Both *Bignell* and *Allison* were considered by a Singapore district court in *Public Prosecutor v Loh Chai Huat*. [FN96] The district judge adopted a wide reading of Section 3 of the SCMA (the equivalent of Section 1 of the UKCMA) on the basis that this gave effect to the legislative intent to capture as many offences involving unauthorized access as possible. She also held that the purpose for the access could be relevant in determining whether access was authorized, that authorization was to be determined at the point of access and that the knowledge requirement included willful blindness to the effects of one's actions [FN97]. In *Lim Siong Khee v Public*

*Prosecutor* [FN98], the question of access 'without authority' under Section 3 of the SCMA (and, correspondingly, Section 2(5) regarding 'access of the kind in question to the program or data') was considered by the Singapore High Court. The Court held that even where a person may have had the consent of another person to access the latter's email account for the purpose of assisting that other person with access while the two were traveling abroad, such consent would not extend to accessing the account once they had returned, in order to send off 'lurid emails' or to track the account-holder's movements. Where free web-based email services were concerned, the Court considered also that 'consent' for the purpose of access meant the consent of the account-holder and not the email service provider. [FN99] In reaching this conclusion, the Court acknowledged this to be the 'general understanding of both consumers and the industry', thus demonstrating a commonsensical and practical approach that tacitly bases a legal rule on social and commercial norms.

Unlike the US, neither the UK nor Singapore statutes expressly include or create offences that depend on a person's having exceeded their authority. Nevertheless, in discussing *Bignell*, the House of Lords in \*122 *Allison* stated that the police computer operator in *Bignell* 'did not exceed his authority' when he acted on the request by the police officers to access and provide them with the data they wanted. In *Loh Chai Hual*, the Singapore district court opined that if the police database was meant to be used only for investigating a police officer's own cases, the officer would have exceeded his authority to access it if he used it to screen for third parties; similarly, if access was to be for a particular purpose, access for an extraneous or forbidden purpose would exceed authorized access. It is interesting that the courts in these countries would be likely to treat any act outside the person's *right* and *ability* to conduct access *of the kind in question* to be an act that exceeded that person's authority. In many instances, of course, this will almost certainly be the case, as to exceed one's authority must necessarily largely follow from having reached the limits of that authority. The UKCMA and SCMA, however, are of particular assistance in this regard because they circumscribe the extent and nature of authorized access, in Sections 17(5) and 2(5) respectively. The judges in the cases discussed above also refer expressly to Parliamentary intent to capture not only hacking into a computer system by outsiders, but also the abuse of authority (such as misuse of network access privileges) by insiders. The distinction between computer misuse by an insider and an outsider is generally statutorily expressed through a distinction between 'access without authorization' (outsider misuse) and 'exceeding authorized access' (insider misuse), as in the US CFAA. The UK and Singapore legislatures, however, seem to have elected to fold these two related concepts into a more general unifying principle of 'unauthorized access', and this seems to have been recognized, even if it was only in *dicta*, by the case law in those jurisdictions. Since the US CFAA already contains a definition for 'exceeding authorized access' that requires access 'without authorization' (in order to obtain access to or alter information within the computer that the accessor is not entitled to access), it is open to the US courts to also adopt an approach toward 'unauthorized access' that resembles the UK and Singapore approaches of, first, conditioning access by reference to the *type* of access at issue in the particular case, and secondly, by expressly relating authorization to both the right (entitlement to control) and the ability (consent to access) to that particular form of access,.

The structure and language of the SCMA and the UKCMA [FN100] are such that the courts in those jurisdictions have to parse the language very finely, in the context of the statutory purpose, in order to determine if and to what extent the alleged criminal activities fall within their scope. While the US CFAA is highly similar in scope and purpose to the SCMA \*123 and the UKCMA, its legislative history and specific language is sufficiently different such that it is possible that US courts may well have different basis and reasons for having a different - whether wider or narrower - interpretation of 'unauthorized access' under the US law. To the extent that none of these legislatures have clearly defined this concept, a different approach by the US courts that would create a greater divergence in meaning with other common law countries utilizing the same general

concept may be unfortunate. The UK and Singapore statutes, and their respective courts, seem to demonstrate a commonsensical approach toward refining the existing statutory definition of 'unauthorised access' without undue linguistic acrobatics. It is true that there may be a stronger basis for this approach in these countries, given the clearer statutory expression of legislative intent therein, but there seems little difficulty in either principle or policy that would prevent the US courts from following the same approach.

It has been noted that computer misuse statutes were passed as a legislative means to deal with forms of cybercrime that could not be dealt with adequately under traditional criminal laws. [FN101] The principles and rules behind trespass, burglary and theft provided a 'natural conceptual point of departure' [FN102], buttressed by the prevalence of the property metaphor [FN103]. As a result, statutes such as the CFAA, UKCMA and SCMA reveal a reliance on property concepts, particularly in the notions of 'access' [FN104] and the causation of damage. [FN105]

Where 'access' is concerned, viewing this concept through a property lens can affect how broadly, and how, a court interprets it. Whether one views virtual 'access' (e.g., to a website, database or computer system) as approximating (metaphorically) real-world entry to a physical place (e.g., a shop or library, including, perhaps, a 'lock' to such a 'place' manifested by the need to key in a password or access code), or whether the same act of virtual access occurs only when the user 'interacts' with the computer (e.g., either by just the sending of a message or data query, or perhaps requiring the consequent response, whether automated or otherwise, by the computer) can affect when, legally, access is deemed to have taken \*124 place. Although no clear approach has emerged in the US case law, at least one court has taken an extremely broad approach to 'access' under the CFAA, stating that '[f]or purposes of the CFAA, when someone sends an e-mail message from his or her own computer, and the message then is transmitted through a number of other computers until it reaches its destination, the sender is making use of all of those computers, and is therefore 'accessing' them.' [FN106]

Additionally, whatever the conclusion on 'access', whether such access is then 'unauthorized' can also depend on various perspectives [FN107]. At least two possibilities in this regard have already surfaced in the US case law on 'unauthorized access': either violating a contractual or other express notice (e.g., the AOL cases, *Register.com*), or bypassing a code-based restriction on access (e.g., *CompuServe* and *eBay*.) Should the US courts adopt a broad approach not just to the question of 'access' but also to that of 'authorization' (as arguably, they may already have done in some of these cases), particularly if they do so without much in-depth analysis of the meaning of each word as well as the phrase as a whole (as in *Register.com*), the implications for open access and doctrinal vagueness can be worrying.

