Illegal Access to Information Systems in the Qatari Criminal Law: A Comparative Study

Dr. Sami Hamdan Al-Rawashdeh[*]

Abstract:

The illegal access to computer networks and information systems has become a widespread phenomenon in light of the tremendous development in the ICT sectors, which requires the implementation of criminal law rules to counter this emerging pattern of criminal activity. As a result, the United States, the United Kingdom and Qatar issued special criminal legislation to combat all forms of cybercrime, including the crime of illegal access of information systems. However, these statutes do not specifically provide definition of an "illegal access". The USA and UK judicial jurisprudence provide different and inconsistent interpretations in this regard.

This study aims at providing a comprehensive analysis of the concept of «illegal access to information systems», in both national and comparative laws, as well as the judiciary efforts in defining such crime. This study reveals that the legal provisions relating to illegal access to the information systems are ineffective and vague, and that their jurisprudence is contradictory and inconsistent. As a result, there is an urgent need for a model legislative regulation that addresses the provisions of this crime clearly.

The Qatari law and courts do not define "illegal access". The prohibition against unauthorized access to computers is new, and remains a mystery, vague and indistinct. Accordingly, there is a clear need to amend the Qatari Prevention of Cybercrimes Act 2014, in order to set up clear guidelines spelling out the meaning of "illegal access" so as to be relied upon by the judiciary.

Keywords:

Illegal Access, Information Systems, The Qatari Criminal Law, Comparative Law, Cybercrimes.

---

[*]**Associate Professor of Criminal Law, School of Law, University of Qatar**

1. Introduction:

"Hacking" is a form of cybercrime.(2) The offence described as "hacking" refers to unlawful access to a computer system, one of oldest computer-related crimes. Following the development of computer networks (especially the Internet), this crime has become a mass phenomenon. Examples of hacking offences include breaking the password of password-protected websites and circumventing password protection on a computer system. But acts related to the term "hacking" also include preparatory acts such as the use of faulty hardware or software implementation to illegally obtain a password to enter a computer system, setting up "spoofing" websites to make users disclose their passwords and installing hardware and software-based keylogging methods that record every keystroke, and consequently any passwords used on the computer and/or device. Many analysts recognize a rising number of attempts to illegally access computer systems, with over 250 million incidents recorded worldwide during the month of August 2007 alone.(3)

(2) The worst rift between Qatar and its closest allies for many years was precipitated by a series of cyber attacks that have been attributed to the United Arab Emirates. The attacks targeted the Qatar News Agency (QNA) Network, Qatar's state-owned media outlet. After apparently gaining access to the network in April this year, the hackers placed a fictitious report of the Emir of Qatar airing tensions with the U.S. president and praising Iran and the Palestinian militant group Hamas. On June 5, Saudi Arabia, the UAE, Bahrain and Egypt severed ties with and imposed a trade and diplomatic embargo on Qatar, accusing Doha of supporting terrorism. They presented Qatar with a list of 13 wide-ranging demands and gave it an ultimatum to comply with them or face unspecified consequences. Doha rejected the demands, which included shutting down the broadcaster Al Jazeera, removing Turkish troops from Qatar's soil, scaling back cooperation with Iran and ending ties with Egypt's Muslim Brotherhood movement. Qatar said that a U.S. media reports had shown that the United Arab Emirates was involved in an alleged hack of Qatar's state news agency in late May that helped spark a diplomatic crisis in the Gulf. The cyber security officials of Qatar have advised all government and private organizations to enhance their existing digital security standards to foil possible cyber-attacks. The Qatar crisis must recall the attention of political actors and civil societies of the urgent need to resume and finalize U.N. efforts to regulate state use of cyber-attacks. Without this regime, cyber-attacks will contribute to fueling a cyber arms race, posing serious risks of conflict escalation, putting cyber stability under pressure, and making international stability a chimera.

(3) The Online-Community Hacker Watch publishes reports about hacking attacks. Based on their =

"Originally, the term "hacker" has been used to define "any person who derives joy from discovering ways to circumvent limitations", or to describe the technologically-gifted inventor. Historically, hackers are not viewed upon as criminals, and their activity was described merely as "searching out information and wasting a lot of time". They find the weaknesses in security systems by evading detection when they can, and discovering information which is private and confidential to institutions and individuals. In that sense, they keep our instincts alert to the insecurities of the internet. Hacking has been described as an intellectual pursuit similar to solving "crossword puzzles". However, it is now accepted that hacking into computer networks is by definition "obtaining unauthorised access to a computer network, involves the use of a computer to obtain access to a computer system by means of keying in access codes and passwords without permission".(4)

The Digital Guards database defines hacking: "unauthorized use, or attempts to circumvent or bypass the security mechanisms of an information system or network".(5) Darlington believes hacking is not limited to accessing data or information but also includes an attack on the privacy of all people.(6)Almost all different opinions agree on the illegality of hacking.(7) Unauthorised access is a crime in which someone, usually knowledgeable and skilled in computer techniques, breaks into an information system, without authorization from the manager, in order to gain access (or control) to its functions (or data). (8)Three main factors have supported the increasing number of

= sources, more than 250 million incidents were reported in the month of August 2007. Source: http://www.hackerwatch.org.

(4) Natasha Jarvie, "Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1" 2003, 9(3), Computer and Telecommunications Law Review 76 at 78.

(5) Digital Guards database (2001), Glossary [online]. Available at http://www.digitalguards.com/Glossary.htm.

(6) Roger Darlington, "Crime on the net" (2001) [online]. Available at http://www.rogerdarlington.co.uk/crimeonthenet.html.

(7) Ahmad Nehaluddin, "Hackers' criminal behaviour and laws related to hacking" 2009, 15(7), Computer and Telecommunications Law Review 159.

(8) Pedro Miguel F. Freitas and Nuno Goncalves, "Illegal access to information systems and the =

hacking attacks: inadequate and incomplete protection of computer systems, development of software tools that automate the attacks, and the growing role of private computers as a target of hacking attacks.(9)

The issue of extending the criminal law to deter computer misuse has recently assumed prominence both in Qatar and overseas. In the late 1980s, several countries investigated the need for the creation of criminal offences specifically directed at computer misuse.(10) The types of computer misuse can be characterized as wrongdoing which directly, and to a serious degree, threatens the security or wellbeing of our society which is increasingly reliant on computers to process, record and transfer information for the purposes of both business and social services. There is a need to deter people who may otherwise be inclined to engage in computer misuse and to punish those who do. In that context we address the conduct which we believe should be encompassed within any criminal law dealing with computer misuse. This conduct is the unauthorised access /*accessing* of data stored in a computer. This is where a person without authority, whether through physical or electronic means, accesses data stored on a computer.

Hackers may gain access remotely, using a computer in his own home or office connected to a telecommunications network. The exploding

= Directive 2013/40/EU" 2015, Vol. 29, No. 1, International Review of Law, Computers & Technology 50–62 at 55.

(9) M. Gercke, UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES, March 2011, at 44-46, available at https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pd [Accessed 30/10/2017].

(10) The Scottish Law Commission (Report on Computer Misuse (Scot Law Com, No 106) 1987) the Attorney-General's Department of Australia (Review of Commonwealth Criminal Law: Interim Report, Computer Crime, November 1988) and the Law Commission of England and Wales (Criminal Law: Computer Misuse (Law Com. No 186) 1989) recommended the adoption of criminal offences directed at computer misuse. These recommendations prompted new legislation in the United Kingdom and Australia making computer misuse a criminal offence. Legislation has also been passed in Canada and Singapore relating to computer misuse (see Appendix A where this legislation is reproduced). Also, the South African Law Commission is currently considering issues in relation to computer related crime (see South African Law Commission, Computer Related Crime, Issue Paper 14, August 1998).

use of information systems and networks has caused countries to become increasingly interconnected. In developed countries, computer networks play a major role in how companies do business, how governments provide services to citizens and enterprises, and how people communicate and exchange information. By providing easy access to information and benefits, "e-government" improves services to citizens and reduces bureaucratic inefficiencies. As in more developed countries, computer networks hold the potential for economic growth and prosperity in developing countries as well. E-commerce increases productivity and allows access to markets in other countries like never before. Further, the Internet also holds out the promise of benefits that particularly may assist developing economies. Secure computer networks can improve infrastructure reliability, such as by enhancing transportation services and improving the consistent delivery of electricity and natural gas. Moreover, secure networks and favorable laws attract foreign investment in such industries as information processing and software development.

"Yet with this blossoming potential come new dangers. Criminals and terrorists have recognized the potential of the Internet and have exploited it. Hackers have broken into bank computers, transferred funds to their own accounts, and extorted the banks; criminals use computers and computer networks to make child pornography cheaply and easily and to distribute it over the Internet to pedophiles they may never meet in person; and terrorists and drug dealers use encrypted electronic communications to evade government surveillance. Indeed, even improvements of critical infrastructures through computerization have a dark side: insecure information networks make infrastructures vulnerable to the attacks of hackers and "malicious code" such as viruses and worms... The threat caused by these crimes is not limited, however, to the direct harms of the crimes themselves: all of the benefits of information networks are at risk if the networks are not safe

and secure".(11)

Natasha Jarvie has argued that: "Our society relies on a matrix of computer networks to ensure effective operation of numerous services. It is now recognised that hackers can cause massive disruption and can, in some circumstances, threaten the safety of the public, whether on purpose, or otherwise…The view of the hacker as a curious creature of exploration is rejected by law enforcement agencies in the US".(12) "The criminalization of illegal access is sometimes intended to act as a barrier to prevent the commission of more serious crimes. It acts as a very special type of crime that proves to be fundamental in fighting cybercrime. Unauthorized access to a specific information system often constitutes a predicate crime in the commission of other crimes related to information technology, such as illegal system interference, illegal data interference, and illegal interception".(13) Article 2 of the Convention on Cybercrime(14) has addressed explicitly this criminal

(11) Richard Downing, "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime" (2005) 43 Columbia Journal of Transnational Law 705 at 708-709.

(12) Natasha Jarvie, "Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1" 2003, 9(3), Computer and Telecommunications Law Review 76 at 78-79.

(13) Pedro Miguel F. Freitas and Nuno Goncalves, "Illegal access to information systems and the Directive 2013/40/EU" 2015, Vol. 29, No. 1, International Review of Law, Computers & Technology 50–62 at 55.

(14)The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime or the Budapest Convention, is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer states Canada, Japan, South Africa and the United States. The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004. As of December 2016, 52 states have ratified the convention, while a further four states had signed the convention but not ratified it. On 1 March 2006, the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are required to criminalize the dissemination of racist and xenophobic material through computer systems, as well as threats and insults motivated by racism or xenophobia. The Convention aims principally at:

1 - Harmonising the domestic criminal substantive law elements of offences and connected =

activity. It states “Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system”. This language provides an important standard by which to measure the comprehensiveness of a country’s basic hacking statute.

