Current problems of moral research and education in the IT environment

A. Voiskounsky
Moscow State University after M.V.Lomonosov, Russia
Moscow City University of Psychology & Education, Russia

Abstract

Prevention of computer crime includes two types of action: first, enhancement of computer security, and second, moral education adjusted to the IT environments. The latter is the main theme of the paper. Research on moral conduct in the IT environment is currently being carried out under the heading of cyberethics. New trends in cyberethics are discussed, aimed at reducing harmful effects of adolescents’ uncontrollable misuse of computers and the Internet. One of the reasons of this misuse is inability of younger generations to transfer rules of moral conduct to the new (virtual) environments. To reduce the number of newcomers to hackers/carders/crackers/phreakers’ communities, world-wide educational courses for adolescents are urgently needed. The objective of these educational programs need to be the development of flexible decision making in moral situations, including those inherent of the IT environments. The programs and training sessions need to be internationally approved and realized, since computer crime is trans-national. It is proposed that the theoretical background of this educational program might be the Kohlberg’s stage theory of moral development, which was worked out within the field of developmental psychology. Fieldwork research is needed, aimed at finding out the specifics of moral views of computer-savvy adolescents in different countries, and at working out programs of moral education which would fit the new environments.

Keywords: cyberethics, education, moral, psychology, computer crime, stages of moral development, Internet.
1 Introduction

Ethics is one of the oldest fields of knowledge; in its development it has undertaken changing views on the origin and functions of moral behavior. Ethics has usually been investigated and taught within philosophy; on the contrary, philosophy could be sometimes found within ethics. No matter what are the “correct”, or “true” relationships between the two fields, it’s well known that both ethics and philosophy have always been inseparable of certain elements of law. Less known perhaps, that both can hardly been separated from individual and group psychology, too.

Law is beyond the theme of this paper, but for the following point. Although ethics and law overlap, usually the matching is only partial. The reason is that whenever any new practical ethical issue emerges, the estimation of it as legal does not necessarily imply the estimation of it as moral, and vice versa; these two categories only rarely coincide. Human psychology takes the most part of responsibility for this discrepancy. This responsibility will be discussed in more details, taken the new issues in practical applications of ethics, namely the so-called cyberethics.

Cyberethics is usually meant as rules of ethical (i.e., right, lawful, and just) behavior in online environments. It should not be confused to legal, the latter being heavily and often fiercely discussed in the field. Cyberethics is largely dependent on universal ethical laws, and at the same time it is in many ways special and peculiar. As Barger puts it in [1], “I do not believe that computer ethics are qualitatively different from medical ethics or legal ethics or any other kind of professional ethics. I do, however, believe that the nature of the computer and its operation gives certain dilemmas in computing a unique character”.

2 Current research on cyberethics: a brief review

Cyberethics goes far beyond the “netiquette” rules worked out at the earlier period of the Internet use. Nowadays, cyberethics refers to both communicative (including chat rooms, web forums, live journal and weblog discussions, guestrooms’ and newsgroups’ exchanges, etc.) and non-communicative services, including collaborative work, online games, shopping and bargaining, shared cognitive actions, etc. Peculiarity of the current stage of the cyberethics is not yet fully realized. Most published sources display complicated issues of computer ethics which deal with, and mostly restrict with crime, safety and security, privacy and civil liberties, porn, harassment and fraud, children protection from Internet damages and identity theft, hacking/carding/phreaking and software pirating, right/left extremism and hacktivism, blackmailing and disseminating junk email, plagiarism and “digital divide”, spoofing, flaming and trolling, etc. (Grodzinsky [2]; Langford [3]; Rotenberg [4]; Spinello and Tavani [5]; Whine [6]). For example, Mason and colleagues [7] distinguish four cyberethical issues: accessibility, accuracy, privacy, and property. New issues arose recently dealing with cyberspace-related rights Lastowka and Hunter [8], and with the ethics of
human research on the Internet (Bruckman [9]; Frankel and Siang [10]; Hudson and Bruckman [11]).

Much the same issues one will find at the available bibliographical/program web sources (cyberethics.cbi.msstate.edu/biblio/, www.cpsr.org/program/ethics/, etc.). As a supplement to universal moral rules, codes of professional ethics have been worked out and are systematically updated. It is worth mentioning the codes of professional ethical conduct (Jamal and Bowie [12]; Rest and Narvaez [13]), particularly in the computer science and information management field (Cronan and Kreie [14]; Grodzinsky [2]; Mason et al. [7]; Panteli [15]). Besides, the ACM Code of Ethics and Professional Conduct (http://www.acm.org/constitution/code.html) is a useful source and is widely discussed, as well as the APA ethical code which was recently revised (http://www.apa.org/ethics/).