### 3.4 Defining 'Unauthorized Access': Proposals and Problems

The potential difficulties with viewing unauthorized access from a pure property perspective have already been noted [FN108]. Professor Orin Kerr has suggested that the US courts adopt a broad construction of the word 'access' and narrow the scope of 'unauthorized access' by limiting the meaning of 'unauthorized' to cases only where code-based restrictions have been circumvented; a violation of contractual restrictions (much less notices of lack of consent) would not suffice. [FN109] Code-based restrictions, however, are to be limited only to those instances where the user tricks the computer into allowing her privileges she would not otherwise have (e.g., by entering a false access code or by exploiting a weakness in the code such as to bypass the program's intended function.) Professor Kerr's formulation of code-based restrictions for unauthorized access purposes thus would not include the sort of behavior at issue in *eBay*, where the spider ignored the technological robot exclu-

sion header (whether or not there was notification or a contractual term governing the existence and treatment of such technology.) Nor would it include other self-help cases such as *CompuServe* and *Intel*, where the plaintiffs had endeavored to block or evade the defendants' activity through \*125 technological and other means. The exclusion of these cases and activities from Professor Kerr's proposal, however, is not necessarily a bad thing. If these cases, which are outside of the CFAA context, continue to be good law (i.e., as tort cases), the plaintiff who can show the necessary interference and damage can still claim against a defendant intruder. Much of the concern over an overly broad interpretation of 'unauthorized access' stems from the fact that computer misuse legislation governs mostly criminal conduct, with only certain allowances for recovery in some civil cases (such as under the CFAA § 1030(a)(5.)) To allow contract-based restrictions (particularly when they are liberally construed in favor of the party imposing the terms) and civil law concerns (e.g., of unfair competition) to dictate the scope of the main 'trigger' concept for criminal liability seems unwise.

The same holds true even outside of the US, possibly even more so. In the UK and Singapore, which were the two jurisdictions whose 'unauthorized access' provisions were examined, there is no allowance under the UKCMA or the SCMA for civil proceedings against the perpetrator of the intrusive act, unlike the US CFAA. This may reduce the risk that civil cases and their interpretations of a concept also utilized in the criminal law will dictate how that concept will be applied in a criminal case. Since the types of private and public interest protected by the civil (tort and contract) law can differ significantly from those protected by the criminal law, this prevention of 'doctrine creep' would be welcome. The fact remains, however, that in the UK and Singapore, those few criminal cases of computer misuse have shown that the courts there adopt a fairly liberal approach toward the concept of 'unauthorized access', albeit for public policy reasons rooted primarily in the criminal law (e.g., the legislative intent to cast as wide a net as possible over as many acts of computer intrusion as possible while remaining technology-neutral. [FN110]) There may thus still be a possibility that, even without a specific allowance for civil proceedings, unauthorized access statutes could 'criminalize the law of contract involving the use of computers' [FN111] in the UK and Singapore. Whether this will turn out to be the case could depend, in large part, on whether or not civil cases arise in these jurisdictions that invite the courts \*126 to consider notions of unauthorized access. Specifically, if civil cases are brought in a UK or Singapore court alleging cyber-trespass, the courts there will have to determine whether or not they will follow the lead of the US courts in adapting the trespass to chattels doctrine to cyberspace. In so doing, they may well have to confront fact situations similar to those in the cases described above, in which case they may have to decide whether or not activities such as violating a TOS, bypassing a technical restriction or ignoring a notice to stop the unwanted act constitutes the necessary interference. In effect, then, the courts in such instances will be asked to rule on 'unauthorized access' in a civil context. The interesting question that could arise in the future, assuming the US approach is the direction the UK and Singapore courts choose to take, is whether or not such decisions will in turn affect the criminal courts' interpretation of 'unauthorized access' under the computer misuse statutes. Given the already-broad approach taken in *Allison* and the Singapore cases, this may not, however, be much of an issue. Conversely, it is also possible that the inapplicability of the UKCMA and SCMA to civil cases would militate against a criminal court's looking to civil cases to inform its decision, particularly as cyber-trespass cases are not expressly predicated on 'unauthorized access', even though in effect, at their broadest, they probably are.

The preceding discussion shows a general similarity in approach between the US, UK and Singapore courts with respect to whether a wide or narrow interpretation of 'unauthorized access' ought to be taken under their respective statutes. Although the UK and Singapore statutes are structured somewhat differently from the US CFAA, the 'trigger' for liability (criminal) is practically identical. The US CFAA, however, has the added complication of an act 'exceeding authorized access', so the US courts will have the additional task in some cases of

parsing and distinguishing that concept from 'access without authorization.' One way of looking at the problem could be to say that where the US federal law distinguishes between 'access without authorization' and 'exceeding authorized access', the UKCMA considers both as aspects of and under the rubric of 'unauthorized access', such that which aspect a particular case raises would be a question of fact and dependent on the circumstances of each case. The problem with this approach, however, is that the Singapore statute appears to have taken a position slightly out of sync with it, in that the SCMA uses both 'unauthorised access' and 'access without authority.' Yet this may not pose too much of a definitional problem as the SCMA seems to use these two phrases almost interchangeably. It may thus be possible to construe 'unauthorized access' as a general concept that includes 'access without authorization (or without authority)' as well as 'exceeding authorized access.' Besides according with some of the usages in the US CFAA and Parliamentary intent in the UK and Singapore, such recognition would certainly introduce an element of uniformity that would be welcome in this rather complex and, so far, relatively unstudied area of law.