The USA federal government, all fifty states, and dozens of foreign countries have enacted computer crime statutes that prohibit “unauthorized access” to computers. No one knows what it means to “access” a computer, or when access becomes “unauthorized.” The few courts that have construed these terms have offered widely varying and inconsistent interpretations. This Article examines why the courts have construed these statutes in an overly broad manner that threatens to criminalize a surprising range of innocuous conduct involving computers. It presents a comprehensive analysis of the meaning of unauthorized

---

= provisions in the area of cyber-crime.

2 - Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form

3 - Setting up a fast and effective regime of international cooperation.

The following offences are defined by the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to copyright and neighbouring rights. It also sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. In addition, the Convention contains a provision on a specific type of trans border access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the Signatory Parties. The Convention is the product of four years of work by European and international experts. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence. Currently, cyber terrorism is also studied in the framework of the Convention.

access offence in the Qatari and comparative laws, and particularly the foundational concepts of "access" and "authorization." It reveals the ambiguities latent in unauthorized access statutes and shows how the courts have struggled to define "access" and "without authorization" in a coherent way. This paper asserts that the legal provisions relating to unauthorized access are currently inefficient, uncertain, and its judicial interpretation is inconsistent. Therefore, there is a pressing need for a better regulatory model. The Qatari law and courts do not define "illegal access". The prohibition against unauthorized access to computers is new, and remains a mystery, vague and indistinct. Accordingly, the Qatari law on cybercrime needs to adopt legal guidelines to help the Qatari courts to better interpret the meaning of unauthorized access.

This study proceeds in three main sections. The first section examines the criminal offence of illegal access according to the US Computer Fraud and abuse Act 1984, and the American judicial jurisprudence on "illegal access" definition. The second one deals with the United Kingdom Computer Misuse Act 1990 and the UK judicial interpretation in this regard. The last section is devoted to the Qatari Prevention of Cybercrimes Act No. 14 of 2014.

2. Unauthorized Access in the USA Law:

2.1. The US Computer Fraud and Abuse Act 1984:

In many situations, intrusions occur not as an end in themselves but as part of a larger criminal scheme. Criminals may, for example, hack into a computer in order to obtain information that they can use to commit some other crime, such as obtaining credit card or bank account numbers in order to make fraudulent purchases or to transfer funds fraudulently. Alternatively, they may use the computer's functions to further the offense, such as using a hacked computer as a storage site for images of child pornography. Some countries have created special statutes to criminalize computer intrusions where the hacker breaks into the computer to further a particular crime. The United States has taken

this approach by criminalizing the act of accessing a computer without authorization, or exceeding authorization, in furtherance of a crime of fraud.(15) A cybercrime statute needs not focus on particular crimes however, but rather can criminalize conduct where an unauthorized access was undertaken with the object of facilitating any crime or any of a broad class of crimes. For example, Australia has made it a crime to access a computer without authorization with the intent to commit a "serious offense" which means an offence that is punishable by imprisonment for life or a period of 5 or more years.(16)

The US Computer Fraud and Abuse Act (CFAA) first passed in 1984, and it is the main federal statute dealing with various aspects of computer crime. It has been amended several times since 1984. The most significant amendments took place in 1986 and 1996.(17) The Statute is 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. Various subsections, in the statute, utilize and distinguish between differing aspects of ‹unauthorized access› as acts of access either "without authorization" or of "exceeding authorized access". 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 accessory is not entitled so to obtain or alter". Moreover, different subsections seem to underscore a potentially significant distinction between doing an act 'intentionally' and doing it 'knowingly'.

(15) Computer Fraud and Abuse Act, 18 U.S.C. §1030(a) (4).

(16) Australia Criminal Code No. 12 of 1995, Part. 10.7, Division. 477.1, available at https://www.legislation.gov.au/Details/C2005C00524.

(17) 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.)

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' where the conduct involved an interstate or foreign communication, is an offence under § 1030(a) (2) (A), (B) and (C) respectively. § 1030(e) (1) defines a 'protected computer' 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'. 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. (18)

"A computer intrusion, also called a "hack," occurs when an individual trespass into a computer or part of a computer system to which that person is not entitled to have access. Such intruders may be divided into two categories: persons who attack from outside the network and wrongfully access a computer "without authorization," and persons who are insiders and thus have authorization to access specific portions of the network but intrude into other parts of it by "exceeding authorized access." Prohibiting computer intrusions is the heart of any network crimes law".(19)

"Although hackers have developed thousands of ways to gain access to a computer system "without authorization," a typical attack by an outsider might occur in the following way: (1) a hacker locates a victim computer system by scanning the Internet and finding a hole in the security of a computer; (2) the hacker runs a specialized software program, also known as an "exploit," tricking the computer into giving him access to it as if he were an authorized user; (3) the hacker runs a second specialized program and gains "root level" access, also known as "superuser" status, giving him complete control over the computer; (4) the hacker reads email or other files, deletes files, causes the system

(18) Mary W.S. Wong, "Cyber-trespass and «unauthorized access» as legal mechanisms of access control: lessons from the US experience", 2007, 15(1) International Journal of Law & Information Technology 90-128 at 116.

(19) Richard Downing, "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime" (2005) 43 Columbia Journal of Transnational Law 705 at 720.

to crash, stores his own files on the system, or uses it as the launching point for further hacking activities; (5) the hacker may then alter logging or accounting systems to make it appear that he has not used the system, and he may change these monitoring programs so that they do not record his presence if he uses the computer in the future; and (6) the hacker installs a "back door" or a specialized program that will allow him quick, root level access if he returns, even if the computer's owner patches the security vulnerability that he initially exploited". (20)

"Obtaining access to a computer by "exceeding authorized access," on the other hand, refers to the activities of "insiders"- persons who, by employment or some other relationship, have authority to access certain areas of a network, but who then use that authorized access to obtain privileges beyond those to which they are entitled". Cybercrimes statutes "may use the phrases «accessing a computer without authorization» and «exceeding authorized access» to treat insiders and outsiders differently. Some network crimes laws do not make this distinction, however, and treat all hackers the same". Some of the other phrases commonly used to describe a hacker›s lack of authority to have access to a computer include: «illegal access,» «access without right,» «access without color of law,» «fraudulently obtaining or maintaining access,» and «unlawfully intruding into a computer.» Determining which of these formulations is appropriate for a particular legal system may depend on the meaning of these words in related laws, how the network crimes law defines them, and the way in which a court of that country is likely to interpret them. Framing the element of the crime in terms of «authorization,» however, may provide the clearest definition and create the least risk of error in interpretation".(21)

(20) Richard Downing, "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime" (2005) 43 Columbia Journal of Transnational Law 705 at 721.

(21) Richard Downing, "Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime" (2005) 43 Columbia Journal of Transnational Law 705 at 721-722.

Like his US federal counterpart, the UK computer misuse statute also reveal a property-based notion of computer crime, as well as a lack of clarity or definition as to the concept of 'unauthorized access. 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". Section 3 of the Singapore Computer Misuse Act 1993 (SCMA)(22) 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.(23)

There are interesting minor variations in language and, possibly, consequential scope, between the two sections. 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. Another difference in the 'unauthorized access' sections of both statutes is the placement of the knowledge 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

(22) In 1993, Singapore passed the Computer Misuse Act (Chapter 50A of the Singapore Statutes), which it has amended many times, and more recently in 2017. The amendments to the Computer Misuse and Cybersecurity Act (CMCA), which were passed in Parliament on 3 April 2017, will take effect from 1 June 2017. These amendments will tackle the increasing scale and transnational nature of cybercrime, as well as the evolving tactics of cybercriminals.

(23) 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] Singj L. S. 263.

as though there is a higher standard for knowledge under the SCMA compared to the UKCMA.(24)

2.2 USA Judicial Interpretations of Unauthorised Access:

2.2.1 Judicial Interpretations of Access

In the *State v. Allen*,(25) the defendant had used his computer, equipped with a modem, to call various modems of the corporate computer owner, using random dialing. Allen was charged with accessing the Bell computer without authorization in violation of the Kansas computer crime statute. The State presented no evidence that defendant had ever entered any computer system of the corporate computer owner. The trial court dismissed the complaint after finding no probable cause existed to believe defendant had committed any crime. Before the Kansas Supreme Court, Allen argued that there was no evidence he had actually accessed the Bell computer. The government relied on the broad statutory definition of access, fairly common among early state computer crime statutes, which stated that access means "to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer. The Kansas Supreme Court held that:

> The problem with the State's analysis is that K.S.A. 21-3755(b)(1) does not criminalize "accessing" (and, thus, "approaching") but rather "gaining or attempting to gain access." If we were to read "access" in this context as the equivalent of "approach," the statute would criminalize the behavior of "attempting to gain approach" to a computer or computer system. This phrase is lacking in any common meaning such that an ordinary person would have great difficulty discerning what conduct was

(24) Mary W.S. Wong, "Cyber-trespass and «unauthorized access» as legal mechanisms of access control: lessons from the US experience", 2007, 15(1) International Journal of Law & Information Technology 90-128 at 11118-119.

(25) 260 Kan. 107; 917 P.2d 848; 1996 Kan. LEXIS 82.

> prohibited, leading to an effective argument that the statute was void for vagueness. The United States Department of Justice has commented about the use of "approach" in a definition of "access" in this context: "The use of the word 'approach' in the definition of 'access,' if taken literally, could mean that any unauthorized physical proximity to a computer could constitute a crime." We read certain conduct as outside a statute's scope rather than as proscribed by the statute if including it within the statute would render the statute unconstitutionally vague. Consequently, although K.S.A. 21-3755 defines "access," the plain and ordinary meaning should apply rather than a tortured translation of the definition that is provided. In addition, K.S.A. 21-3755 is certainly rendered ambiguous by the inclusion of the definition of "access" as a verb when its only use in the statute is as a noun. As criminal statute, any ambiguity is to be resolved in favor of the accused. Webster's defines "access" as "freedom or ability to obtain or make use of. This is similar to the construction used by the trial court to find that no evidence showed that Allen had gained access to Southwestern Bell's computers. Until Allen proceeded beyond the initial banner and entered appropriate passwords, he could not be said to have had the ability to make use of Southwestern Bell's computers or obtain anything. Therefore, he cannot be said to have gained access to Southwestern Bell's computer systems as gaining access is commonly understood. The trial court did not err in determining the State had failed to present evidence showing probable cause that Allen had gained access to Southwestern Bell's computer system.(26)

A federal district court suggested a similar approach in *Moulton v. VC3,*(27) a civil dispute between two computer security companies. *The Moulton* case harnessed a civil remedy added to the federal computer

(26) 917 P.2d 848 at 852-853.