Important as they are, cyberethical issues and professional ethical codes have already been thoroughly discussed within the professional community. Moreover, useful empirical research has been done in the field. For example, illegal computer-related behaviors (ranging from illegal copying of licensed software pieces to changing/stealing data in other persons’ computers) are widely spread and often initiated by middle/high-school students: surveys held recently in San Diego, CA make it evident (McGuire et al. [16]). Ruf and Thomas [17] investigated the likelihood that university students would cheat, dependent on certain IT-related cases (copying spreadsheets, illegally sharing access to an electronic textbook, downloading and selling music CDs, copying computer programs) and on gaining varying awards (i.e., moderate or higher than moderate). Not a surprise, differing factors are shown to influence selectively the university students’ ethical/unethical behavior. Close to this is the conclusion made by Cronan and Kreie [14]: various combinations of legal or professional (i.e., codes of conduct) factors, or factors referring to personal beliefs and attributes (religious values, morals, experience, etc.), and to social environments impact processes of ethical decision making in the IT environment.

Culture specifics is believed to represent a valuable factor. Specific religious beliefs widely common in India (namely, belief in cyclic processes of personal birth and subsequent rebirth) are shown to influence significantly the likelihood of software piracy and deterioration of privacy in the IT field (Debnath and Bhal [18]). Research held in Korea within an adult sample demonstrated that moral judgment is dependent on Ss’ age, sex, and position in administrative hierarchy (Kim [19]).

Attitudes towards the computer/Internet abuse may vary greatly dependent on certain cultural backgrounds, too (Voiskounsky et al. [20]). Nevertheless, attitudes towards software license infringement, or use of viruses, or misuse of corporate computing resources are shown to be significantly different among professionals belonging to nine cultures; an important finding is that representatives of no nation (out of the nine investigated) might be characterized as holders of perverted, or totally opposite moral attitudes, compared to what is believed to be correct in Great Britain or in the USA (Whitman et al. [21]). Ang and Lo [22] found that the attitudes towards illegal copying of software pieces
depend upon three major factors, namely: (1) perceived personal gain (e.g., social acceptance, favour, repay of debt, etc.), (2) altruism, and (3) perceived negative consequences – if the illegacy is out.

2.1 The Internet misuse within the hackers’ communities

Besides attitudes, we believe that the actual level of knowledge in the area of cyberethics is of great importance, too. Let us take for example the activities characteristic for hackers/crackers/carders/phreakers/hacktivists (Sterling [23]; Taylor [24]). This underground population, though strongly differing in intentions, in methods used, in publicity, etc. is very special for a discussion of the cyberethics issues. Indeed, each protection device that is installed to prevent crime turns out to be rapidly confronted by circumventing techniques. Unsolicited intrusions into distant computers and databases, provocations of web-servers’ denials of service, spoofing, dissemination of computer viruses happen more and more often. Thus, the hackers’ population and the hackers’ qualification is ever growing; the same is believed to be true with the harm resulting from their improper actions.

There are different classifications of those who cause computer crime; we are going to mention only few of them. According to the one, we are recommended to distinguish the following subgroups: professional criminals or “cyberwar” terrorists, white collar criminals, disgruntled employees, and teenager hackers (Nicholson et. al. [25]; Shinder and Tittel [26]). Rodgers [27] classifies subgroups of hackers dependent on their expertise, areas of interests (software, hardware, cell phones, the Internet, etc.) and behaviour patterns: he differentiates tool kit/newbies, cyber-punks, internals, coders, old guard hackers, professional criminals, and cyber-terrorists. Obviously, there are no exact borders between them. In full correspondence with the reality, both classification schemes include children and teenagers. The least qualified newcomers (often children or adolescents) to the hackers’ underground are known as newbies, or wannabes. Every day wannabes enter this population, reasoning that hacking is a fashionable hobby or a profitable occupation. Newbies start with the simplest tasks just for fun, then some of them turn to more advanced tasks and gradually become either qualified crackers/carders, or else professionals in computer security; the majority of those who go on doing only elementary hacking tasks soon enough leave the population of hackers (Voiskounsky and Smyslova [28]).

One might suppose that the great amount, if not the majority of computer hacking/cracking/phreaking episodes in which middle/high school or college students are actors, stem from the fact that they are often unable to prognosticate the effects of their actions, and thus are simply unaware of the consequences - damaging, illegal, and at least unethical. Had the children/adolescent newbies knew of the harmful results, or could they foresee the problems they cause, many of them would never again use the cracking “vandalware”. “Mild and usually unintentional forms of deviance are the result of carelessness, playful mischief, immaturity, or simple ignorance” (Suler and Philips [29]). Being unaware does not always mean being ignorant, indifferent, or non-curious; taken children and adolescents, it often means psychological inability to transfer well-known
behavioral patterns into new situations. No wonder, in the cyberspace one usually finds oneself in peculiarly unfamiliar situations; this is equally correct for grown-ups and for children or adolescents.

3 A new direction of research in cyberethics

We are approaching the essence of this paper. It might be phrased in the following way. Decisions on some of the new cyberspace-related problems would not be based on exclusively ethical ground; traditional cyberethics seems to be insufficient. Instead, decision making needs to be based on data gained in developmental psychology and education. Thus, the newest trend within cyberethics is its overlap with psychology.

