Richard A. Spinello

CYBERETHICS

Morality and Law in Cyberspace

FOURTH EDITION

CYBERETHICS

Morality and Law in Cyberspace

FOURTH EDITION

Richard A. Spinello
Carroll School of Management
Boston College
Chestnut Hill, Massachusetts

JONES & BARTLETT
LEARNING

World Headquarters
Jones & Bartlett Learning
40 Tall Pine Drive
Sudbury, MA 01776
978-443-5000
info@jblearning.com
www.jblearning.com

Jones & Bartlett Learning
Canada
6339 Ormindale Way
Mississauga, Ontario L5V 1J2
Canada

Jones & Bartlett Learning
International
Barb House, Barb Mews
London W6 7PA
United Kingdom

Jones & Bartlett Learning books and products are available through most bookstores and online booksellers. To contact Jones & Bartlett Learning directly, call 800-832-0034, fax 978-443-8000, or visit our website, www.jblearning.com.

Production Credits
Publisher: David Pallai
Senior Acquisitions Editor: Timothy Anderson
Production Director: Amy Rose
Editorial Assistant: Melissa Potter
Production Assistant: Rebekah Linga
Senior Marketing Manager: Andrea DeFronzo
V.P., Manufacturing and Inventory Control: Therese Connell
Composition: Northeast Compositors, Inc.
Cover Design: Timothy Dziewit
Cover Image: (top) ©Htu/ShutterStock, Inc.; (bottom) ©Andrey Burmakin/ShutterStock, Inc.
Printing and Binding: Malloy, Inc.
Cover Printing: John Pow Company

Library of Congress Cataloging-in-Publication Data
Spinello, Richard A.
Cyberethics : morality and law in cyberspace / Richard A. Spinello. — 4th ed.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-0-7637-9511-5 (paper.)
ISBN-10: 0-7637-9511-9 (ibid.)
1. Internet—Moral and ethical aspects. 2. Cyberspace—Moral and ethical aspects. 3. Computers and civilization. 4. Law and ethics. I. Title.
TK5105.875.I57S68 2011
303.48'34—dc22
2010014406

6048
Printed in the United States of America
14 13 12 11 10 10 9 8 7 6 5 4 3 2 1

In memory of my grandmothers,
Guiseppa Padrevita and *Olga Spinello*

PREFACE

Since *CyberEthics: Morality and Law in Cyberspace* first appeared ten years ago, the social and technical landscape of cyberspace has undergone remarkable changes. There are new technologies, for example, that make it easier to download and disseminate digital music and movies. There are also many new virtual communities such as craigslist which are helping to create a "sharing" economy. At the same time, there have been extraordinary legal developments—new laws like the Children's Internet Protection Act and various court decisions (such as MGM v. Grukster)—defining new constraints for Web surfers. We have tried to take all of these developments into account in this new edition.

The growth of the Internet has been one of the most remarkable phenomena of the last century. In the early 1980s, the Internet was known to only a handful of scientists and academics, but it is now being regularly used by well over 1 billion people, and many predict that it will continue to revolutionize everything from the practice of medicine to education. The Internet is more than merely a communications network. It is an infrastructure, helping to create a new social and economic order characterized by global connectivity and the decentralization of authority.

The success of the Internet would not have been possible without the recent development of the World Wide Web, which has made a wide variety of media (such as text, video, and audio) available through a user-friendly interface. The Web has ignited electronic commerce and changed the face of Internet communications. Web sites like Twitter have already had a dominating influence on the culture.

This rapid development of the Web and the entire Internet economy is not without its social costs. If it is easier to publish and spread truthful and valuable information, it is also easier to spread libel, falsehoods, and pornographic material. If it is easier to reproduce and remix digitized information, it is also easier to violate copyright protection. And if it is easier to build personal relationships with consumers, it is also easier to monitor consumers' behavior and invade their personal privacy. Thus, the Internet's vast capabilities can be misused to undermine private property and mock our traditional sense of moral propriety.