(27) No. 1:OOCV 434-TWT, 2000 WL 33310901 (N.D. Ga. Nov. 7, 2000).

crime statute in 1994 to provide additional protection for computer misuse victims. One company sued the second when an employee of the second company performed a "port scan" on the first company's computers. A port scan is a common network security test that sends a query to each open port on the target computer to see if that port is open and ready to receive incoming traffic. A port is a sort of electronic door, and an open port is akin to an open door and therefore a possible security vulnerability. When scanned, an open port will return a message to the requesting computer instructing it that it is open; a closed port will return an error message. Consistent with *Allen,* the *Moulton* court concluded without analysis that the second company's port scan did not access the first company's computer.

While both *Moulton* and *Allen* suggest that accessing a computer is limited to uses that in a virtual sense get "inside" the computer, two other opinions have adopted a significantly broader approach.(28) In *State v. Riley*, (29)Joseph Riley was convicted of three counts of computer trespass and four counts of possession of a stolen access device after he used his home computer to obtain long distance telephone access codes from telephone company computers. On appeal, Riley contends that his convictions of computer trespass against Telco must be reversed because his conduct, repeatedly dialing Telco's general access number and entering random 6- digit numbers in an attempt to discover access codes belonging to others, does not satisfy the statutory definition of computer trespass. He argues that acts accomplished by simply dialing the telephone are not encompassed within the statutorily defined crime of computer trespass and are merely the equivalent of placing a telephone call. He contends he is not guilty of computer trespass because he did not enter, read, insert, or copy data from the telephone system's computer switch. Instead, he argues, RCW

(28) ORIN S. KERR, "CYBERCRIME›S SCOPE: INTERPRETING «ACCESS» AND «AUTHORIZATION» IN COMPUTER MISUSE STATUTES" [2003] 78 New York University Law Review 1596 at 1626.

(29) Supreme Court of Washington, En. Banc. March 4, 1993,121 Wash.2d 22846 P.2d 1365.

9.26A.110, dealing with telephone fraud, is more appropriately applied. The Washington statute contained a definition of "access" essentially identical to that in the Kansas statute from Allen. The Court rejected the appellant argument and held that:

> Riley's acts were not equivalent to placing a telephone call. He used his home computer to dial Telco's general access number and enter random 6–digit numbers representing customer access codes every 40 seconds for several hours at a time. Moreover, RCW 9A.52.110 criminalizes the unauthorized, intentional "access" of a computer system. The term "access" is defined under RCW 9A.52.010(6) as "to approach ... or otherwise make use of any resources of a computer, directly or by electronic means." Riley's repeated attempts to discover access codes by sequentially entering random 6–digit numbers constitute "approach[ing]" or "otherwise mak[ing] use of any resources of a computer". The switch is a computer. Long distance calls are processed through the switch. Riley was approaching the switch each time he entered the general access number, followed by a random 6–digit number representing a customer access code, and a destination number. Therefore, Riley's conduct satisfied the statutory definition of "access" and so was properly treated as computer trespass.(30)

It is possible to interpret the difference between *Allen* and *Riley.* In *Allen,* the court viewed computers as virtual spaces, and accessing the computer as akin to getting inside the space. Although the *Riley* court does not make its standard clear, it appeared to see computers more as physical machines, and accessing the computer as sending a communication to that machine. As a result, the conduct that did not constitute access in *Allen* did so in *Riley.*(31)

(30) Supreme Court of Washington, En. Banc. March 4, 1993,121 Wash.2d 22846 P.2d 1365 at 1373.

(31) ORIN S. KERR, "CYBERCRIME›S SCOPE: INTERPRETING «ACCESS» AND «AUTHORIZATION» IN COMPUTER MISUSE STATUTES" [2003] 78 New York University Law Review 1596 at 1627.

An even broader interpretation of access appears in a civil decision, *America Online, Inc. v. National Health Care Discount, Inc*(32). In this dispute, Internet service provider (ISP) brought action against Iowa Corporation engaged in selling discount optical and dental service plans, alleging that corporation hired e-mailers to send unauthorized and unsolicited bulk e-mail advertisements to ISP's customers, in violation of state and federal law. AOL argues the evidence in this case is sufficient to establish NHCD's liability to AOL under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 *et seq.* Specifically, AOL argues NHCD violated 18 U.S.C. §§ 1030(a)(5) and (a)(2)(C). The court has considered whether NHCD's contract e-mailers intentionally accessed AOL's computers. The court answered in the affirmative, offering an expansive interpretation of "access":

> The CFAA does not define "access," but the general definition of the word, as a transitive verb, is to "gain access to." As a noun, "access," in this context, means to exercise the "freedom or ability to ... make use of" something. The question here, therefore, is whether NHCD's e-mailers, by harvesting e-mail addresses of AOL members and then sending the members UBE messages, exercised the freedom or ability to make use of AOL's computers. The court finds they did. For 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. This is precisely what NHCD's e-mailers did with respect to AOL's computers.(33)

"Although the *NHCD* court relied on the same dictionary definition of "access" as had the *Allen* court, the court in *NHCD* reached a quite different interpretation of its meaning. To the *NHCD* court, access is

(32) United States District Court, N.D. Iowa, Western Division. September 29, 2000, 121 F.Supp.2d 1255.

(33) United States District Court, N.D. Iowa, Western Division. September 29, 2000, 121 F.Supp.2d 1255 at 1272-1273.

a physical world concept, not a virtual world concept: The question is not whether the sender of the communication gains a virtual entrance into the computer from the sender's standpoint, but whether the communication itself is transmitted through the computer. As a result, sending an e-mail through a computer accesses the computer even if a user might not perceive the interaction as an access. Despite the common term, and even common statutory and dictionary definitions, the few courts to have interpreted access have reached inconsistent conclusions".(34)

2.2.2 Judicial Interpretations of Authorization:

In USA, Courts have faced even greater difficulties trying to interpret the meaning of authorization. (35) The earliest significant case interpreting authorization is the Second Circuit's opinion in *United States v. Morris*(36), sometimes known as the Internet worm case. The facts of this case are as follows: in the fall of 1988, Morris was a first-year graduate student in Cornell University's computer science Ph.D. program. Through undergraduate work at Harvard and in various jobs he had acquired significant computer experience and expertise. When Morris entered Cornell, he was given an account on the computer at the Computer Science Division. This account gave him explicit authorization to use computers at Cornell. Morris engaged in various discussions with fellow graduate students about the security of computer networks and his ability to penetrate it. In October 1988, Morris began work on a computer program, later known as the INTERNET "worm" or "virus." The goal of this program was to demonstrate the inadequacies of current security measures on computer networks by exploiting the

(34) ORIN S. KERR, "CYBERCRIME›S SCOPE: INTERPRETING «ACCESS» AND «AUTHORIZATION» IN COMPUTER MISUSE STATUTES" [2003] 78 New York University Law Review 1596 at 1628.

(35) ORIN S. KERR, "CYBERCRIME›S SCOPE: INTERPRETING «ACCESS» AND «AUTHORIZATION» IN COMPUTER MISUSE STATUTES" [2003] 78 New York University Law Review 1596 at 1628

(36) United States Court of Appeals, Second Circuit. March 7, 1991, 928 F.2d 504.

security defects that Morris had discovered. The tactic he selected was release of a worm into network computers. On November 2, 1988, Morris released the worm from a computer at the Massachusetts Institute of Technology. MIT was selected to disguise the fact that the worm came from Morris at Cornell. Morris soon discovered that the worm was replicating and reinfecting machines at a much faster rate than he had anticipated. Ultimately, many machines at locations around the country either crashed or became "catatonic." When Morris realized what was happening, he contacted a friend at Harvard to discuss a solution. Eventually, they sent an anonymous message from Harvard over the network, instructing programmers how to kill the worm and prevent reinfection. However, because the network route was clogged, this message did not get through until it was too late. Computers were affected at numerous installations, including leading universities, military sites, and medical research facilities. Morris was found guilty, following a jury trial, of violating 18 U.S.C. § 1030(a)(5)(A). He was sentenced to three years of probation, 400 hours of community service, a fine of $10,050, and the costs of his supervision.

He appealed his conviction and argued the government had to prove not only that he intended the unauthorized access of a federal interest computer, but that he also intended to prevent others from using it. The court found that the mental state requirement of the statute was enacted to proscribe intentional acts of unauthorized access. In comparing the statute to its predecessor, the court concluded the "intentionally" standard only applied to the access and not to the damages phrase of the statute. Defendant argued his conduct constituted at most "exceeding authorized access" rather than "unauthorized access," because he was authorized to communicate with other computers and to send electronic mail. The court found the evidence was sufficient for the jury to determine defendant's action fell within the area of unauthorized use. It also found that the worm was designed to invade computers at which he had no authority, express or implied, and the

decision was affirmed. The Court held that:

Congress was not drawing a bright line between those who have some access to any federal interest computer and those who have none. Congress contemplated that individuals with access to some federal interest computers would be subject to liability under the computer fraud provisions for gaining unauthorized access to other federal interest computers. The evidence permitted the jury to conclude that Morris's use of the SEND MAIL and finger demon features constituted access without authorization. While a case might arise where the use of SEND MAIL or finger demon falls within a nebulous area in which the line between accessing without authorization and exceeding authorized access may not be clear, Morris's conduct here falls well within the area of unauthorized access. Morris did not use either of those features in any way related to their intended function. He did not send or read mail nor discover information about other users; instead he found holes in both programs that permitted him a special and unauthorized access route into other computers…Morris also contends that the District Court should have instructed the jury on his theory that he was only exceeding authorized access. The District Court decided that it was unnecessary to provide the jury with a definition of "authorization." We agree. Since the word is of common usage, without any technical or ambiguous meaning, the Court was not obliged to instruct the jury on its meaning. An instruction on "exceeding authorized access" would have risked misleading the jury into thinking that Morris could not be convicted if some of his conduct could be viewed as falling within this description. Yet, even if that phrase might have applied to some of his conduct, he could nonetheless be found liable for doing what the statute prohibited, gaining access where he was unauthorized and causing loss.(37)

Several cases have examined the meaning of authorization in the context of employee misconduct. The most remarkable of these

(37) 928 F.2d 504 at 510-511.

cases is *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*[38] Shurgard Storage Centers, Inc. (plaintiff) and Safeguard Self Storage, Inc. (defendant) are competitors in the self-storage business. The plaintiff alleges that the defendant embarked on a systematic scheme to hire away key employees from the plaintiff for the purpose of obtaining the plaintiff's trade secrets. The plaintiff also alleges that some of these employees, while still working for the plaintiff, used the plaintiff's computers to send trade secrets to the defendant via e-mail. The plaintiff's complaint alleges misappropriation of trade secrets, conversion, unfair competition, violations of the Computer Fraud and Abuse Act (CFAA), tortious interference with a business expectancy, and seeks injunctive relief and damages. The defendant has moved to dismiss the CFAA claim pursuant to Fed.R.Civ.P. 12(b)(6), docket no. 7 no. 7. The Court now DENIES the defendant's motion to dismiss the CFAA claim for the reasons set forth in this order. The District Court held that for purposes of stating claim under CFAA, former employees lost access to computers when they allegedly became agents of competitor. The court adopted the plaintiff's theory of authorization, which was that "the authorization for its...employees ended when the employees began acting as agents for the defendant.' The court found its guidance in the Restatement (Second) of Agency: "Unless otherwise agreed, the authority of an agent terminates, if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal." 'Applying this standard, the court concluded that the defendant's employees "lost their authorization and were 'without authorization' when they allegedly obtained and sent the proprietary information to the defendant via e-mail.'[39] "*Shurgard's* agency theory of authorization is strikingly broad. Under *Shurgard,* whenever an employee uses a computer for reasons contrary to an employer's interest, the employee does not act as the employer's

(38) United States District Court, W.D. Washington, at Seattle. October 30, 2000, 119 F.Supp.2d 1121.