Each coin has two sides. Failing to transfer norms of ethical behavior into the cyberspace and thus “innocently” committing cybercrime, children and adolescents at the same time often become victims of deceptors, paedophiles and/or manipulators: they use to inform strangers about personal data, meet grown-up “friends” face-to-face and undergo sexual harassment, etc. The use of connected computers for communication, work, cognition, and gaming brings new educational and ethical dilemmas and problems to parents and educators – problems in the area in which caregivers, teachers and school principals usually lack training. The use of the Internet by K-12 students states technical, legal, organizational and ethical (or cyberethical) problems – this time overlapping psychological ones.

The world-wide community of the Internet users as well as non-users should work hard to teach new generations the essentials of the cyberethics. The latter is certainly based on traditional moral and should extend the moral norms into IT-related environment. Not that computer crime would perish, but at least the recruitment of “newbies” and wannabes might be reduced. This challenge is worth trying. Importantly, some theoretical models of ethical behavior stress the importance of the so-called "ethical sensitivity", that is, the ability to distinguish ethical or unethical behavior (Bommer et. al [30]; Wortuba [31]). The factors influencing the discrimination between ethical or unethical are shown to vary from case to case (Cronan and Kreie [14]). An ability to recognize ethical issues and to assess ethical/unethical alternatives is dependent on one's priority structure of values (Wortuba [31]).

3.1 Organizational support for research in new areas of the cyberethics

Facing the new challenge, concerned educators, IT and justice experts, and parents express their concern. Books by Schwartau on the theme [32] got a bestseller status; this fact might be taken as a signal of concern. Several organizations and associations (www.cybercitizenpartners.org, www.cybersmart.org/, www.internetwatch.org.uk/, www.staysafeonline.info, disney.go.com/cybersafety/, etc.) claimed readiness to consult every interested person or group on the newest issues of cyberethics. Enthusiasts worked out recommendations for safe use of the Web by children and adolescents: for
example, a SUSI project, or Safer Use of Services on the Internet (www.besafeonline.org/) has recently started in Scotland. More ambitious project Cybercitizen Awareness Program (www.cybercitizenpartners.org) is supported by the U.S. Department of Justice and the Information Technology Association of America. Within this project, several US-wide conferences have been held. Different governmental sources have worked out and compiled plenty of useful recommendations for children, for parents and for educators (www.cybercrime.gov/rules/cybercitizen.htm, www.usdoj.gov/criminal/cybercrime/, etc.).

In attempts to ensure security and to make web-navigations of K-12 students as safe as possible, the abovementioned web-pages and books refer exclusively to the traditional cyberethics. In an effort to prevent or obstruct improper/unethical use of computers the usually proposed measures are such as: enhanced security, prompt and fair reporting, tough sanctions, etc. All this is only one side of the coin. The other is in minimizing harm caused by K-12 students. To minimize harm, an educational program is urgently needed: children and adolescents need to be taught the likely unethical consequences of uncontrollable use of information and communication technologies.

### 3.2 New educational issues

Every high-school student of the coming generations needs to be the recipient of the would-be educational program; the advanced course should be taught to the most experienced computer/Internet users, including owners of homepages, hackers, gamers, winners of local and national competitions of high-school age programmers, creative software developers, etc. Such a program need to be international, since there are no borders in the cyberspace. Moreover, only a limited amount of “web-targets” are popular among hackers, including mostly the US-located web-sites and web-pages. These include the US Department of Defense, and the major world-known companies, especially those operating in the IT field. To secure the “web-targets” it’s preferable to combine computer security measures (firewalls, etc.) and the educational measures. The latter might help in reducing the number of wannabes and “newbies”, i.e. the newcomers to the hackers/carders/crackers/phreakers community.

The educational courses need to be based on psychological data describing stages of moral development during childhood and adolescence (and the adult age, too). The most sophisticated theory that proved its value is that introduced by Kohlberg in [33] and partly modified and developed by his followers (Turiel [34]). The Kohlberg’s stages include pre-traditional moral, traditional moral, and post-traditional moral (each stage is subdivided into two substages). Necessary corrections need to be made that stem from the Lefebvre’s differentiation of ethical principles inherent for a democratic and for a totalitarian society (Lefebvre [35]). This correction might be useful since totalitarian-type moral views and attitudes (as Lefebvre found) survive long enough after the transfer to the democratic social system. To make it more evident, we might remind that an Israeli hacker of certainly Russian origin was recently arrested in Israel (Shachtman [36]).
It is unlikely to come upon the highest stages of moral development testing children’s and adolescents’ judgments. It is true, however, that many adults never reach the highest stage of moral judgments throughout their life. It seems even less probable that teenagers be mature enough to base their judgments on independent moral system of post-traditional value. It is widely believed (irrespective of whether the belief is true) that when online, the majority of children and adolescents stay on a lower stage of moral development than in real life. The possible explanation lies in the anonymity of the Internet-mediated contacts. For example, rather few teenagers would steal a wallet from someone’s pocket; at the same time many of them are eager to purchase goods – and especially services – using stolen card numbers. Thus, to adapt the adolescents’ system of moral judgments to the Internet anonymity is a challenge. Traditional books on cyberethics miss this challenge. New books and educational courses have all the chances to meet the challenge: in these sources, we believe, cyberethics will overlap developmental psychology.

References