Our primary purpose in this revised edition is to carefully review the social costs and moral problems that have been triggered by the expanded use of this communications and information network. Although some of these problems are familiar ones, many are new to the fields of computer ethics and public policy. For example, although much work has been done on the topic of intellectual property, little attention has been paid to the ethical dimension of issues such as fair use. In the process of examining these issues, we identify some of the legal disputes that have become paradigm cases in cyberlaw juris prudence.

The Internet is also a challenge to legal systems, which have had a difficult time keeping up with this borderless global technology. In the past, the Internet was an unstructured electronic terrain, a frontier with few rules and restrictions. But now that cyberspace has become a widely used forum for our economic transactions and social interactions, many argue that anarchy must yield to some type of order and that new laws must be crafted to restrict and punish asocial users. Some civil libertarians, however, steadfastly resist intrusive government intervention. "Keep your hands off our Net" is one of their favorite slogans. But is that philosophy still tenable or is it just too romantic and antiquated for a commercialized Internet?

If we do agree that the Net needs some type of order, the key question is how that order should be imposed or how the Net should be governed. A framework of laws and regulation is one solution, but there are others, such as greater reliance on self-regulation from below with the help of technology. Why not let technology correct itself? There are, after all, viable Internet architectures to deal with some of the Internet's social problems, perhaps even more effectively than a centrally imposed set of regulations. These two approaches represent the fundamental options for the future of Internet regulation. Should the state, for example, promulgate and enforce laws that ban pornography? Or should individual users rely on filtering devices to keep it out of their homes and schools? Is the proper model centralized state controls or decentralized individual controls?

In Chapter 2, we present the case for greater reliance on a decentralized, bottom-up approach to governing the Internet. Its proponents argue that this approach best fits the Internet's open architecture along with the logic of this medium. It can also overcome some of the administrative difficulties of controlling an international network. It is quite difficult for any nation to exercise local jurisdiction over the information available in cyberspace. But it is often possible for technology itself to constrain behavior without the need for the heavy hand of government. According to this perspective, the role for government involvement in regulating the Internet should be as modest as possible. There may be externalities or market imperfections that cannot be handled by technology such as monopolistic behavior that threatens the Internet economy. Such situations may warrant strong government intervention but, otherwise, Internet stakeholders should be allowed to govern themselves.

On the other hand, there are many perils in depending on self-regulation, especially when we empower the regulator with sound technology. There could be excesses such as the privatization of unfair copyright regulations or irresponsible content control. This has led many scholars and analysts to call for more comprehensive, top-down regulations to ensure that the Internet is governed with regularity and fairness. Their viewpoint is also presented in Chapter 2.

Thus, our second purpose in this book is to stimulate the reader's reflection on the broad issue of Internet governance. How one resolves this fundamental question will provide an important context for addressing the formidable social problems triggered by the explosive growth of the Internet.

To accomplish these objectives, we first lay out some theoretical groundwork drawn from the writings of contemporary legal scholars like Larry Lessig and philosophers like Kant, Finnis, and Foucault. We then focus on four broad areas: content control and free speech, intellectual property, privacy, and security. For each of these critical areas, we consider the common ethical and public policy problems that have arisen and how technology or law would propose to solve some of those problems.

The first of these four topics concerns the fringes of Internet communication such as pornography, hate speech, and spam (unsolicited commercial e-mail). We review the history of public policy decisions about the problem of pornography and treat in some depth the suitability of automated content controls. Are these controls technically feasible and can they be used in a way that is morally acceptable to the relevant stakeholders? We also consider other prominent free speech issues such as appropriate standards for bloggers.

We then review the new breed of intellectual property issues provoked by the steady commercialism of the Internet and the proliferation of Web sites. These include ownership of domain names and how digital technology complicates the emergence of open source software copyright. Also discussed is the growing reliance on digital rights management systems, an electronic means of ensuring that copyright protections are followed.

Perhaps the most notorious and widely publicized social problem is the ominous threat that the Internet poses to personal privacy. The Internet seems to have the potential to further erode our personal privacy and to make our lives as consumers and employees more transparent than ever before. What, if anything, should be done about online databases overflowing with personal information? The covert gathering of information from consumers visiting Web sites, the use of "cookies" and spyware, and the strict monitoring of employees' Internet interactions are other problematic concerns. Here again we explore whether certain protective technologies can be part of the solution.

