Unauthorised Access: Beyond Mere Cyber Trespass

By

Apar Gupta*

1. Introduction

It is indeed appropriate to remark that, "[i]t was the best of times, it was the worst of times . . ."[1] after surveying the possibilities and the tribulations, the internet provides. The primary concern of amongst internet users today is safety, security, and potential for misusing the computer system.

In 1999 prompted by United Nations Commission on International Trade Law's Model Law on Electronic Commerce[2] (MLEC) and notable developments in Asian countries such as Singapore and Malaysia, India commenced with providing a legal framework for internet activity.[3] The Union Cabinet approved the bill on May 13, 2000 and it was finally passed by both the houses of Parliament by May 17, 2000. The Act received presidential

* Final Year Candidate, LLB (Hons.), Guru Gobind Indraprastha University, New Delhi. The author would like to thank Prof. M.L. Upadhyaya for his unflinching guidance and mentorship.

[1] Charles Dickens, *A Tale of Two Cities* 1 (Oxford Illustrated Dickens ed., Oxford University Press 1998).

[2] United Nations Commission on International Trade Law, *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*, 12 June 1996, *available at* http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html (*last visited* Apr. 22, 2006) [hereinafter Guide to Enactment].

[3] Indira Carr, *India Joins the Cyber-Race: Information Technology Act 2000*, 6(4) Int. Tr. L. Reg. 122 (2000).

assent on June 9, 2000 as the Information Technology Act, 2000 (hereinafter 'ITA').[4] India aims to regulate all digital activity through the ITA.

Chapter IX of the ITA that reads as penalties and adjudications and contains several sections that *inter alia* provide for the imposing of civil penalties to maintain security and safety. Section 43(h) provides for penalties which been fixed as damages by way of compensation not exceeding Rs. 1,00,00,000 to affected persons. Technologically all the cyberwrongs contained under Section 43 require the basic action of unauthorized access because the subsequent actions flow from unauthorized access and hence a study on it is extremely pertinent.

2. Rationale for Providing for the Cybercrime of Unauthorised Access

In cyberspace when an unauthorized user gains access to data contained in computer, computer system or computer network, the consequences can be diverse and devastating for the data subjects. Among the more obvious risks is the possibility that an affected individual or organization will become a victim of identity and data theft[5] and will suffer ruinous losses to credit and reputation,[6] expenses to rectify unauthorized intrusion, and perhaps even lost business opportunities. The Law Commission of England and Wales

[4] Information Technology Act, 2000 (India) *available at* http://www.mit.gov.in/itbillonline/it_framef.asp (*last visited* Apr. 23, 2006) [*hereinafter* Information IT Act].

[5] *See gen*. R. Bradley McMahon, Note, *After Billions Spent to Comply with HIPAA and GLBA Privacy Provisions, Why Is Identity Theft the Most Prevalent Crime in America?*, 49 Vill. L. Rev. 625, 627-29 (2004); Anthony E. White, Comment, *The Recognition of a Negligence Cause of Action for Victims of Identity Theft: Someone Stole My Identity, Now Who Is Going to Pay for It?*, 88 Marq. L. Rev. 847, 851-52 (2005).

[6] *See, e.g.*, White, *supra* note 5, at 847-48.

noting the arguments in favor of enacting a provision prohibiting unauthorized access, stated that:[7]

> [F]irst, the actual losses and costs incurred by computer system owners whose security systems are (or might have been) breached; secondly, that unauthorized entry may be the preliminary to general criminal offenses; and thirdly, that the general willingness to invest in computer systems may be reduced, and effective use of such systems substantially impeded, by repeated attacks and the resulting feeling of insecurity on the part of computer operators.

To redress this Section 43(a) provides for penalties for when a person without authorisation, "accesses or secures access to such computer, computer system or computer network".

3. Defining Access

The genesis of the definition of "Access" is owed to the first proposal to enact federal computer crime legislation in the United States, with Senator Ribicoff's significant, 1977 bill proposing a Federal Computer Systems Protection Act.[8] The bill stated, "access means to approach, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of, a computer, computer system, or computer network."[9] This definition was criticized by the United States Justice Department on the

---

[7] *See* The Law Commission, Working Paper No. 186, *Criminal Law-Computer Misuse* 4 (1989).

[8] S. 1766, 95th Cong. (1977) (U.S.).