#### **\*127 4 Conclusion**

The US cyber-trespass cases offer an interesting study of the problem of providing a legal remedy in cases of unwanted intrusive activity, where such activity is considered unwarranted in the sense that it is seen to damage the plaintiff's legitimate business or other interests. In granting injunctive remedies against further and repeated intrusions, the US courts have applied and extended a longstanding common law doctrine in a fairly imaginative and liberal way. Despite the volley of academic alarm over the extent of this application and the implications thereof [FN112], it is possible to view the courts' actions, simply, as doing the right thing once the plaintiff presents a convincing case that her interests are in need of a legal remedy. One may thus question the method (particularly where this either confuses different doctrines and concepts, or pays short shrift to the implications or risks of doing so) but not the fairness of the result. A non-US court should thus pay heed not just to the conceptual leaps it may be asked to make in the context of the traditional trespass to chattels doctrine, but also to the competing interests involved in ruling one way or the other. Although the rise of anti-'spam' legislation and specific remedies therefor may alleviate the need for trespass notions to be applied to 'spam' cases, there will be other instances where the plaintiff will have no other recourse than to try to persuade a court to apply cyber-trespass principles, including where the defendant is alleged to have engaged in unfair competitive behavior. Whether a non-US common law court will tread the same path as the US courts have done remains to be seen, but it is hoped that, whatever the outcome, a more thorough conceptual examination, interest-balancing exercise and risk analysis will be performed than seems to have been the case hitherto in the US.

The other main point of this article has been the lack of recognition of the potential overlap between a broad doctrine of cyber-trespass and the concept of 'unauthorized access' in computer misuse legislation (and cases arising thereunder.) Since the latter concept applies primarily to criminal conduct outside the US, it is perhaps not surprising that the overlap has not been acknowledged by a non-US court which has in any case yet to see its first case of cyber-trespass. On the other hand, the fact that 'unauthorized access' can also form the basis for a civil claim in the US, coupled with the line of cyber-trespass cases there, means that an analysis of the implications of an overlap between the two concepts is perhaps timely, but has to date not been highlighted as much as it could have been.

**\*128** Non-US courts could thus have a unique opportunity to explore the conceptual and practical implications of both cyber-trespass and 'unauthorized access' principles. It is also not too late, nor irrelevant, for US courts faced with a civil claim under the CFAA to do so. Any such judicial analysis would be a welcome move

toward consistency and a greater comparative understanding of concepts that have a common basis and similar grounds in the jurisdictions highlighted in this article.

[FN1]. LLB (NUS), LLM (Cantab.), Professor of Law, Franklin Pierce Law Center, USA, E-mail: fatamagistra@gmail.com This paper was funded by the Office of Research at the Singapore Management University (SMU), where the author was an Associate Professor of Law. I would like to thank Professor Bobby Mariano and the staff at the SMU Office of Research, my former colleagues at SMU and my current colleagues at Pierce Law for their encouragement and support of this research. All errors and omissions remain, of course, my own.

[FN1]. If not entirely meaningfully, in particular, there has been doubt cast on whether there is a distinct area of law known as 'cyberlaw'; see, e.g., Joseph H. Sommer, 'Against Cyberlaw', 15 *Berkeley Tech. L. J.* 1145 (2001), and Frank Easterbrook, 'Cyberspace and the Law of the Horse', 1996 *U. Chi. Legal F.* 207. See also a response to Professor Easterbrook by Lawrence Lessig, 'The Law of the Horse: What Cyberlaw Might Teach', 113 *Harv. L. Rev.* 501 (1999.)

[FN2]. Meaning, generally, the common law of the United Kingdom and as followed in its former colonies and territories.

[FN3]. See I. Trotter Hardy, 'The Ancient Doctrine of Trespass to Websites', 1996 *J. Online L.* art 7.

[FN4]. There also seems to be comparatively little academic commentary on this issue outside of the US, perhaps understandably given the lack of case law even under traditional trespass to goods and/or 'unauthorized access' principles. An analysis of the US cyber-trespass cases in the broader context of proposing that the 'rule' in the English case of *Wilkinson v Downton* (commonly viewed as narrowly limited to the availability of a claim in tort for nervous shock) is wide enough to include acts that would have been actionable under the older forms of action (such as trespass on the case) is, however, provided by John Adams in 'Trespass in a Digital Environment', (2002) *I.P.Q.* 1. This argument is discussed further *infra*.

[FN5]. See Kerr, *infra* n 84 and Schjolberg, *infra* n 70; for the present, the reader should note that the phrase 'unauthorized access' is used to cover other terms and phrases also used in such statutes, e.g., 'exceeding authorized access', 'access without right', 'access without authority', and so on.

[FN6]. Interestingly, however, the US Computer Fraud and Abuse Act (the main federal law governing computer misuse) contemplates and permits civil actions as well as criminal prosecutions. Certain of the former type of cases will be discussed *infra*.

[FN7]. At least, in relation to the federal US law of 'unauthorized access' to computer systems: see the Computer Fraud and Abuse Act (18 U.S.C. § 1030 *et seq.*)

[FN8]. See, e.g., R.F.V. Heuston and R.A. Buckley, *Salmond & Heuston on the Law of Torts* (21<sup>st</sup> ed., Sweet & Maxwell: 1996.) Margaret Brazier also covers similar ground, fairly comprehensively and at similar length, in *Street on Torts* (8<sup>th</sup> ed., Butterworths: 1988.) In *Winfield and Jolowicz on Tort* (15<sup>th</sup> ed., Sweet & Maxwell: 1998), W.V.H. Rogers also discusses the origin of these actions and describes trespass to goods fairly thoroughly, if briefly, as do Markesinis and Deakin, in *Tort Law* (4<sup>th</sup> ed., Oxford University Press: 1999.)

[FN9]. Salmond & Heuston state that 'A trespass to goods is actionable *per se* without any proof of actual dam-

age. Any unauthorized touching ... is actionable at the suit of the possessor of it, even though no harm ensues' (at 95, citing *dicta in Leitch v Leydon* [1931] AC 90.) Winfield & Jolowicz assert this principle slightly less generally, stating that '[d]espite the fact that trespass is actionable *per se*, there is some authority to the effect that trespass to goods requires proof of some damage [though] the general view of textbook writers is to the contrary' (at 585-6.)