Finally, we treat the critical area of security with an initial focus on the perennial problem of trespass in cyberspace. We dwell on what constitutes trespass and why it can be so damaging. Also discussed is the vulnerability of the Internet to cyberspies. In this context we treat encryption technology as a means of ensuring that transmitted data are confidential and secure. The encryption controversy epitomizes the struggle between government control and individual rights that is shaping many of the public policy debates about the Internet. Should users be able to encrypt data without giving the government backdoor access? Or is this too big a threat to national security? In addition to a cursory overview of the federal government's policies on encryption, we analyze this matter from a moral framework to expose this dilemma to a slightly different perspective. The chapter concludes with an overview of security issues and electronic commerce.

It should be apparent by now that this book is a bit more narrowly focused than traditional books about computer or information ethics; topics are limited to the particular moral problems that emerge in the realm of cyberspace. However, if one considers the rapid evolution of the Internet and the great potential of Web communications, what is presented here represents the new generation of moral issues that will occupy computer ethicists, lawyers, and public policy makers for many years to come.

Also, throughout the book we implicitly embrace the philosophy of *technological realism*, which sees technology as a powerful agent for change and forward progress in society. But, unlike more utopian views, this position does not ignore the dangers and deterministic tendencies of technology along with its potential to cause harm and undermine basic human rights and values.

In our view, corporations and individuals, although heavily influenced by information technology, are not yet in its thrall—they still have the capacity to control its use and curtail its injurious side effects. Such control requires prudent decision making, which will help to ensure that computer technology is used wisely and cautiously, in a way that enhances the human condition and the opportunity for human flourishing. It also demands that all information technologies, including those targeted at the social problems of cyberspace, be implemented with respect for standards of justice and fairness.

Like most traditional books on ethics, this one is optimistic about the tenacity of the human spirit and the depth of moral conviction, even in cyberspace. The technology determinists believe that the forces of technology have already won the war, but the realists contend that the struggle continues on and that the final outcome is still in doubt.

Acknowledgments

I am most grateful to those who have adopted the first two editions of this book: they have given me valuable feedback and suggestions that are incorporated into this new edition. I am indebted to Joyce O'Connor in the Carroll School of Management at Boston College for her assistance in help-

ing me handle some of the mechanics involved in publishing this manuscript. Many thanks also to several individuals at Jones & Bartlett Learning, especially Tim Anderson and Melissa Potter, for their help in publishing this fourth edition. Finally, I owe a great debt of gratitude to my wife, Susan T. Brinton, for her patience and continued tolerance for the lonely life of an author.

Richard A. Spinello
Hyde Park, MA

CONTENTS

CHAPTER ONE

The Internet and Ethical Values

> The end [of ethics] is action, not knowledge.
> —Aristotle[1]

More than three decades have passed since the first communications were transmitted over a fledgling global network, which would later be called the *Internet*. At the time, few would have predicted the Internet's explosive growth and persistent encroachment on our personal and professional lives. This radically decentralized network has been described in lofty terms as empowering and democratizing. It has lived up to this ideal by creating opportunity for many new voices with extraordinary reach. Although the claim that the Internet will revolutionize communications may be hyperbole, there is no doubt that the Internet has the potential to magnify the power of the individual and fortify democratic processes.

Many governments, however, are clearly threatened by some of this decentralized power and they have sought to impose some centralized controls on this anarchic network. The United States has attempted to regulate speech through the ill-fated Communications Decency Act and to restrict the use of encryption technology through its key recovery scheme. More draconian regulations have been imposed by countries like Iran, China, and Saudi Arabia. The Net and its stakeholders have steadfastly resisted the imposition of such controls, and this has led to many of the tensions and controversies we consider throughout this book.

Although the control of technology through law and regulation has often been a futile effort, "correcting" technology with other technology has been more effective. The regime of law has had a hard time suppressing the dissemination of pornography on the Internet, but blocking software systems that filter out indecent material have been much more successful. This reflects the net's paradoxical nature—it empowers individuals and allows them to exercise their rights such as free speech more vigorously, but it also makes possible effective technical controls that can undermine those rights.