[9] *See also* Michael M. Krieger, *Current and Proposed Computer Crime Legislation*, 2 Comp. L.J. 721, 723 (1980).

ground that "approach" is a physical concept and appears to include being close to a computer.[10] Since then the term has undergone through various amendments with each enactment having its own flavor of the definition.[11]

The term access in common parlance means gaining entry into a computer. This maybe explained by an analogy to a tangible object. For example, a user trying to use a password-protected computer network being confronted by a screen that requires a valid username and password to proceed. We might say that this screen is akin to a lock on a front door, and that entering a username and password is like using a key to open the lock.[12] The definition in Section 2(1)(a) of the Act aims to include all nomenclatures of "access" by stating that it includes, "grammatical variations and cognate expressions" of the term. Moreover, the class of acts does not merely mean to gain entry and it includes "instructing or communicating" with respect to "with the logical, arithmetical, or memory function resources of a computer, computer system or computer network".

4. Taxonomy of Unauthorised Access

An unauthorized act is one which is done without authority; specif. (of a signature or indorsement), made without actual, implied, or apparent authority.[13]Courts have distinguished between the two ways in which access may occur without authorisation. First, a user can violate a contractual agreement with the owner or operator of the

[10] *See* Donn B. Parker, *Computer Crime: Criminal Justice Resource Manual* 84 (1989).

[11] *See, e.g.,* Kan. Stat. Ann. Sec. 21-3755(a)(1) (1971 & Supp. 2003); Wash. Rev. Code Ann. Sec. 9A.52.010(6).

[12] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" In Computer Misuse Statutes,* 78 N.Y.U. L. Rev. 1596 (2003); *See Trulock v. Freeh*, 275 F.3d 391, 409 (4th Cir. 2001).

[13] Blacks Law Dictionary (ed. Bryan A. Garner 2004).

computer. Under the broad contractual theory of authorization, any violation of the terms of service or terms of use of any computer a person accesses violates the statutory prohibition on unauthorized access.[14] Second, a user can circumvent a code-based restriction on the user's privileges. In the first case, if a company authorizes an employee to access the system for one reason, but the employee then accesses it for another reason, that employee become "unauthorized".[15] An example would be use that violates the Terms of Service that an ISP imposes on its customers. In the latter case, the use is unauthorized in the sense that it bypasses a code-based effort to limit the scope of the user's privileges. An example might be use of a stolen password to bypass the password gate designed to block access to a victim's account.[16]

5. Unauthorised Access

Section 2(1)(a) broadly coupled with Section 43, may have the effect of courts holding that a competitor's use of a "scraper" software program to methodically glean prices from a tour company's public Web site, in order to allow systematic undercutting of those prices, exceeded the authorized access otherwise allowed to Web users.[17] Similarly, in *America Online, Inc. v. National Health Care Discount, Inc.*,[18] a case concerning a defendant who sent e-mail spam, the court held that the Computer Fraud and Abuse

[14] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1569 (2003).

[15] Tyler Paetkau & Roxanne Torabian-Bashardoust, *California Deals With Id Theft*, 13-JUN Bus. L. Today 37, 41 (2004).

[16] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1600-01 (2003).

[17] *EF Cultural Travel BV v. Explorica, Inc.*, 274 F. 3d 577 (1st Cir. 2001).

[18] *America Online, Inc. v. National Health Care Discount, Inc.*, 121 F. Supp. 2d 1255 (N.D. Iowa 2000).

Act's[19] (hereinafter CFAA) prohibition against "accessing" computers is violated when someone sends an e-mail message from one's own computer that is then transmitted through other computers (without permission) until it reaches its destinations.

It is evident that all unauthorized accesses in cyberspace is not equal. The manner in which access is gained and what is subsequently done will have a bearing on the determination of the conduct as to which cyberwrong was committed.[20] The provisions of the CFAA are analogous to Section 43 of the ITA in this respect. The CFAA includes seven distinct crimes, listed in Sections 1030(a)(1) through (a)(7), almost all of which are triggered by "access without authorization" to computers. For example, one crime prohibits unauthorized access to government computers,[21] another prohibits unauthorized access to computers that results in damage,[22] and a third prohibits unauthorized access or exceeding authorized access to computers such that the user obtains private information.

[19] The Computer Fraud and Abuse Act, 18 U.S.C. sec. 1030.

[20] American Law Institute, *Internet Law for the Practical Lawyer*, SK102 ALI-ABA 139, 146 (2005).

[21] *See* 18 U.S.C. sec. 1030(a)(3).

[22] *See* 18 U.S.C. sec. 1030(a)(5).