[FN10]. See, e.g., Markesinis and Deakin, who write (at 407) that '[i]t is not altogether clear whether liability is based on damage or whether the tort is actionable *per se*. It may be possible to distinguish between deliberate touchings, which are actionable *per se*, and unintended or careless acts of touching, which require damage.'

[FN11]. See *Street on Torts*, *supra* n 8, at 60.

[FN12]. Meaning the actionable wrong (or the act complained of) and not the damage or loss caused and suffered.

[FN13]. *Salmond & Heuston on the Law of Torts*, *supra* n 8, at 4-7.

[FN14]. *Ibid.*

[FN15]. Except for abolishing the action in detinue; the Act now uses the term 'wrongful interference' as a comprehensive phrase for all torts affecting dispossession, interferences and other interests in goods, including conversion.

[FN16]. The Act has been described by *Winfield & Jolowicz*, *supra* n 8, as 'a piecemeal attempt to deal with certain deficiencies in the common law [arising from the 'long survival and overlap of a number of different heads of liability] and is in no way a code governing interference with goods.' In the same passage, the authors assert that trespass remains 'essentially a wrong to possession'.

[FN17]. In *CompuServe, Inc. v Cyber-Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997.)

[FN18]. Restatement (Second) of Torts (1965.)

[FN19]. 'Intermeddling' means 'intentionally bringing about a physical contact with the chattel': see *ibid.*, § 217.

[FN20]. § 218, *ibid.*

[FN21]. According to § 217, comment (a) to the Restatement, where an interference causes no harm either to the chattel itself or to any other 'legally protected interest of the possessor, [it] affords the possessor a privilege to use force to defend his interest in its exclusive possession.' § 218, comment (e), further states that '[t]he interest of a possessor of a chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel. In order that an actor who interferes with another's chattel may be liable, his conduct must affect some other and more important interest of the possessor.'

[FN22]. *Prosser and Keeton on Torts* (5th ed., 1984), § 15, p 92.

[FN23]. § 218, comment (e.)

[FN24]. *Supra* n 17.

[FN25]. 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996).

[FN26]. In this case, commencing with the manual entry of randomly-guessed authorization codes followed subsequently by the use of software to automate searches for those codes.

[FN27]. Bulk unsolicited electronic mail messages.

[FN28]. Which the court found based on the fact that any value CompuServe realized from its computer equipment was 'wholly derived from the extent to which that equipment can serve its subscriber base.' In addition, damage to the value of the chattel could be found in the burden the 'spam' presented to the system and the resources employed to deal with it.

[FN29]. 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

[FN30]. 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *aff'd* 356 F. 3d 393.

[FN31]. 114 Cal. Rptr. 2d 244 (2002), *rev'd* 30 Cal. 4<sup>th</sup> 1342 (2003.)

[FN32]. See, e.g., Dan L. Burk, 'The Trouble With Trespass', *J. Small & Emerging Bus. L.* 1 (Vol. 3, 1998), Edward W. Chang, 'Bidding on Trespass: *eBay, Inc. v Bidder's Edge, Inc.* and the Abuse of Trespass Theory in Cyberspace Law', 29 *AIPLA Q.J.* 445 (2001), Steve Fischer, 'When Animals Attack: Spiders and Internet Trespass', 2 *Minn. Intell. Prop. Rev.* 139 (2001), Richard Warner, 'Border Disputes: Trespass to Chattels on the Internet', 47 *Vill. L. Rev.* 117 (2002), Jeffrey M. Rosenfeld, 'Spiders and Crawlers and Bots, Oh My: The Economic Efficiency and Public Policy of Online Contracts that Restrict Data Collection', 2002 *Stan. Tech. L. Rev.* 3, Laura Quilter, 'The Continuing Evolution of Cyberspace Trespass to Chattels', 17 *Berkeley Tech. L. J.* 421 (2002), R. Clifton Merrell, 'Trespass to Chattels in the Age of the Internet', 80 *Wash. U. L. Q.* 675 (2002), and Richard A. Epstein, 'Cybertrespass', 70 *U. Chi. L. Rev.* 73 (2003.) Academic comment on the California Supreme Court decision in *Intel v Hamidi* include George H. Fibbe, 'Screen-Scraping and Harmful Cybertrespass After Intel', 55 *Merrill L. Rev.* 1011 (2004), Patty M. DeGaetano, '*Intel Corp. v Hamidi*: Private Property, Keep Out - The Unworkable Definition of Injury for a Trespass to Chattels Claim in Cyberspace', 40 *Cal. W. L. Rev.* 355 (2004), Steven Kam, '*Intel Corp. v Hamidi*: Trespass to Chattels and a Doctrine of Cyber-Nuisance', 19 *Berkeley Tech. L. J.* 427 (2004) and a comment in the Recent Development section of the Fall 2003 issue of the Harvard Journal of Law and Technology, 'Trespass to Chattels and the Internet: *Intel v Hamidi*', 17 *Harv. J. L. & Tech.* 283 (2003.)

[FN33]. For example, eBay claimed successfully against the online auction aggregator Bidder's Edge, where the latter had conducted unauthorized, regular, 'real-time' automated searches (and consequent results gathering) of eBay's auction listings by utilizing 'spidering' search technology. The parties had previously attempted to negotiate a license for such activity, and eBay had also engaged in technological 'self-help' by utilizing robot exclusion headers to detect electronic robot activity. Register.com claimed successfully against Verio, who had used a robot to search Register.com's publicly-accessible WHOIS registrant database, and then sent unsolicited emails to those registrants offering Verio's competing services.

[FN34]. The fact that the plaintiff in a case may first have relied on 'self-help' mechanisms, including technological tools such as robot exclusion headers and 'spam' filters, can also be taken to show that the plaintiff has thereby used her best efforts to defend her chattel's 'inviolability', in that the 'self-help' constituted the 'reasonable force' to defend her property required by §218 of the Restatement.

[FN35]. See McGowan, *infra* n 59.

[FN36]. Particularly where such proprietary assertions can be viewed as an expansion of property rights: see discussion *infra*.