(39) 119 F.Supp.2d 1121 at 1124.

agent and therefore is accessing the employer's computers. Motive determines whether access is authorized or unauthorized. Given that the federal computer crime statute uses access without authorization as the trigger for often-serious criminal liability, the apparent effect of *Shurgard* is to criminalize an employee's use of an employer's computer for anything other than work-related activities".(40)

Courts have adopted slightly narrower interpretations of unauthorized access in criminal employee misconduct cases. In *United States v. Czubinski*,(41) the defendant Czubinski was employed as a Contact Representative in the Boston office of the Taxpayer Services Division of the Internal Revenue Service ("IRS"). To perform his official duties, which mainly involved answering questions from taxpayers regarding their returns, Czubinski routinely accessed information from one of the IRS's computer systems known as the Integrated Data Retrieval System ("IDRS"). Using a valid password given to Contact Representatives, certain search codes, and taxpayer social security numbers, Czubinski was able to retrieve, to his terminal screen in Boston, income tax return information regarding virtually any taxpayer information that is permanently stored in the IDRS "master file" located in Martinsburg, West Virginia. In the period of Czubinski's employ, IRS rules plainly stated that employees with passwords and access codes were not permitted to access files on IDRS outside of the course of their official duties. In 1992, Czubinski carried out numerous unauthorized searches of IDRS files. He knowingly disregarded IRS rules by looking at confidential information obtained by performing computer searches that were outside of the scope of his duties as a Contact Representative. Defendant was convicted of wire fraud and computer fraud by the United States District Court for the District of Massachusetts. Defendant appealed. The Court of Appeals held that

(40)ORIN S. KERR, "CYBERCRIME›S SCOPE: INTERPRETING «ACCESS» AND «AUTHORIZATION» IN COMPUTER MISUSE STATUTES" [2003] 78 New York University Law Review 1596 at 1633-1634.

(41) United States Court of Appeals, First Circuit. February 21, 1997, 106 F.3d 1069.

interstate transmission element of wire fraud could be inferred from circumstantial evidence that defendant's searches of master taxpayer files caused information to be sent to his computer terminal in different state. Defendant's unauthorized browsing of confidential taxpayer information did not defraud Internal Revenue Service (IRS) of its property within meaning of wire fraud statute. Defendant's unauthorized browsing of confidential taxpayer information did not deprive taxpayers of their intangible, nonproperty right to honest government services; and defendant could not be convicted of computer fraud in connection with his browsing of confidential taxpayer files. The Court held that:

We have never before addressed section 1030(a)(4). Czubinski unquestionably exceeded authorized access to a Federal interest computer. On appeal he argues that he did not obtain "anything of value." We agree, finding that his searches of taxpayer return information did not satisfy the statutory requirement that he obtain "anything of value." The value of information is relative to one's needs and objectives; here, the government had to show that the information was valuable to Czubinski in light of a fraudulent scheme. The government failed, however, to prove that Czubinski intended anything more than to satisfy idle curiosity. The plain language of section 1030(a)(4) emphasizes that more than mere unauthorized use is required: the "thing obtained" may not merely be the unauthorized use. It is the showing of some additional end—to which the unauthorized access is a means—that is lacking here. The evidence did not show that Czubinski's end was anything more than to satisfy his curiosity by viewing information about friends, acquaintances, and political rivals. No evidence suggests that he printed out, recorded, or used the information he browsed. No rational jury could conclude beyond a reasonable doubt that Czubinski intended to use or disclose that information, and merely viewing information cannot be deemed the same as obtaining something of value for the purposes of this statute.(42)

(42) 1997, 106 F.3d 1069 at 1078.

This "language in *Czubinski* suggests that employers have a right to limit their employees' use of company computers to work solely motivated by a desire to serve the company. Czubinski had exceeded his authorized access by accessing the IRS computers for personal reasons when employees were allowed to access the computer only for official reasons".(43)

A Georgia state court applied a similar approach in *Fugarino v. State.*(44) The defendant, a computer programmer was convicted in the Superior Court, Gwinnett County of computer trespass in connection with deletion of code from his employer's computer system. On appeal following his conviction, the Court of Appeals held that testimony showed that Fugarino used a computer owned by the company with the intention of deleting or removing data from that computer. The burden on the State was not to show that Fugarino had completed the act of deleting or removing data from his computer but to show that he had used a computer, knowing that he did not have the authority to do so, with the intention of deleting data. There is sufficient evidence in this case to allow a reasonable trier of fact to find that a computer trespass had occurred. The term "without authority" is defined by the legislature in OCGA § 16-9-92(11) as "the use of a computer or computer network in a manner that exceeds any right or permission granted by the owner of the computer or computer network." The owner of the company testified that he did not give Fugarino authority or permission to delete portions of the company's program. Moreover, the vindictive and retaliatory manner in which Fugarino deleted large amounts of computer code indicates that he knew he lacked authority to do so. Therefore, there was sufficient evidence to allow a rational trier of fact to conclude beyond a reasonable doubt that Fugarino used a computer, owned by his employer, with knowledge that such use was without authority and

(43) ORIN S. KERR, "CYBERCRIME›S SCOPE: INTERPRETING «ACCESS» AND «AUTHORIZATION» IN COMPUTER MISUSE STATUTES" [2003] 78 New York University Law Review 1596 at 1634.

(44) Court of Appeals of Georgia. March 14, 2000, 531 S.E.2d 187.

with the intention of removing programs or data from that computer.(45)

State v. Olson(46) case reveals a roughly similar approach, albeit one that led to a reversal of the defendant's conviction. Laurence Olson was a police officer who used a police computer database to access and print out driver's license photographs of female college students who attended the nearby University of Washington. Olson was tried and convicted of accessing a government computer without authorization in violation of Washington's computer trespass statute. On appeal, he argued that his access was not explicitly unauthorized. The court evaluated Olson's claim by examining the workplace rules that governed Olson's conduct. The court concluded that while "the evidence shows that certain uses of retrieved data were against departmental policy, it did not show that permission to access the computer was conditioned on the uses made of the data. The court reversed the conviction.

Such approach was rejected by the Court of Appeals of Maryland in *Briggs v. State*.(47) In November, 1994, the Scarborough Group, Inc. (Scarborough), a medium-sized securities investment company, hired Terry Briggs as a computer programmer and system administrator. Briggs, a twenty-three-year old computer specialist, was hired to program and design software to maintain the company computer system. As part of his job responsibilities, he entered data in the computer system and placed passwords on the files to secure the data. The management of the entire computer system was entrusted to Briggs. Following a dispute on July 24, 1995, about the terms of his employment contract, Briggs resigned as an employee of the company. Shortly after Briggs left the company, Scarborough realized that some of its computer files were secured with passwords known only to Briggs. Scarborough and Briggs were unable to resolve the situation. Scarborough filed a civil suit against Briggs, and also contacted the Anne Arundel County

(45) 531 S.E.2d 187 at 189.

(46) Court of Appeals of Washington, Division 1. April 29, 1987, 735 P.2d 1362

(47) Court of Appeals of Maryland. January 22, 1998, 704 A.2d 904.

police. The State charged Briggs in a two-count criminal information: count one, theft of computers, in violation of Article 27, § 342(a)(1) and, count two, unauthorized access to computers, in violation of Article 27, § 146(c)(2). At trial, Scarborough contended that Briggs changed the passwords two days before the meeting about Briggs's employment contract, and put them in a subdirectory named "ha-ha he-he," dated July 22, 1995 by the computer. Scarborough maintained that Briggs never had permission to place the company files in a directory and to protect the file with passwords, without anyone else in the company having access to the passwords. Although he denied any knowledge about "ha-ha he-he," Briggs admitted that he placed passwords on company files months earlier as part of his job in securing files, but that he had difficulty remembering the passwords because so much time had passed.

The trial court denied Briggs's motion for judgment of acquittal, and the jury found Briggs guilty of unauthorized access to computers in violation of Article 27, § 146(c)(2)(i). On Appeal, the Court of Appeal held that Employee had "authorization" to access his employer's computers, and thus employee did not commit offense of unauthorized access to computers by securing files with passwords known only to employee, even if employee exceeded scope of his authority in doing so. The employee had authority to enter data into computer and to place passwords on files to secure data. Briggs's access was not unauthorized under Article 27, § 146, the unauthorized access to computers statute. If the law is to be broadened to include Briggs's conduct, it should be modified by the Legislature, not by this Court.

In the set of cases interpreting authorization involving contracts governing the use of computers, the American courts held that the breach of contract make the access unauthorized where two parties are bound by a contract that implicitly or explicitly regulates access to a computer, and one side uses the computer in a way that arguably breaches the

contract. In *EF Cultural Travel BV v. Explorica, Inc*,[48] tour company sued competitor and individual executives of competitor, alleging that competitor's use of "scraper" software program to systematically glean company's prices from its website violated Computer Fraud and Abuse Act (CFAA), Copyright Act, and Racketeer Influenced and Corrupt Organizations Act (RICO). Company moved for preliminary injunction on CFAA claim. The United States District Court for the District of Massachusetts granted injunction, and competitor appealed. The Court of Appeals held that Competitor's use of "scraper" computer software program to systematically and rapidly glean prices from tour company's website, in order to allow systematic undercutting of those prices, "exceeded authorized access" within meaning of Computer Fraud and Abuse Act (CFAA), as required to support company's civil enforcement action against competitor and its executives, assuming program's speed and efficiency depended on competitor's executive's breach of broad confidentiality agreement with company, his former employer.