Although the primary axis of discussion in this book is the ethical issues that surface on the Internet, we must devote attention to these related matters of cyber governance and public policy. Thus, we explore in some detail the tensions between the radical empowerment that the Net allows and the impulse to tame this technology through laws and other mechanisms.

Because this is a book about ethics, about *acting* well in this new realm of cyberspace, we begin by reviewing some basic concepts that will enrich our moral assessment of these issues. Hence, in this introductory chapter our purpose is to provide a concise overview of the traditional ethical frameworks that can guide our analysis of the moral dilemmas and social problems that arise in cyberspace.

More important, we also elaborate here on the two underlying assumptions of this work: (a) the *directive* and architectonic role of moral ideals and principles in determining responsible behavior in cyberspace and (b) the capacity of free and responsible human beings to exercise some control over the forces of technology (technological realism). Let us begin with the initial premise concerning the proper role of cyberethics.

Cyberethics and the "Law of the Horse"

An ethical norm such as the imperative to be truthful is just one example of a constraint on our behavior. In the real world, there are other constraints including the laws of civil society or even the social pressures of the communities in which we live and work. There are many forces at work limiting our behavior, but where does ethics fit in?

This same question can be posed about cyberspace, and to help us reflect on this question we turn to the framework of Larry Lessig. In his highly influential book, *Code and Other Laws of Cyberspace*, Lessig first describes the four constraints that regulate our behavior in real space: law, norms, the market, and code.

Laws, according to Lessig, are rules imposed by the government which are enforced through *ex post* sanctions. There is, for example, the complicated IRS tax code, a set of laws that dictates how much taxes we owe the federal government. If we break these laws, we can be subjected to fines or other penalties levied by the government. Thanks to law's coercive pedagogy, those who get caught violating tax laws are usually quick to reform.

Social norms, on the other hand, are expressions of the community. Most communities have a well-defined sense of normalcy, which is reflected in their norms or standards of behavior. Cigar smokers are not usually welcome at most community functions. There may be no laws against cigar smoking in a particular setting, but those who try to smoke cigars will most likely be stigmatized and ostracized by others. When we deviate from these norms, we are behaving in a way that is socially "abnormal."

The third regulative force is the market. The market regulates through the price it sets for goods and services or for labor. Unlike norms and laws, market forces are not an expression of a community and they are imposed immediately (not in *ex post* fashion). Unless you hand over $2 at the local Starbucks you cannot walk away with a cup of their coffee.

The final modality of regulation is known as architecture. The world consists of many physical constraints on our behavior—some of these are natural (such as the Rocky Mountains) whereas others are human constructs (such as buildings and bridges). A room without windows imposes certain constraints because no one can see outside. Once again "enforcement" is not *ex post* but at the same time the constraint is imposed. Moreover, this architectural constraint is "self-enforcing"—it does not require the intermediation of an agent who makes an arrest or who chastises a member of the community. According to Lessig, "the constraints of architecture are self-executing in a way that the constraints of law, norms, and the market are not."[2]

In cyberspace we are subject to the same four constraints. Laws, such as the ones that provide copyright and patent protection, regulate behavior by proscribing certain activities and by imposing *ex post* sanctions for violators. It may be commonplace to download and upload copyrighted digital music, but this activity breaks the law. There is a lively debate about whether cyberspace requires a unique set of laws or whether the laws that apply to real space will apply here as well with some adjustments and fine tuning. Judge Frank Easterbrook has said that just as there is no need for a "law of the horse," there is no need for a "law of cyberspace."[3]

Markets regulate behavior in various ways—advertisers gravitate to more popular Web sites, which enables those sites to enhance services; the pricing policies of the Internet service providers determine access to the Internet; and so forth. It should be noted that the constraints of the market are often different in cyberspace than they are in real space. For instance, pornography is much easier and less expensive to distribute in cyberspace than in real space, and this increases its available supply.

The counterpart of architectural constraint in the physical world is software "code," that is, programs and protocols that make up the Internet. They too constrain and control our activities. These programs are often referred to as the "architectures of cyberspace." Code, for example, limits access to certain Web sites by demanding a username and password. Cookie technology enables e-commerce, but compromises the consumer's privacy. Sophisticated software is deployed to filter out unsolicited commercial e-mail (or spam). In the long run, code may be more effective than law in containing spam, which rankles many users.