[FN37]. See the amicus brief filed by 28 law professors in the *eBay* case in support of Bidder's Edge, filed June 22, 2000, available online at [http://jurist.law.pitt.edu/amicus/biddersedge\\_v\\_ebay.pdf](http://jurist.law.pitt.edu/amicus/biddersedge_v_ebay.pdf) (page last accessed June 16, 2005.)

[FN38]. Its primary business is not domain name registration but website hosting and other Internet-related services such as access and collocation: see <http://www.verio.com> (page last accessed August 1, 2005.)

[FN39]. *Supra* n 37.

[FN40]. See Burk, *supra* n 32, at 23-28 and the sources cited therein.

[FN41]. Michael J. Madison, 'Rights of Access and the Shape of the Internet', 44 *B. C. L. Rev.* 33 (2003), and Burk, *supra* n 32. See also Dan Hunter, 'Cyberspace as Place and the Tragedy of the Digital Anticommons', 91 *Cal. L. Rev.* 439 (2003), Mark A. Lemley, 'Place and Cyberspace', 91 *Cal. L. Rev.* 521 (2003). Jacqueline Lipton, 'Mixed Metaphors in Cyberspace: Property in Information and Information Systems', 35 *Loy. U. Chi. L. J.* 235 (2003), and Ronnie Cohen and Janine S. Hiller, 'Towards a Theory of Cyberplace: A Proposal for a New Legal Framework', 10 *Rich. J. L. & Tech.* 2 (2003.) The arguments put forth by some of these authors are analyzed in the context of trespass by David McGowan, 'The Trespass Trouble and the Metaphor Muddle', Minnesota Legal Studies Research Paper No. 04-5. Professor McGowan also discusses Professor Burk's analysis of the real property/personal property reasoning in the cyber-trespass cases, and contends that many of these authors were not correct in asserting that the courts in the cyber-trespass cases conflated real and personal property principles. For an early proposal to apply trespass theory and property rights to websites, see I. Trotter Hardy, *supra* n 3.

[FN42]. See Orin S. Kerr, 'The Problem of Perspective in Internet Law', 91 *Geo. L. J.* 357 (2003) and Brett M. Frischmann, 'The Prospect of Reconciling Internet and Cyberspace', 35 *Loy. U. Chi. L. J.* 205 (2003), for a thought-provoking analysis of the 'outcome-determinative' nature of differing perspectives of the Internet; *viz.*, the 'internal' (subjective to the user who is enabled and affected by it) and the 'external' (viewing the internet as essentially a tangible communications medium.) Professor Frischmann suggests that both perspectives provide different but accurate, and thus 'descriptively valid', snapshots of the facts and interests in a cyberlaw dispute.

[FN43]. *Ticketmaster Corp. v Tickets.com, Inc.*, 2000 U.S. Dist. LEXIS 12987 (C.D. Cal. 2000.) The court apparently also thought that if the act constituted a trespass under state law, it would be caught by the pre-emption provisions of the US Copyright Act.

[FN44]. Comment (c) to § 217 of the Restatement.

[FN45]. Madison, *supra* n 41. Professor Madison notes that the courts in the cyber-trespass cases have not highlighted the requirement of intention in the tort (which he points out is a rather 'ambiguous' concept), but have, rather, focused on a fairly loose interpretation of the damage caused by the defendant's activity constituting 'intermeddling' and the plaintiff's lack of consent to such activity. Although he suggests that the courts may have largely treated intention as merely a threshold distinguishing knowingness from negligence, he notes, fur-

ther, that this has had the effect of conflating trespass to chattels with trespass to land.

[FN46]. *Winfield & Jolowicz on Tort, supra* n 8, at 50. The example given is of a man who throws his coffee dregs out of his office window knowing that people may be passing by underneath it.

[FN47]. *Ibid.*

[FN48]. Before the California Supreme Court overturned the Appeals Court in *Intel*, a similar point had been made by Professor Dan Burk in relation to the Appeals Court decision in *Intel* and the earlier cases; see Burk, *supra* n 32.

[FN49]. Whether the 'place' is defined as that arena where computers, networks, servers, routers and so on connect people and enable their interaction, or as that 'virtual world' where interactions still cause the kind of tangible reactions and consequences as the 'real world' with which it is often compared and analogized.

[FN50]. Some judges do distinguish between real and personal property, but acknowledge that, e.g., ongoing trespasses to computer systems can be 'more akin to the traditional notion of a trespass to real property than the traditional notion of a trespass to chattels because even though it is ongoing, it will probably never amount to a conversion': *per* the court in *eBay v Bidder's Edge, supra* n 29.

[FN51]. As has been pointed out by some commentators, while cases prior to and relied on by *CompuServe* and subsequent decisions have found that microscopic particles and sound waves constituted trespass, they were mostly cases of trespass to land. As such, this serves as an example of the easy borrowing from real property doctrine in this area. Although it may be possible and even necessary that certain tiny and/or intangible intrusions could be sufficiently substantial (e.g., by repeated occurrence) to sustain a trespass to chattels action (the example that springs to mind would naturally be 'spam'), the point remains that the application of real property-based reasoning should be only where appropriate, and within the conceptual framework of the trespass torts.

[FN52]. See McGowan, *supra* n 41 and the authors whose 'metaphor claims' he discusses.

[FN53]. In the main, pre-*Intel*, damage had been found in what amounted, basically, to the commercial value of the chattel, measured by its value to the normal business functions of its possessor rather than the market value of the chattel itself; e.g., the potential server and network overloads that could occur if the defendant's acts remained unchecked and undeterred (e.g., *eBay*), the loss of customer goodwill and use of resources to deal with 'spam' (*CompuServe*.)

[FN54]. Hardy, *supra* n 3.

[FN55]. Burk, *supra* n 32.

[FN56]. Adams, *supra* n 4. He notes that the US courts 'have rediscovered a powerful weapon which, understood properly in its historical context, is capable of encompassing many objectionable Internet activities ...'. The premise for an action on the case in instances of cyber-trespass is drawn from, of all things, the 'rule' in the English case of *Wilkinson v Downton* (1897) 2 Q. B. 57, which has traditionally been formulated as a narrow rule governing recovery in tort for nervous shock, and thereby classified by modern texts as a 'residuary' tort (*Winfield & Jolowicz on Tort, supra* n 8.) Adams argues, however, that the contemporary view of the case was broader and fit well into the ambit of an action on the case, which can be pressed into action to deal with the sort of Internet-based activities that would not otherwise amount to trespass as traditionally conceived.