The American courts adopted the same approach in *America Online v. LCGM, Inc.*[49] In this case, Internet service provider brought action against operators of web sites, and principals of those operators, alleging that defendants sent unauthorized and unsolicited bulk e-mail advertisements to provider's customers, in violation of state and federal law. On provider's motion for summary judgment, it was held that the facts before the Court establish that defendants violated 18 U.S.C. § 1030(a)(2)(C) of the Computer Fraud and Abuse Act, which prohibits individuals from "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] information from any protected computer if the conduct involved an interstate or foreign communication." Defendants' own admissions satisfy the Act's requirements. Defendants have admitted to maintaining an AOL membership and using that membership to

(48) 274 F.3d 577 (1st Cir. 2001).
(49) 46 F. Supp. 2d 444 (E.D. Va. 1998).

harvest the e-mail addresses of AOL members. Defendants have stated that they acquired these e-mail addresses by using extractor software programs. Defendants' actions violated AOL's Terms of Service, and as such were unauthorized.

In *Register.corn v. Verio*,(50)plaintiff Register.com, a registrar of Internet domain names, moves for a preliminary injunction against the defendant, Verio, Inc. ("Verio"), a provider of Internet services. Register.com relies on claims under Section 43(a) of the Lanham Act, 15 U.S.C. § 1125(a); the Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030, as amended; as well as trespass to chattels and breach of contract under the common law of the State of New York. In essence Register.com seeks an injunction barring Verio from using automated software processes to access and collect the registrant contact information contained in its WHOIS database and from using any of that information, however accessed, for mass marketing purposes. The District Court held that:

> The issue of the scope of Verio's authorization to access the WHOIS database is also central to the Court's analysis of Register.com's claims that Verio is violating two discrete provisions of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. Register.com claims both that the use of software robots to harvest customer information from its WHOIS database in violation of its terms of use violates 18 U.S.C. §§ 1030(a)(2)(C) and (a)(5)(C), and that using the harvested information in violation of Register.com's policy forbidding the use of WHOIS data for marketing also violates those sections. That is, that both Verio's method of accessing the WHOIS data and Verio's end uses of the data violate the CFAA. Both §§ 1030(a)(2)(C) and (a)(5)(C) require that the plaintiff prove that the defendant's access to its computer system was unauthorized, or in the case of § 1030(a)(2)(C) that it was unauthorized or exceeded authorized access. However, although each section requires

(50) 126 F. Supp. 2d 238 (S.D.N.Y. 2000).

proof of some degree of unauthorized access, each addresses a different type of harm. Section 1030(a)(2)(C) requires Register.com to prove that Verio intentionally accessed its computers without authorization *and thereby obtained information.* Section 1030(a)(5)(C) requires Register.com to show that Verio intentionally accessed its computer without authorization *and thereby caused damage…* because Register.com objects to Verio's use of search robots they represent an unauthorized access to the WHOIS database.(51)

3. Unauthorized Access in the UK Law:

3.1 The Computer Misuse Act 1990:

The Computer Misuse Act 1990 ("the Act") was introduced primarily to deal with traditional "hacking" offences, for example unauthorized access to a computer. It was amended by the Police and Justice Act 2006 to tackle the then new and growing internet based problem of "denial-of-service" attacks. In the same year, the Fraud Act 2006 was enacted to improving the ease with which on-line fraud could be prosecuted. Today, most on-line frauds (such as on-line /internet banking fraud, i.e. fraudulent withdrawals from internet bank accounts using stolen identities) are prosecuted under the Fraud Act, and Computer Misuse Act offences are used for "pure" hacking or denial-of-service prosecutions. All the aforementioned examples of offences form part of what is colloquially termed "cybercrime" or occasionally "e-crime". There are essentially three main offences created by the Act, namely unauthorised access to a computer, unauthorised access with intent to commit another offence, and doing an act intending to impair the operation of a computer. A new s.3A introduces offences of making, supplying or obtaining any article for use in offences under sections 1-3. The first offence, which created by section 1, is that of causing a computer to perform any function with intent to access any program or data, knowing that such access is unauthorised. Examples of acts that would constitute a section 1 offence include using another

(51) 126 F. Supp. 2d 238 at 251.

person's identifier (ID) and /or password without proper authority in order to access data or a program; displaying data from a computer to a screen or printer; or even simply switching on a computer without proper authority.

Section 1 can be regarded as the basic offence and is frequently the precursor to the commission of other, more serious offences. The offence is complete once a defendant has caused a computer, which would include his own computer, to perform a function with intent to secure access, whether such access is actually secured or not is irrelevant.

The intent under section 1 of the CMA need not be directed at:

1. Any particular program or data;
2. A program or data of any particular kind; or
3. A program or data held in any particular computer.

The concept of authorisation is key to understanding the act. The convention on cybercrime uses the concept of "access without right" which may be useful analogy.

Section 17 gives the interpretation of "unauthorised access" for the purpose of section 1.Access is unauthorised where an individual is not entitled to or has not been given consent for the type of access in question.

The offence of unauthorised access requires proof of two *mens rea* elements of section 1(1):

1. there must be knowledge that the intended access was unauthorised;
2. there must have been an intention to secure access to any program or data held in a computer.

There has to be knowledge on the part of the offender that the offender that the access is unauthorised; mere recklessness is not sufficient. This covers not only hackers but also employees who deliberately

exceed their authority and access parts of the a system officially denied to them.

The *actus reus* of the offence requires the defendant to "cause a computer to perform any function." This is meant to exclude mere physical contact with a computer and the scrutiny of data without any interaction with a computer. Thus, the reading of confidential computer output, the reading of data displayed on the screen and, more controversially, "computer eavesdropping," are not within the scope of the offence. On the other hand, the offence does not require that the defendant must *succeed* in obtaining access to the program or data or be successful in subverting computer security measures in place. A remote hacker would, thus, "cause a computer to perform any function" if he accessed it remotely and the computer responded, such as by activating a computer security device or by offering a log-on menu. An employee would "cause a computer to perform any function" as soon as he switched on his desk-top micro and would be guilty of the offence if the requisite *mens rea* could also be proved. The substantive offence is thus drafted in such a way as to include conduct which might normally be thought to fall within the scope of the law of attempt. (52)

"There are two limbs to the *mens rea* of the offence. The first limb is the "intent to secure access to any program or data held in any computer." The word "any" makes it clear that the intent need not relate to the computer which the defendant is at that time operating. Subsection (2) explains that the defendant's intent need not be directed at any particular program or data, so as to include the common case of the hacker who accesses a computer without any clear idea of what he will find there. Recklessness is insufficient; still less would careless or inattentive accessing of the computer suffice for liability. The second limb is that the defendant must know at the time when he causes the computer to perform the function that the access which he intends to

(52) Martin Wasik, "The Computer Misuse Act 1990" [1990] Criminal Law Review 767 at 769.

secure is unauthorised. The prosecution must prove both limbs".(53)

The second offence, under section 2, is that of committing an offence under s.1 with intent to commit or facilitate the commission of another offence (where that further offence carries a sentence of 5 years imprisonment or more). An example of conduct constituting a section 2 offence would be accessing without authority another person's personal data (such as name and bank account number) from a computer with the intention of using those details to transfer money from an on-line bank account. Section 2 of the UK Computer Misuse Act 1990 has criminalized unauthorised access with intent to commit or facilitate commission of further offences. It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion. A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

The third main offence is that of doing an unauthorised act in relation to a computer (knowing that such act is unauthorised), with the intention of impairing the operation of any computer or program or impairing the reliability of any data; or intending to hinder access to any program or data held in any computer. This offence is created by section 3. Examples of acts that would constitute a section 3 offence include sending a virus or other malware to another computer (embedded in an email, for example); or using a mail program to bombard another computer/server with multiple emails so that the performance of the recipient computer/server is impacted (i.e. a "denial of service" attack).

Part 2 of the Serious Crime Act 2015 ('the SCA'), amends the Computer Misuse Act 1990. The changes take effect from 3 May 2015. A new s.3ZA is inserted in the 1990 Act which covers "Unauthorised

(53) Martin Wasik, "The Computer Misuse Act 1990" [1990] Criminal Law Review 767 at 769; Stefan Fafinski, "Access denied: computer misuse in an era of technological change" 2006, 70(5) Journal of Criminal Law 431.

acts causing, or creating risk of, serious damage". This appears to be an aggravated form of the existing offence under s.3, the difference being that the act must cause "serious damage of a material kind", or create a significant risk of such damage and, in particular, that the person concerned intends by doing the act to cause such damage or is reckless as to whether such damage is caused. Damage is of a "material kind" if it is damage to human welfare, the environment, the economy or national security. Note that the damage may be suffered in any country. The offence is indictable only with a maximum penalty of 14 years' imprisonment, but where the serious damage (or significant risk thereof) is to national security or to human welfare causing loss of life or illness or injury, the maximum penalty is life imprisonment. (Pt 2 s.41 of the SCA).

The other two material amendments to the 1990 Act are necessary for compliance with Directive 2013/40 on attacks against information systems. The first amends s.3A (making, supplying or obtaining articles for use in offences under s.1 or s.3) so as to close a loophole whereby it was an offence to obtain an article with a view to supplying it to another for the commission of an offence but it was not an offence to obtain for personal use with the intention of committing an offence. Thus, for example, an individual obtaining malware with a view to committing an offence himself would not be committing an offence under the existing s.3A, but will be caught by the amended s.3A as proposed. (Pt 2 s.42 of the SCA). The second amendment arising from the Directive widens the territorial scope of the Act by amending the two sections (ss.4 and 5) dealing with jurisdiction. It extends the categories of "significant link to the jurisdiction" in s.5 of the Act to include "nationality". This will provide a basis for the UK to prosecute a UK national who commits any s.1 to 3A offence whilst outside the UK and where the offence has no link to the UK other than the defendant's nationality, provided that the offence was also an offence in the country where it took place. (Pt 2 s.43 of the SCA).

More to the point of the present discussion, however, is the actual definition in the UK statute as to what constitutes 'unauthorised access',. 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 the UKCMA speaks expressly of access 'to any program or data held in any computer'. 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.

3.2 UK Judicial Interpretations of Unauthorised Access:

3.2.1 The House of Lords Interpretation of "Unauthorized Access":

In *Regina v Bow Street Metropolitan Stipendiary Magistrate and Another*(54), the House of Lords shed some authoritative light as to the interpretation of the phrase 'access of the kind in question.' The facts of this case can be summarised as follows: Joan Ojomo was an employee of American Express. She was assigned to the credit section of the Company's office in Plantation, Florida, as a credit analyst. In her daily work it was possible for her to access all customers' accounts, but she was only authorised to access those accounts that were assigned to her. However, she accessed various other accounts and files which had not been assigned to her and which she had not been given authority to

(54) [2000] 2 A.C. 216; [1999] 3 W.L.R. 620; [2000] 1 Cr. App. R. 61. See case commentary: "Misuse of computer - unauthorised access to computer program or data - meaning of unauthorised" [1999] Criminal Law Review 970-972.

work on. Having accessed those accounts and files without authority, she gave confidential information obtained from those accounts and files to, among others, Mr Allison. The information she gave to him and to others was then used to encode other credit cards and supply PIN numbers which could then be fraudulently used to obtain large sums of money from automatic teller machines.