Finally, there are norms that regulate cyberspace behavior, including Internet etiquette and social customs. For example, flaming and spamming were always considered "bad form" on the Internet and those who did it were chastised by other members of the Internet community. Just as in real space, cyberspace communities rely on shame and social stigma to enforce cultural norms.

But what role does ethics play in this neat regulatory framework? Lessig apparently includes ethical standards in the broad category he calls "norms," but in our view cultural norms should be segregated from ethical ideals and principles. Cultural norms are nothing more than variable social action guides, completely relative and dependent upon a given social or cultural environment. Their validity depends to some extent on custom, prevalent attitudes, public opinion, and a myriad of other factors. Just as customs differ from country to country, the social customs of cyberspace could be quite different from the customs found in real space. Also, these customs will likely undergo some transformation over time as the Internet continues to evolve.

The fundamental principles of ethics, however, are metanorms; they have universal validity. They remain the same whether we are doing business in Venezuela or interacting in cyberspace. Like cultural norms they are prescriptive, but unlike these norms, they have lasting and durable value because they transcend space and time. Ethics is about (or should be about) intrinsic human goods and the moral choices that realize those goods. Hence the continuity of ethical principles despite the diversity of cultures.

Our assumption that ethics and customs (or cultural norms) must be kept distinct defies the popular notion of ethical relativism, which often equates the two. A full refutation of that viewpoint is beyond the scope of our discussion here. But consider this reflection of the contemporary philosopher Phillippa Foot:

> Granted that it may be wrong to assume identity of aim between people of different cultures; nevertheless there is a great deal all men have in common. All need affection, the cooperation of others, a place in community, and help in trouble. It isn't true to suppose that human beings can flourish without these things—being isolated, despised or embattled, or without courage or hope. We are not, therefore, simply expressing values that we happen to have if we think of some moral systems as good moral systems and others as bad.[4]

None of this by any means invalidates Lessig's framework. His chief insight is that "code and market and norms and law together regulate in cyberspace as architecture and market and norms and law regulate in real space."[5] Also, according to Lessig, "Laws affect the pace of technological change, but the structures of software can do even more to curtail freedom. In the long run the shackles built by programmers could well constrain us more."[6] This notion that private code can be a more potent constraining force than public law has significant implications. The use of code as a surrogate for law may mean that certain public goods or moral values once protected by law will now be ignored or compromised by those who develop or utilize this code. Moreover, there is a danger that government itself will regulate the architectures of cyberspace to make it more controllable. We have already seen this happen in countries like Iran and China. In the hands of the private or public sector the architectures of cyberspace can have extraordinary regulatory power.

Thus, Lessig's model is quite instructive and we rely on it extensively in the pages to come. However, I would argue that the model would be more useful for our purposes if greater attention were given to the role of fixed ethical values as a constraining force. But how do these values fit with the other regulatory forces?

Before we can answer this question we must say something about the nature of those values. The notion that there are transcendent moral values grounded in our common human nature has a deep tradition in the history of philosophy. It is intuitively obvious that there are basic human goods that contribute to human well-being or human flourishing. Although there are several different versions of what these goods might be, they do not necessarily contradict each other. Some versions of the human good are "thin," while others are "thick." James Moor's list of core human goods includes life, happiness, and autonomy. According to Moor, *happiness* is "pleasure and the absence of pain," and *autonomy* includes those goods that we need to complete our projects (ability, security, knowledge, freedom, opportunity, reason). Individuals may rank these values differently but all human beings attribute value to these goods or "they would not survive very long."[7]

Oxford philosopher John Finnis offers a thicker version of the human good. He argues persuasively for the following list of intrinsic goods: life, knowledge, play (and skillful work), aesthetic experience, sociability, religion, and practical reasonableness (which includes autonomy). According to Finnis, participation in these goods allows us to achieve genuine human flourishing. They are opportunities for realizing our full potential as human beings, for being all that we can be. Hence the master principle of morality: one's choices should always be open to *integral human fulfillment*, the fulfillment of all persons and communities. None of our projects or objectives provides sufficient reason for setting aside or ignoring that responsibility.