[FN57]. See Adams, *ibid*, and Quilter, *supra* n 32.

[FN58]. These issues include the questions: (a) whether and how consent or assent to terms (or a legally binding acceptance thereof) can be manifested in electronic contracts such as 'clickwrap' and 'browsewrap' contracts, (b) the problems posed by standard form contracts and 'contracts of adhesion' (or unfair and unilaterally-imposed contractual terms), and (c) the enforceability of such contracts. There has been, to date, only one UK case on these issues, in respect of when acceptance of the terms of a 'shrinkwrap' license took place: *Beta Computers Europe Ltd v Adobe Systems Europe Ltd*, 1996 FSR 367. In this area, as in cyber-trespass, the US courts have seen far more litigation activity than elsewhere. See, e.g., *Step-saver Data Systems, Inc. v Wyse Technology*, 939 F.2d 91 (3d Cir. 1991), *Pro CD, Incorporated v Matthew Zeidenberg and Silken Mountain Web Services, Inc.*, 86 F. 3d 1447 (7<sup>th</sup> Cir. 1996), *Hill v Gateway 2000, Inc.*, 105 F. 3d 1147 (7<sup>th</sup> Cir. 1997), *Hotmail Corp. v Van\$ Money Pic Inc.*, 47 U.S.P.Q.2d 1020 (N.D. Cal. 1998), *Brower v Gateway 2000 Inc.*, 676 N.Y.S.2d 569 (1<sup>st</sup> Dep't 1998), *M. A. Mortensen Co. v Timberline Software Corp.*, 970 P. 2d 803 (Wash. Ct. App. 1999), *Caspi v. Microsoft Network, LLC*, 732 A. 2d 528 (N.J. Super. Ct. App. Div. 1999), *Klocek v Gateway, Inc.*, 104 F. Supp. 2d 1332 (D. Kan. 2000), *Register.com, Inc. v Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), *iLan Sys., Inc. v NetScout Serv. Level Corp.*, 183 F. Supp. 2d 328 (D. Mass. 2002), and *Christopher Specht, John Gibson, Michael Fagan, Sean Kelly, Mark Gruber and Sherry Weindorf (individually and on behalf of all others others similarly situated) v. Netscape Communications Corporation and America Online, Inc.*, 150 F.Supp.2d 585 (2001.) For just a few examples of the academic commentaries generated by these issues and cases, see, e.g., Robert A. Hillman and Jeffrey J. Rachlinski, 'Standard Form Contracting in the Electronic Age', 77 *N. Y. U. L. Rev.* 429, Donnie L. Kidd, Jr. and William H. Daughtrey, Jr., 'Adapting Contract Law to Accommodate Electronic Contracts: Overview and Suggestions', 26 *Rutgers Computer & Tech. L. J.* 215, Dan Streeter, 'Into Contract's Undiscovered Country: A Defense of Browse-Wrap Licenses', 39 *San Diego L. Rev.* 1363, James J. White, 'Default Rules in Sales And The Myth of Contracting Out', 48 *Loy. L. Rev.* 53, Roger E. Schechter, 'The Unfairness of Click-On Software Licenses', 46 *Wayne L. Rev.* 1735, Drew Block, 'Caveat Surfer: Recent Developments In The Law Surrounding Browse-Wrap Agreements, And The Future of Consumer Interaction With Websites', 14 *Loy. Consumer L. Rev.* 227 and Melissa Robertson, 'Is Assent Still A Prerequisite For Contract Formation In Today's Economy?' 78 *WALR* 265. Madison, *supra* n 41, also discusses these issues and cases in the specific context of access control, together with other mechanisms besides cyber-trespass, such as anti-circumvention technology.

[FN59]. See David McGowan, 'Website Access: The Case for Consent', 35 *Loy. U. Chi. L. J.* 341 (2003), arguing that property rules and not liability rules ought to govern website access; website owners are deemed to consent to any lawful use of that site, unless her choice to exclude (i.e., no consent) is notified to the user.

[FN60]. *Supra* n 37.

[FN61]. Such as copyright for original material, or even for some databases possessing the requisite amount of originality. In the EU, databases can be protected under national laws implementing the *sui generis* right created by the EU Database Directive of 1996 (Directive 96/9/EC.)

[FN62]. See, e.g., the situations, cases and proposals discussed in Madison, *supra* n 41.

[FN63]. It should be noted that, besides *CompuServe*, the US courts have also applied trespass to chattels analysis to other cases of 'spamming' brought by another Internet service provider: see, e.g., *America On Line, Inc. v LCGM, Inc.* 46 F. Supp. 2d 444 (E. D. Va. 1998) and *America On Line, Inc. v IMS*, 24 F. Supp. 2d 548 (E. D. Va. 1998). Since this paper was completed, US courts have (in preliminary rulings denying defendant's motion

to dismiss) indicated that trespass to chattel may be a ground for action against unwanted installation of 'spyware' on a home computer: see, e.g., *Stephen Sotelo v DirectRevenue LLC*, No. 05 C 2562 (N.D. Ill. Aug. 29, 2005) and *Thomas Kerrins v Intermix Media, Inc.* No. 2: 05-cv-05408-RGK-SS (C.D. Cal. Jan. 10, 2006).

[FN64]. In the US, the CAN-SPAM Act was signed into federal law by President Bush in 2003. There has been a growing number of articles analyzing the need for and efficacy of this and similar legislation; for a few examples, see Elizabeth A. Alongi, 'Has the U.S. Canned Spam?', 46 *Ariz. L. Rev.* 263 (2004), Adam Mossoff, 'Spam - Oy, What a Nuisance!', 19 *Berkeley Tech. L. J.* 625 (2004), and Adam Zitter, 'Good Laws for Junk Fax? Government Regulation of Unsolicited Solicitations', 72 *Fordham L. Rev.* 2767 (2004.)