The evidence concerning Joan Ojomo's authority to access the material data showed that she did not have authority to access the data she used for this purpose. At no time did she have any blanket authorisation to access any account or file not specifically assigned to her to work on. Any access by her to an account which she was not authorised to be working on would be considered a breach of company policy and ethics and would be considered an unauthorised access by the Company. The computer records showed that she accessed 189 accounts that did not fall within the scope of her duties. Her accessing of these accounts was unauthorised. Using these methods, she and her fellow conspirators defrauded American Express of approximately US$1,000,000. Mr Allison was arrested with forged American Express cards in his possession and was photographed using one such card to obtain money from an automatic teller machine in London. The proposed charges against Mr Allison therefore involved his alleged conspiracy with Joan Ojomo for her to secure unauthorised access to data on the American Express computer with the intent to commit the further offences of forging cards and stealing from that Company. It is Joan Ojomo's alleged lack of authority which is an essential element in the offences charged.

The United States Government sought the extradition of the accused from England. The allegation was that he had obtained account information from an employee of a charge card company, who was authorised to access its computer records solely for the purposes of her employment and had used that information to encode forged credit cards and obtain fresh personal identification numbers, so as to draw

large sums of money from automatic teller machines. The Secretary of State for the Home Department made an order to proceed, pursuant to section 4(2) of Schedule 1 to the Extradition Act 1989 , specifying two proposed charges of conspiring with the employee to commit an offence under section 2(1) of the Computer Misuse Act 1990, namely securing unauthorised access to a computer system contrary to section 1(1) of the Act with the additional intent to commit theft and forgery. A third charge alleged the causing of an unauthorised modification of the contents of a computer system, contrary to section 3 of the Act.

The magistrate declined to commit the accused on the first two charges on the ground that the term "unauthorised access," as defined in section 17(5) of the Act of 1990, did not extend to a person who was authorised to control the computer in question but misused the information thereby obtained. The magistrate held, however, that the provision of information leading to the issuing of a new personal identification number amounted to the causing of an unauthorised modification of the contents of a computer system and committed the accused in custody on the third charge to await the Secretary of State's decision on his extradition. The U.S. Government sought judicial review of the magistrate's refusal to commit on the first two charges. The accused applied for a writ of habeas corpus on the ground, inter alia, that offences under the Act of 1990 were not extraditable. The Divisional Court, refusing both applications, held that, by virtue of paragraph 20 of Schedule 1 to the Act of 1989, read with article III of Schedule 1 to the United States of America (Extradition) Order 1976 and section 15 of the Act of 1990, conspiracies to commit offences contrary to sections 2 and 3 of the Act of 1990 were extradition crimes in respect of which extradition to the United States of America could be granted; but that the effect of section 17(5) of the Act of 1990 was that the conduct of the employee with whom the accused was alleged to have conspired did not amount to an offence under section 1(1) of that Act so as to warrant the accused's extradition on that ground.

On appeal by the U.S. Government, the House of Lords allowed the appeal and held that section 1 of the Computer Misuse Act 1990 was not concerned with authority to access kinds of data, but with authority to access the actual data involved, for that section was designed to combat all forms of unauthorised access, whether by insiders or outsiders. It was also supported by the purpose of section 17(5) of the Act which identified two ways in which authority could be acquired, *i.e.* by being a person entitled to authorize or one who had been so authorised by such a person. That subsection also made clear that the authority must relate not simply to the data or program but also to the actual kind of access secured. Similarly, the word "control" did not mean the ability to operate or manipulate the computer, but rather to authorize or forbid. It did not derogate from the requirement that the authorisation had to relate to the relevant data or program or part of a program. Nor did it introduce any concept that authorisation to access one piece of data should be treated as authorising access to other pieces of data of the same kind. Accordingly, since in the instant case O had been given authority to access only that part of the company's data relating to work assigned to her, the access by her of any data for the purpose of the alleged conspiracy with the accused A. was unauthorised access within section 1(1). It followed that the Divisional Court had erred in its decision and the case would be remitted to the magistrate for reconsideration. The House of Lords held that:

Section 17 is an interpretation section. Subsection (2) defines what is meant by access and securing access to any programme or data. It lists four ways in which this may occur or be achieved. Its purpose is clearly to give a specific meaning to the phrase "to secure access". Subsection (5) is to be read with subsection (2). It deals with the relationship between the widened definition of securing access and the scope of the authority which the relevant person may hold. That is why the subsection refers to "access of any kind" and "access of the kind in question". Authority to view data may not extend to

authority to copy or alter that data. The refinement of the concept of access requires a refinement of the concept of authorisation. The authorisation must be authority to secure access of the kind in question. As part of this refinement, the subsection lays down two cumulative requirements of lack of authority. The first is the requirement that the relevant person be not the person entitled to control the relevant kind of access. The word "control" in this context clearly means authorize and forbid. If the relevant person is so entitled, then it would be unrealistic to treat his access as being unauthorised. The second is that the relevant person does not have the consent to secure the relevant kind of access from a person entitled to control, authorize, that access. Subsection (5) therefore has a plain meaning subsidiary to the other provisions of the Act. It simply identifies the two ways in which authority may be acquired by being oneself the person entitled to authorize and by being a person who has been authorised by a person entitled to authorize. It also makes clear that the authority must relate not simply to the data or programme but also to the actual kind of access secured. Similarly, it is plain that it is not using the word "control" in a physical sense of the ability to operate or manipulate the computer and that it is not derogating from the requirement that for access to be authorised it must be authorised to the relevant data or relevant programme or part of a programme. 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 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.(55)

The ruling by the House of Lords has clarified several ambiguities in

(55) [2000] 2 A.C. 216 at 223-224.

the Computer Misuse Act 1990.(56) It has been argued that the House of Lords judgment clarified two ambiguities in the Computer Misuse Act 1990. The first was the interpretation of "unauthorised access", and the second was whether the Act applied to the activities of "insiders".(57) There is no doubt now that the Act applies to employees. "If the House of Lords had allowed the law to stand and not allowed the appeal, a gap would have been exposed in the law whereby obviously fraudulent behaviour, as in Allison's case, would have escaped criminal sanction. This would have defeated the purpose of enacting the Computer Misuse Act, which was to close the gaps in the criminal law relating to computers".(58) The decision removed the ambiguity regarding the interpretation of "unauthorised" and it is now certain that this term relates to the specific data accessed rather than the same "kind of data" (59)as suggested by Astil J. in *D.P.P v Bignell* .(60)

3.2.2 Access for Private Purposes:

In *Bignell* case, the respondents were officers serving in the Metropolitan Police. They instructed police computer operators to extract details of the registration and ownership of two cars from the Police National Computer for their own personal use. As a result they were charged with offences contrary to section 1 of the Computer Misuse Act 1990 . The respondents were convicted by the Stipendiary Magistrate. They appealed against those convictions to the Crown Court, contending that their use of the computer, even if it had been for private purposes, was not within the definition of "unauthorised access" provided by

(56) 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).

(57) Kelly Stein, "Unauthorised access" and the U.K. Computer Misuse Act 1990: House of Lords "leaves no room" for ambiguity" 2000, 6(3) Computer and Telecommunications Law Review 63.

(58) Kelly Stein, "Unauthorised access" and the U.K. Computer Misuse Act 1990: House of Lords "leaves no room" for ambiguity" 2000, 6(3) Computer and Telecommunications Law Review 66.

(59) Kelly Stein, "Unauthorised access" and the U.K. Computer Misuse Act 1990: House of Lords "leaves no room" for ambiguity" 2000, 6(3) Computer and Telecommunications Law Review 66.

(60) [1998] 1 Cr.App.R. 1.

section 17(5) of the Act. The Crown Court upheld the submission and allowed the appeal. The prosecution appealed by way of case stated.

Queen's Bench (Divisional Court dismissed the appeal. It held that the primary purpose of the Computer Misuse Act 1990 was to protect the integrity of computer systems by criminalising the breaking into or "hacking" of computer systems and not the integrity of the data stored on them. No offence under section 1 of the Act was committed where a person caused the computer to perform a function to secure access to information held at a level to which that person was entitled to gain access, even if he intended to secure access for an unauthorised purpose. In the present case the respondents had had authority to secure access by reference to section 17(2)(c) and (d) , it therefore followed that they did not fall within section 17(5). That being so, they had not committed an offence contrary to section 1 even though they had used their authority to access for an unauthorised purpose. "The narrower Bignell interpretation of the language and purpose of the Computer Misuse act 1990 would have limited the mischief the Act was meant to deal with". (61)

It has been argued that 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

(61) Mary W.S. Wong, "Cyber-trespass and «unauthorized access» as legal mechanisms of access control: lessons from the US experience", 2007, 15(1) International Journal of Law & Information Technology 90-128 at 120; Clive Gringras, "To be great is to be misunderstood: the Computer Misuse Act 1990" 1997, 3(5) Computer and Telecommunications Law Review 213-215.

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 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". (62)

The Singapore High Court In *Lim Siong Khee v Public Prosecutor* (63) considered 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'). 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. The Court also took into account the privacy policies and terms of service of several leading free web-based email service providers. 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. The Singapore district court adopted a wide reading of Section 3 of the SCMA (the

(62) Mary W.S. Wong, "Cyber-trespass and «unauthorized access» as legal mechanisms of access control: lessons from the US experience", 2007, 15(1) International Journal of Law & Information Technology 90-128 at 120-121.

(63) [2001] 2 SLR 342.

equivalent of Section 1 of the UKCMA) in *Public Prosecutor v Loh Chai Huat*.(64) This gives effect to the legislative intent to capture as many offences involving unauthorised access as possible. It 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.

In *R* v *Cropp*,(65), the defendant, without authority, keyed commands into a computer and thereby obtained by means of the same computer a discount, to which he was not entitled, on goods being purchased at a supplier. He was tried on, inter alia, a count charging an offence contrary to section 2(1) of the Computer Misuse Act 1990 by securing unauthorised access to a computer, in contravention of section 1(1) of the Act of 1990, with intent to commit a further offence of false accounting. On a submission of no case to answer the trial judge ruled that, on a true construction of section 1(1)(a) of the Act of 1990, a second computer had to be involved, so that section 2(1) was inapplicable to the facts, and he upheld the submission. The Attorney-General referred to the Court of Appeal under section 36 of the Criminal Justice Act 1972 the question whether, in order for a person to commit an offence under section 1(1) of the Act of 1990 the computer which the person caused to perform any function with the required intent had to be a different computer from the one into which he intended to secure unauthorised access to any program or data held therein. The Court of Appeal (Attorney General's Reference (No.1 of 1991)),(66) held that, in section 1(1)(a) of the Act of 1990 the words "causes a computer to perform any function with intent to secure access to any program or data held in any computer," in their plain and ordinary meaning, were not confined to the use of one computer with intent to secure access into another computer; so that section 1(1) was contravened

(64) [2001] SGDC 174.