[FN65]. This consisted of annoyance and upset on the part of some recipients of Hamidi's anti-Intel emails, and employee time spent in dealing with them.

[FN66]. The Court also referred expressly to the academic debate surrounding the use of the metaphor of a real 'place' to describe cyberspace, although it declined to take a position on the matter.

[FN67]. See Fibbe, *supra* n 32.

[FN68]. See the Case Comment in 17 *Harv. J. L. & Tech.* 283, *supra* n 32, which, while welcoming the limitations on damage re-introduced by the *Intel* Court, also pointed out the difficulties with proving the requisite damage in factual situations of the sort in the case.

[FN69]. There are also state laws (statutes) dealing with similar acts; see Kerr, *supra* n 84.

[FN70]. Different countries may protect different aspects of computer-related crime, and either in the form of specific computer crime statutes or within more general criminal laws. Common law countries that have laws dealing with computer misuse and unauthorized access include the UK (the Computer Misuse Act of 1990), Australia (the Cybercrime Act of 2001), and Singapore (the Computer Misuse Act of 1993, as amended in 1998 and 2003.) For a fuller listing of countries and their computer crime legislation specifically dealing with unauthorized access, see Stein Schjolberg, 'The Legal Framework: Unauthorized Access to Computer Systems: Penal Legislation in 44 Countries', last updated August 2003 and available online at <http://www.mosstingrett.no/info/legal.html> (page last accessed August 6, 2005.)

[FN71]. There have been several US cases on this particular issue, though they have (to date) been concerned mostly with 'clickwraps' and 'shrinkwraps' (which term refers to contractual provisions found inside the physical packaging of CD-ROMS and software; such packaging is often wrapped in plastic material such that the terms cannot be viewed without breaking the wrapping and opening the packaging.) There has been one clear 'browsewrap' case where the validity of such contracts was actually in issue: *Specht v Netscape*, *supra* n 58, which held that an arbitration clause was not valid as it (and other contractual terms) could be viewed by the user only if she clicked on several consecutive hyperlinks that took her through different webpages. Contrasted with the ease by which she could download the software at issue (by simply clicking on a 'download' button displayed on the initial webpage), the court concluded that she could not be said to have manifested assent to the terms sought to be imposed on her. For further analysis and commentary on the question of assent and validity in electronic and online contracts, see the articles cited *supra* n 58. Post-*Specht* cases that touched on similar issues include *Pollstar v Gigamania Ltd*, 2000 WL 33 266437 (E. D. Cal. 2000) and *Softman Products Company v Adobe Software Systems Inc.*, 171 F Supp. 2d 1075 (C. D. Cal. 2001.)

[FN72]. F.3d 58 (1st Cir. 2003.)

[FN73]. 46 F.Supp.2d 444 (E.D. Va. 1998.)

[FN74]. 121 F.Supp. 2d 1255 (N.D. Iowa 2000.)

[FN75]. See the cases and commentary noted *supra*, n 58.

[FN76]. Although, to the extent that *Specht* and cases such as *ProCD v Zeidenberg* can be said to provide sufficient guidance on the direction of US law in this respect, US courts may have far less difficulty with this process than other common law jurisdictions, where this specific issue has either yet to arise to be decided judicially, or at best has been raised only sporadically.

[FN77]. For a history of the various major changes to the Act and their implications, see Reid Skibell, 'Cybercrimes and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act', 18 *Berkeley Tech. L. J.* 909 (2003.) It is beyond the scope of this paper to examine more general, albeit important, issues raised by cybercrime, e.g., the scope of what constitutes a cybercrime, the need for specific cybercrime laws to capture activities not otherwise covered by traditional criminal laws, and international and jurisdictional matters. On these issues, see, e.g., Marc D. Goodman and Susan W. Brenner, 'The Emerging Consensus on Criminal Conduct in Cyberspace', 2002 *UCLA J. L. & Tech.* 3, and Richard W. Downing, 'Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws To Combat Cybercrime', 43 *Colum. J. Transnat'l L.* 705 (2005.) Some commentators have noted the application by US courts of tort remedies to cybercrime (including trespass to chattel claims in the cases discussed in the main text), as an illustration of the necessity for and efficacy of private law enforcement in this area: Michael L. Rustad, 'Private Enforcement of Cybercrime on the Electronic Frontier', 11 *S. Cal. Interdisc. L.J.* 63 (2001.) This possibility has also been acknowledged specifically in the area of computer viruses: Robin A. Brooks, 'Deterring the Spread of Viruses Online: Can Tort Law Tighten the Net?', 17 *Rev. Litig.* 343 (1998.)

[FN78]. Although access 'without authorization' is not defined in the CFAA, 'exceeding authorized access' is defined as 'access[ing] a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter'. In this article, the term 'unauthorized access' is used generally to include both forms; where a distinction is necessary, each phrase will be used accordingly.

[FN79]. A 'protected computer' is defined as including a computer 'used in interstate or foreign commerce or communications, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States' (§ 1030(e)(2)(B.)) It is noteworthy also that the term 'computer' is fairly widely and exhaustively defined, as meaning 'an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device' (§ 1030(e)(1.))

[FN80]. Other additional offences include 'knowingly and with intent to defraud traffic[ing] (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization' where such trafficking affects interstate or foreign commerce or the computer concerned is used by the US Government (§ 1030(a)(6)), and 'transmit[ing] in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer' with an intention to extort (§ 1030(a)(7.))

[FN81]. § 1030(g.)

[FN82]. *ibid.* It should be noted that it is this subsection that clearly authorizes a person who suffers loss or damage because of any of the acts listed above to bring a civil action.

[FN83]. See, e.g., Patricia L. Bellia, 'Defending Cyberproperty', 79 *N. Y. U. L. Rev.* 2164 (2004), noting difficulties with adopting either property rules or liability rules as a basis for protection of cyberproperty, and that the choice between them is far more complex and involves perhaps some variant or 'hybrid' rules. See also McGowan, 'Website Access: The Case for Consent', *supra* n 59.

[FN84]. Orin S. Kerr, 'Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes', 78 *NYU L.R.* 1596 (2003.) For a list of countries with such laws, other than the US and as of 2002, see Schjolberg, *supra* n 70, and noted also in Kerr.

[FN85]. Bellia, *supra* n 83, and Kerr, *ibid.* Some of the cases, such as the AOL cases, *Explorica* and *Register.com*, have also been discussed in the main text, *supra*.

[FN86]. The Singapore Computer Misuse Act is included in this discussion for a number of reasons: (1) it is an early (1993) but often updated (most recently in 2003) example of a general computer misuse statute; (2) it resembles closely the UK Act, which as the main computer misuse law of a major common law jurisdiction provides a useful comparison to the US position; and (3) it also resembles (in some definitions and offences) the US CFAA. For example, the Singapore definition of a computer is 'an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include (a) an automated typewriter or typesetter; (b) a portable hand held calculator; (c) a similar device which is non-programmable or which does not contain any data storage facility; or (d) such other device as the Minister may, by notification in the *Gazette*, prescribe': Section 2(1), the Computer Misuse Act (Cap 50A, Singapore Statutes, 1998 Rev. Ed.)

[FN87]. The UK Act was passed in 1990, the original Singapore statute in 1993.

[FN88]. For a description of the history and scope of the SCMA, see Christopher Lee Gen-Min, 'Offences Created by the Computer Misuse Act 1993', [1994] *Sing. J. L. S.* 263.

[FN89]. Particularly as it relates only to accessing a program or data held in a computer. As explained *infra*, however, there ought in principle to be no reason why accessing program or data should be treated differently from accessing a computer, a network, a system or generally.

[FN90]. *Supra* n 84.

[FN91]. Both statutes also state expressly what securing access to such program or data means, *viz.*, 'a person secures access to any program or data held in a computer if by causing a computer to perform any function he (a) alters or erases the program or data; (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; (c) uses it; or (d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner), and references to access to a program or data (and to an intent to secure such access) shall be read accordingly': Section 2(2)

(SCMA) and Section 17(2) (UKCMA.)

[FN92]. [1999] 3 WLR 620.

[FN93]. For a case comment on *Allison*, see Kelly Stein, 'Unauthorised Access and the UK Computer Misuse Act 1990: The House of Lords Leaves No Room for Ambiguity', *C.T.L.R.* 2000, 6(3), 63-66 (2000.) For a case comment on *Bignell*, see Clive Gringras, 'To Be Great Is To Be Misunderstood: the Computer Misuse Act 1990', *C.T.L.R.* 1997, 3(5), 213-215 (1997.)

[FN94]. [1998] Cr.App.R. 1.

[FN95]. The lower court in *Allison*, being constrained by the earlier decision in *Bignell*, had read the UKCMA similarly, *viz.*, its purpose was to protect the integrity of computer systems where the integrity of data would be protected by the 1998 UK Data Protection Act.

[FN96]. [2001] SGDC 174.

[FN97]. On the facts, however, she found in favor of the accused as he lacked the requisite *mens rea* and it was also not clear that the purpose of accessing the database in question was such as to render him unauthorized to access it. The case concerned a junior police officer who accessed a police database at the request of a senior officer, who only informed the former that the data was wanted for personal reasons after the act of access had been performed. Although the accused had used a case number from one of his own investigations to access the database, which was technically forbidden, the court found that this was common practice amongst the officers, who were also accustomed to assisting each other with information and requests on investigations other than their own. The facts and result of *Loh Chai Huat* thus resemble those of *Bignell*, even adopting a wide reading of 'unauthorized access' as *per Allison*.

[FN98]. [2001] 2 SLR 342.

[FN99]. The Court also took into account the privacy policies and terms of service of several leading free web-based email service providers.

[FN100]. In particular, the statement that access means 'of the kind in question' and the legislative inclusion of definitions for 'unauthorised access' and 'securing access to a program or data held in a computer.'

[FN101]. See, e.g., Skibell, *supra* n 77, and Kerr, *supra* n 84.

[FN102]. Kerr, *ibid.*

[FN103]. Aaron Burstein, 'A Survey of Cybercrime in the United States', 18 *Berkeley Tech. L. J.* 313 (2003.)

[FN104]. e.g., access to a program or data held in a computer, modifying the contents of a computer (UKCMA and SCMA), interfering with or obstructing the lawful use of a computer or disclosing passwords or access codes (SCMA), § 1030(a)(6) (US CFAA.) It is difficult, however, to see what other 'trigger' or underlying general principle could have been used for computer misuse besides the fact of 'unauthorized access.' Perhaps the real problem is not what the 'trigger' is or how it is phrased, but rather how it is interpreted by the courts.

[FN105]. e.g., damage meaning 'impairment to a computer or the integrity or availability of data, a program or

system, or information' that, *inter alia*, causes physical injury or economic loss of a certain amount 'in value' (SCMA and CFAA.)

[FN106]. *AOL v NHCD*, *supra* n 72. See also the discussion in Kerr, *supra* n 84.

[FN107]. Kerr, *ibid*.

[FN108]. See discussion *supra*; see also Bellia, *supra* n 85, and Kerr, *ibid*.

[FN109]. *Ibid*.

[FN110]. In this respect, it is noteworthy that the UKCMA does not even have a definition of 'computer', unlike the US CFAA and the SCMA. In 2004, the All Party Internet Group (APIG) of the UK issued a report on the UKCMA, calling for certain updates and extensions to be made, particularly in light of the European Union Council Framework Decision on attacks against information systems in 2002 and the Convention on Cybercrime of 2004. Interestingly, adding a definition for 'computer' was not one of the recommendations. See <http://www.apig.org.uk> for a copy of the report (page last accessed August 10, 2005). Since this paper was completed, amendments to the UKCMA have been introduced into Parliament as part of the proposed Police and Justice Bill 2006, and are (as of June 2006) being debated in the House of Lords. The amendments include a very broad offence aimed at 'denial of service' attacks, which criminalizes any 'unauthorised act in relation to a computer', if done with the 'requisite intent and the requisite knowledge'.

[FN111]. Kerr, *supra* n 84.

[FN112]. See the articles noted *supra* n 32.  
15 Int'l J.L. & Info. Tech. 90

END OF DOCUMENT