(65) Unreported, 4 July 1990.

(66) [1993] Q.B. 94; [1992] 3 W.L.R. 432; [1992] 3 All E.R. 897.

where a person caused a computer to perform a function with intent to secure unauthorised access to any program or data held in the same computer. Lord Taylor of Gosforth CJ commented: "[Counsel for the Attorney-General] pointed to the surprising, and indeed unlikely lacunae which this Act would have left in the field of interference with computers if the construction for which [counsel for the respondent] contends were correct … [The] kind of activity of going straight to the in-house computer and extracting confidential information from it could be committed with impunity so far as the three offences in this Act are concerned".(67)

The decision of the trial judge in Cropp was criticized on the ground that it "seemed incongruous with the purpose that the Act declared in its own long title: securing computer material against unauthorised access. Had the Court of Appeal not overturned the judgment of a lower court a large gap would have been left in the legislation.(68) If *Cropp* were to be followed, this would have the effect of limiting the scope of the Act to networked systems alone; whilst this would not seem to be too problematic in the modern networked society, it is particularly surprising in the context of the time when many more computers were standalone".(69) The decision in *Cropp* has ensured the survival of s 1 as a weapon against 'insider hackers'.(70)

3.2.3 Exceeding authorized Access

"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 *Allison* stated that the police computer operator in *Bignell* 'did not

(67) Attorney-General's Reference (No. 1 of 1991) [1993] QB 94 at 100.

(68) E. Susan Singleton, "Computer Misuse Act 1990 - recent developments" 1993, 14(1), Company Lawyer 22.

(69) Stefan Fafinski, "Access denied: computer misuse in an era of technological change" 2006, 70(5) Journal of Criminal Law 432.

(70) E. Susan Singleton, "Computer Misuse Act 1990 - recent developments" 1993, 14(1), Company Lawyer 22 at 23.

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 Huat,* 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 *fight* 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".(71)

The UKCMA circumscribes the extent and nature of authorized access, in Sections 17(5) and 2(5) respectively. The courts 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 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. UKCMA seems 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 UK and Singapore jurisdictions.(72) US CFAA defines the term "exceeds authorized access". It means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessory is not entitled so to

(71) Mary W.S. Wong, "Cyber-trespass and «unauthorized access» as legal mechanisms of access control: lessons from the US experience", 2007, 15(1) International Journal of Law & Information Technology at 122.

(72) Mary W.S. Wong, "Cyber-trespass and «unauthorized access» as legal mechanisms of access control: lessons from the US experience", 2007, 15(1) International Journal of Law & Information Technology at 122.

obtain or alter.(73)

The UK and its respective courts seem to demonstrate a commonsensical approach toward refining the existing statutory definition of 'unauthorised access' without undue linguistic acrobatics. "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. The principles and rules behind trespass, burglary and theft provided a 'natural conceptual point of departure"0 2, buttressed by the prevalence of the property metaphor. As a result, statutes such as the CFAA, UKCMA and SCMA reveal a reliance on property concepts, particularly in the notions of 'access' and the causation of damage. 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 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".(74)

(73) 18 U.S.C. § 1030(e)(6).

(74) Mary W.S. Wong, "Cyber-trespass and «unauthorized access» as legal mechanisms of access control: lessons from the US experience", 2007, 15(1) International Journal of Law & Information Technology at 123-124. (Footnotes omitted).

It has been argued that "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".(75)

(75) Mary W.S. Wong, "Cyber-trespass and «unauthorized access» as legal mechanisms of access control: lessons from the US experience", 2007, 15(1) International Journal of Law & Information Technology at 126.

4. Unauthorized Access in the Qatari Law:

On 16 September 2014, the Qatari government promulgated a Cybercrime Prevention Act No.14 of 2014 in an effort to increase the tools for combating online and cybercrimes. The new law imposes many sanctions and several penalties for offences committed through the Internet, IT networks, computers and other related crimes. The legislation is aimed at safeguarding the country's technological infrastructure and strengthening cyber security within Qatar. There are several types of crimes which are dealt with in the Law, ranging from crimes committed directly to electronic data and software, to the use of technology to facilitate the commission of traditional crimes such as defamation.

The deliberate unauthorised access to any website, information system (including hardware), network or item that falls within the definition of information technology is a crime, which can result in either imprisonment for up to three years and/or a fine of QR500, 000. More significantly, any unauthorised access to websites or information systems, including hardware, belonging to any government agency, authority or entity will result in imprisonment for a maximum of three years and a fine limited at QR500, 000. Article 2 of the Act provides that "Whoever gains access via the Internet or an Information Technology means, without right, to a Website or an electronic Information System of any governmental agency bodies, institution, authority, or corporation affiliated with the government of the State of Qatar, shall be punished by imprisonment for a period not exceeding three years, and by a fine not exceeding five hundred thousand (500,000) Riyals. The punishment set forth in the preceding paragraph shall be doubled if the act of access resulted in obtaining electronic information or data; obtaining information or data related to the State's domestic or foreign security, its national economy, or any other governmental data deemed confidential by nature or by way of issued directions; deleting, impairing, destroying, or publishing such electronic information and data; harming beneficiaries or users;

or obtaining ineligible funds, services, or benefits".

Article 3 of the Act states that "Whoever intentionally accesses without right, by any method, an electronic Website, Information System, Information Network, or any Information Technology means or part of it, or exceeds authorised access, or continues his/her visit or access after having knowledge of its illegality, shall be punished by imprisonment for a period not exceeding three years, and a fine not exceeding five hundred thousand (500,000) Riyals, or either of these two penalties. The punishment set forth in the preceding paragraph shall be doubled if the act of access resulted in cancelling, omitting, adding, disclosing, impairing, modifying, transmitting, capturing, copying, publishing, or republishing electronic information or data stored in an Information System; harming users or beneficiaries; destroying, stopping, or disabling an electronic Website, Information System, or Information Network; changing, cancelling, or modifying the content, designs, method of using an electronic Website; or impersonating the owner or the administrator of such Website".

The Qatari law prohibits individuals from using unauthorized access or exceeding authorized access to obtain information. By obtaining information, a hacker violates the confidentiality of the information stored on the computer. This invasion of privacy can take the form of the theft of financial information, medical information, and government or national security information as well as trade secrets or proprietary business information. The Qatari Act of 2014 criminalizes unauthorised access whether the perpetrator obtained information or not. However, if he managed to obtain information or data this will affect severity of punishment. According to the Anti-Cybercrime Act, obtaining information or data through computer hacking is an aggravated circumstance. Moreover, the 2014 Act distinguishes between types of stolen data for purposes of severity of punishment. Such approach is adopted by the Qatari statute under Articles 2/2 and 3/2 of the aforementioned Act.

Cyber intrusions that involve access to confidential information can have

a severe impact on privacy that may not be easy to quantify in monetary terms. The Qatari 2014 Act consider the special sensitivity of certain kinds of information and assign greater corresponding penalties. For example, the theft of certain government records or national security information may pose such a danger that it is punished more severely, regardless of whether the information has monetary value.

Unauthorised access was criminalized by the Qatari Penal Code No. 11 of 2004. Article 371 states that "Whoever accesses data saved onto a computer or who is caught hacking into the data system or a part thereof, without right, shall be punished with imprisonment for a term not exceeding three years and/or a fine not exceeding ten thousand (QR 10.000) Riyals". This section applies only to data stored in computers.

According to Article 51 of the Act, the penalties specified for the crimes prescribed under the provisions of this Law shall be doubled if a public official commits or facilitates committing the crime by abusing his powers or authorities. Under Article 50 of the Act whoever attempts to commit a felony or a misdemeanor prescribed under the provisions of this Law shall be punished by imprisonment for a period not exceeding half of the maximum penalty imposed for committing the consummated offence.

Article 52 provides that In the event of a conviction for any offences set forth in this Law, the court may, in addition to the specified punishment, order to deport the non-Qatari offender out of the State. Under Article 53, In addition to the penalties set forth in this law, and without prejudice to the rights of *bona fide* third parties, the court shall, in all cases, order to confiscate devices or programs or means used in, or any funds obtained form, the offences set forth in this law. Moreover, the court shall order the closure of the place or blocking of electronic Websites where the offence has occurred or whereby crimes are committed, as the case may be. Article 54 states that the penalties stipulated by this Act should be discharged, if any of the offenders initiated to inform the competent authorities about the crime and the participants involved

prior to the knowledge of the authorities and before the damage occurrence. The court may order the suspension of the execution of the penalty if the information was communicated to the authorities after they had already become aware of the crime, but in circumstances where this information led to the arrest of the rest of the perpetrators.

In Qatar, the criminal offence of unauthorised access is committed whether computer users had implemented security measures or not. The new wording does not make the infringement of security measures a prerequisite for the punishment of unauthorized access to information systems, and it is not an essential element to trigger criminal legal responsibility. In UK, during passage of the Bill attempts were made to add a provision whereby hackers would be able to offer a defense if computer users had not implemented security measures. The amendment failed. However, subsequently, Michael Colvin, the Act's proposer, has stated: "If companies do not invest in their own computer security strategy, then they cannot expect the sympathy of the courts when people are charged under the provisions".(76) In Kuwaiti Anti-Cybercrime Act No.63 of 2015 defines :unauthorised access": Unlawful Intentional access, by any method, an electronic Website, Information System, Information Network, or any Information Technology means by circumventing or bypassing the security measures, partially or completely, for any purpose without authorisation, or exceeding granted authorization.(77) The concept of a 'security measure of an information system' is not a legal one by nature and should be analysed from the perspective of computer technologies as these are better suited to define them. The way we see it, from a technological perspective, a violation of a security measure does not necessarily mean overcoming either a visible or invisible barrier by force or by elaborate technical means. It can actually be the opposite. Of course, it is perfectly clear that the most manifest violation of a security measure is the one that is visible to the 'hacker' and which needs an additional operation to

(76) Ian Walden, "Update on the Computer Misuse Act 1990", 1994 Journal of Business Law 522 at 525.

(77) Article (1) of the Kuwait Anti-Cyber Crime Act No. 63 of 2015.

be defeated, usually through hacking techniques or tools. But there is much more to computer security measures than that.(78)

Unlike UK Computer Misuse Act 1990, Qatari Act of 2014 does not criminalize "making, supplying or obtaining articles for use in computer misuse offences". Therefore, complicity provisions in Article 39 of the Qatari Penal Code No. 11 of 2004 must be applied. This Article states that: The following shall be deemed as accomplice: 1. Whoever abets the commission of an offence which occurs as a consequence of such abetting. 2. Whoever agrees with another on the commission of an offence which occurs as result of such agreement. 3. Whoever knowingly aids the perpetrator in any manner in the commission thereof, making the occurrence thereof possible, due to such aid. Whoever knowingly supplies the principal to an offence with a weapon, instrument or anything else to commit an offence or deliberately assists the principal in any other way to carry out acts thereof. In UK, Section 37 of the Police and Justice Act 2006 has placed into the CMA a new offence of "making, supplying or obtaining articles for use in computer misuse offences". This meets the requirements of the Cybercrime Convention. It targets the creation, supply and use of so-called "hackers' tools". It is this measure which has caused the most controversy beyond the walls of the Palace of Westminster. Notably, APIG advised the Government not to legislate on this particular matter.(79) The main problem stems from the fact that "researchers in information security, penetration testers and other professionals in the field … may develop and make available such tools in the course of their study or business". (80) In short, these items are easily accessible and are widely used for legitimate purposes on a regular basis. It seems that the courts will be left with the difficult task of drawing the line of their illegal use.(81)

(78) Pedro Miguel F. Freitas and Nuno Goncalves, "Illegal access to information systems and the Directive 2013/40/EU" 2015, Vol. 29, No. 1, International Review of Law, Computers & Technology 50–62 at 60.

(79) APIG Report, Revision of the Computer Misuse Act (June 2004).

(80) Walden, Computer Crimes and Digital Investigations (2007), p.196.

(81) Neil MacEwan, "The Computer Misuse Act 1990: lessons from its past and predictions for its future" [2008] Criminal Law Review 955-967 at 965.

5. Conclusion:

The act of accessing a computer system without proper authorization has existed since the early days of the development of information technologies. Illegal access threatens interests such as the integrity of information systems. The legal interest is infringed not only when a person without authorization alters or 'steals' data in a computer system belonging to another, but also when a perpetrator merely 'looks around' in the computer system. The latter infringes upon the confidentiality of the data, and considerable actions on the part of the victim may be required to check the integrity or status of the system. 'Pure' or 'mere' illegal access to a computer system does not require that the offender accesses system files or other stored data. Criminalization of illegal access thus represents an important deterrent to many other subsequent acts against the confidentiality, integrity and availability of computer systems or data, and other computer-related offences, such as identity theft and computer-related fraud or forgery.

Illegal access to a computer is a "basic offence" for the commission of other dangerous threats, such as illegal interception, fraud, forgery, and many other computer crimes and cybercrimes. Hence, anticipating the criminalization of the conduct of access is also justified. The provision protects the legal interest of integrity and security of computer systems. The aim of the offence is not only to guarantee the owner a peaceful use of his/her information system, but also to guarantee that any access to the system is realized by an authorized subject. The Qatari Act of 2014 provides for criminalization of illegal access to the whole or part of an information system. It does not limit the object of illegal access to data or Information. It criminalizes access to an electronic Website, Information System, Information Network, or any Information Technology means or part of it. The provision covers access to a computer system, computer network, or to a computer connected to another computer, such as a LAN, Intranet or wireless. The objective element of the offence requires that the subject gain

access to the whole or any part of a computer system. That permits to cover the frequent situation where the access may be authorised but not the access to specific files or programs.

The Qatari law provides for the option of criminalization of mere unauthorized access to an information system. It does not require further condition to criminalize such behaviour, such as "bypassing security". Thus, it does not require criminalization of illegal access if it results in 'destruction, blocking, modification or copying of information or the disruption of the functioning of the computer, the computer system or related networks. Such approach enables the Qatari law to adopt a broader legislation on illegal access. The Qatari law requires the crime of illegal access to be committed intentionally. However, the definition of what constitutes 'intent' is usually left to Article 32 of the Qatari Criminal Code. Analysis of primary source legislation, however, shows that, for those illegal access provisions that specifically mention state of mind, the mental elements of '*intentionally*' are used– indicating that some form of intentionality is most usually required for the offence. Thus, in the Qatari law illegal access offence cannot be committed '*recklessly.*' The *mens rea* requires that the system be accessed "intentionally", which means that the conducts caused by negligence are not punishable.

The conduct of access must be realized "without authorisation", which means that the conduct of access authorized by the owner of the system, or by another legitimate holder of it, will not be punished. For the same reason, the conduct of access to a system that allows open and free access to the public is not criminalized. In this case, access is legal. The 2014 Act provides for aggravating circumstances if access leads to the 'obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries, or to the acquirement of secret government information', or for illegal access committed by the offender 'in the course of or because of

the discharge of his functions or has facilitated commission of the offences. The most common aggravating circumstance seen during primary source legislation review, however, was the involvement of computers critical to the functioning of infrastructure such as public services or government computers. The law provided special protection by way of increased penalties for illegal access to computers run by state authorities, or that could be linked to the functioning of critical infrastructure.

This research reveals the ambiguities latent in unauthorized access statutes and shows how the courts have struggled to define "access" and "without authorization" in a coherent way. Unauthorised access is a problem which deserves the attention of the criminal law. It shows that although the basic meaning of traditional crimes such as murder, burglary, and theft is broadly understood but it is not so with computer crimes, in particular illegal access to information system. The prohibition against unauthorized access to computers is new and remains a mystery. It is not clear what access a computer does mean, and under what circumstances does access become "unauthorized". The " difficulty that courts have encountered with concepts such as "access" and "authorization" present the rule, not the exception. Given the high-technology atmospherics of the fact patterns and the rapid advances in computer technology, confusion over the purpose and scope of the statutes may have been inevitable".(82) The scope of unauthorized access statutes is uncertain, and no one seems to know what these new laws cover.

Unauthorised access to computer material is becoming more prevalent, and more serious. Information stored on a computer system will not be protected by physical barriers to access or by the law of trespass or theft, as is information recorded on paper. A person who obtains access

(82) ORIN S. KERR, "CYBERCRIME›S SCOPE: INTERPRETING «ACCESS» AND «AUTHORIZATION» IN COMPUTER MISUSE STATUTES" [2003] 78 New York University Law Review 1596 at 1667.

to a computer can find in one place vast amounts of information which previously might have been stored in a multitude of locations. The facilities of the computer may be used to search for, select and process specific data at very high speeds. The consequences of unauthorised access, in the digital age, go far beyond what is possible with paper-based or manual systems.

Unlike access achieved by other means, where access is achieved by unauthorised computer access, the person who achieves access may use the computer to amend or otherwise use the information. The possible consequences of amending information stored on a computer are wide-ranging and serious. Such conduct could affect the country's economy and the lives of many people. Also, a person who gains unauthorised access to information stored in a computer may be tempted to go on and commit more serious activities such as theft or destruction of data.

Courts, legislatures, and commentators should adopt a more sophisticated understanding of the scope and meaning of unauthorized access statutes. Courts and commentators alike often speak of «access» and «authorization» as if the terms were self-defining.› But they are not. Adopting a clear definition for unauthorized access offers several distinct advantages. it protects the privacy of users who guard their information effectively, but it also allows individuals to use the Internet without fear of criminal prosecution On a doctrinal level, the recommended approach tracks the traditional treatment that analogous issues have received in criminal law, namely in the interpretation of consent defenses for crimes such as burglary, trespass, and rape. The approach is also consistent with the traditional theories of criminal punishment. Finally, the approach avoids constitutional difficulties, such as vagueness or overbreadth, that broader interpretations of unauthorized access statutes may create.

References:

A- Books and Articles:

- Ahmad Nehaluddin, "Hackers' criminal behaviour and laws related to hacking" 2009, 15(7), Computer and Telecommunications Law Review 159.
- APIG Report, *Revision of the Computer Misuse Act* (June 2004).
- Case commentary: "Misuse of computer - unauthorised access to computer program or data - meaning of unauthorised" [1999] Criminal Law Review 970.
- Christopher Lee Gen-Min, "Offences Created by the Computer Misuse Act 1993" [1994] Singj L. S. 263.
- Clive Gringras, "To be great is to be misunderstood: the Computer Misuse Act 1990" 1997, 3(5) Computer and Telecommunications Law Review 213.
- Digital Guards database (2001), Glossary [online]. Available at http://www.digitalguards.com/Glossary.htm.
- E. Susan Singleton, "Computer Misuse Act 1990 - recent developments" 1993, 14(1), Company Lawyer 22.
- Ian Walden, "Update on the Computer Misuse Act 1990", 1994 Journal of Business Law 522.
- Kelly Stein, ""Unauthorised access" and the U.K. Computer Misuse Act 1990: House of Lords "leaves no room" for ambiguity" 2000, 6(3) Computer and Telecommunications Law Review 63.
- M. Gercke, UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES, March 2011, at 44-46, available at https://www.itu.int/ITUD/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pd.
- Martin Wasik, "The Computer Misuse Act 1990" [1990] Criminal Law Review 767.

- Mary W.S. Wong, “Cyber-trespass and “unauthorized access” as legal mechanisms of access control: lessons from the US experience”, 2007, 15(1) International Journal of Law & Information Technology 90.
- Natasha Jarvie, “Control of cybercrime - is an end to our privacy on the Internet a price worth paying? Part 1” 2003, 9(3), Computer and Telecommunications Law Review 76.
- Neil MacEwan, “The Computer Misuse Act 1990: lessons from its past and predictions for its future” [2008] Criminal Law Review 955.
- ORIN S. KERR, “CYBERCRIME’S SCOPE: INTERPRETING “ACCESS” AND “AUTHORIZATION” IN COMPUTER MISUSE STATUTES” [2003] 78 New York University Law Review 1596.
- Pedro Miguel F. Freitas and Nuno Goncalves, “Illegal access to information systems and the Directive 2013/40/EU” 2015, Vol. 29, No. 1, International Review of Law, Computers & Technology 50.
- Reid Skibell, ‘Cybercrimes and Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act’, 18 Berkeley Tech. L.J 909 (2003.)
- Richard Downing, “Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime” (2005) 43 Columbia Journal of Transnational Law 705.
- Roger Darlington, “Crime on the net” (2001) [online]. Available at http://www.rogerdarlington.co.uk/crimeonthenet.html.
- Stefan Fafinski, “Access denied: computer misuse in an era of technological change” 2006, 70(5) Journal of Criminal Law 431.
- The Attorney-General’s Department of Australia (Review of

Commonwealth Criminal Law: Interim Report, Computer Crime, November 1988).

- The Law Commission of England and Wales (*Criminal Law: Computer Misuse* (Law Com. No 186, 1989).
- The Scottish Law Commission (Report *on Computer Misuse* (Scot Law Com, No 106, 1987).
- Walden, *Computer Crimes and Digital Investigations* (UK: Oxford University Press, 2007).

B-Legislation:

- Computer Fraud and Abuse Act 1984 (USA).
- Computer Misuse Act 1990 (UK).
- Computer Misuse Act 1993 (Singapore).
- Cybercrime Prevention Act No.14 of 2014 (Qatar).

Table of Content: