Cyberethics

This new textbook offers an accessible introduction to the topic of cybersecurity ethics. The book is split into three parts. Part I provides an introduction to the field of ethics, philosophy and philosophy of science, three ethical frameworks – virtue ethics, utilitarian ethics and communitarian ethics – and the notion of ethical hacking. Part II applies these frameworks to particular issues within the field of cybersecurity, including privacy rights, intellectual property and piracy, surveillance, and cyberethics in relation to military affairs. The third part concludes by exploring current codes of ethics used in cybersecurity. The overall aims of the book are to: provide ethical frameworks to aid decision making; present the key ethical issues in relation to computer security; highlight the connection between values and beliefs and the professional code of ethics. The textbook also includes three different features to aid students: 'Going Deeper' provides background information on key individuals and concepts; 'Critical Issues' features contemporary case studies; and 'Applications' examine specific technologies or practices which raise ethical issues. The book will be of much interest to students of cybersecurity, cyberethics, hacking, surveillance studies, ethics and information science.

The federal Bureau of Investigation (FBI) is a national agency dedicated to investigation federal crimes. Founded as a small team of special agents on July 26, 1908, the Bureau was first charged with enforcing the growing body of federal laws covering the United States as a whole. Almost from the beginning of its 100-year history, the Bureau has been the subject of legend and controversy. It has also evolved into a vast and sophisticated national law-enforcement agency. Whether as a federal crime-fighting force or a source of investigative support of local and state police forces, the modern FBI strives to embody its ideals of fidelity, bravery, and integrity. Computers have changed the way people do business, gather information, communicate...and engage in crime. From remote locations in cyber space, criminals can break into a computer and steal valuable information, including credit card and social security numbers, leading to the theft of people's money and identities. Today, the FBI attacks cyber-crime by using sophisticated technology and developing wide-ranging partnerships with companies, academic communities, law enforcement agencies, and concerned individuals-all determined to protect the online community from scam artists, predators, and thieves.

This book of readings is a flexible resource for undergraduate and graduate courses in the evolving fields of computer and Internet ethics. Each selection has been carefully chosen for its timeliness and analytical depth and is written by a well-known expert in the field. The readings are organized to take students from a discussion on ethical frameworks and regulatory issues to a substantial treatment of the four fundamental, interrelated issues of cyberethics: speech, property, privacy, and security. A chapter on professionalism rounds out the selection. This book makes an excellent companion to

CyberEthics: Morality and Law in Cyberspace, Third Edition by providing articles that present both sides of key issues in cyberethics.

Cyber environments have become a fundamental part of educational institutions, causing a need for understanding the impact and general principles of ethical computer use in academia. With the rapid increase in the use of digital technologies in classrooms and workplaces worldwide, it is important that part of the training that takes place for students is how to be good cyber citizens, who are ethical in the decisions that they make and in their interactions with others across digital platforms. Emerging Trends in Cyber Ethics and Education is a pivotal reference source that provides vital research on the application of ethics and education within online environments. While highlighting topics such as computer simulation, corporate e-learning, and plagiarism detection, this publication explores effective ways of utilizing digital landscapes for online education, as well as the methods of improving cyber security frameworks. This book is ideally designed for educators, IT developers, education professionals, education administrators, researchers, and upper-level graduate students seeking current research on secure and educational interactions in digital landscapes.

"This book traces the emergence of the new interdisciplinary field of technoethics by exploring its conceptual development, important issues, and key areas of current research. Compiling 50 authoritative articles from leading researchers on the ethical dimensions of new technologies"--Provided by publisher.

Halbert (legal studies, Temple U.) and Ingulli (business, Richard Stockton College, Pomona, NJ) provide an undergraduate text suitable for any course (economics, sociology, media studies, computer science, etc.) that looks at how cyberspace is affecting culture. They consider major "crunch points" i

"This book introduces the reader to the key concepts and issues that comprise the emerging field of Technoethics, the interdisciplinary field concerned with all ethical aspects of technology within a society shaped by technology"--Provided by publisher.

Cyberethics: Morality and Law in Cyberspace, Seventh Edition provides a comprehensive and up-to-date investigation of the internet's influence on our society and our lives.

This open access book provides the first comprehensive collection of papers that provide an integrative view on cybersecurity. It discusses theories, problems and solutions on the relevant ethical issues involved. This work is sorely needed in a world where cybersecurity has become indispensable to protect trust and confidence in the digital infrastructure whilst respecting fundamental values like equality, fairness, freedom, or privacy. The book has a strong practical focus as it includes case studies outlining ethical issues in cybersecurity and presenting guidelines and other measures to tackle those issues. It is thus not only relevant for academics but also for practitioners in cybersecurity such as providers of security software, governmental CERTs or Chief Security Officers in companies.

Revised and updated to reflect new technologies in the field, the fourth edition of this popular text takes an in-depth look at the social costs and moral problems that have emerged by the ever expanding use of the Internet, and offers up-to-date legal and philosophical examinations of these issues. It focuses heavily on content control, free speech, intellectual property, and security while delving into new areas of blogging and social networking. Case studies throughout discuss real-world events and include coverage of numerous hot topics. In the process of exploring current issues, it identifies legal disputes that will likely set the standard for future cases.Instructor Resouces:-PowerPoint Lecture Outlines

CyberEthics: Morality and Law in Cyberspace, Third Edition takes an in-depth look at the social costs and moral problems that have arisen by the expanded use of the internet, and offers up-to-date legal and philosophical perspectives. The text focuses heavily on content control and free speech, intellectual property, privacy and security, and has added NEW coverage on Blogging. Case studies featured throughout the text offer real-life scenarios and include coverage of numerous hot topics, including the latest decisions on digital music and movie downloads, the latest legal developments on the Children's Internet Protection Act, and other internet governance and regulation updates. In the process of examining these issues, the text identifies some of the legal disputes that will likely become paradigm cases for more complex situations yet to come.

The Asian continent which is composed of tiger and emerging economies, is both a big producer and consumer of computer mediated communication. Research on cyberspace in the Asian context, however, began only after the 1990's when the digital revolution spread outside the West. These initial studies which were largely dependent on Western categories, did not probe into the socio-cultural contexts in which the technologies emerged and have developed. This has changed though in the past years. This anthology hopes to contribute, in particular, to the analysis of the mutually constitutive interaction of the use of cyberspace and Asian cultures, with particular attention to ethical, feminist, and religious perspectives especially within Catholic Christianity. Core themes discussed in the contributors' essays are the democratizing potential of cyberspace, the digital/gender divide, global division of digital/virtual labor, cyber-violence against women, women's resistance as well as collusion with masculinist capitalist interests on the Net, masquerading, just internet relations, how web 2.0 spaces are shaping dynamics of power and authority in the church, cyberspace as sacred time and space, and models of spirituality for the digital era.

What are internal and external Cyberethics relations? When a Cyberethics manager recognizes a problem, what options are available? What potential environmental factors impact the Cyberethics effort? How will we insure seamless interoperability of Cyberethics moving forward? Do the Cyberethics decisions we make today help people and the planet tomorrow? This instant Cyberethics self-assessment will make you the credible Cyberethics domain authority by revealing just what you need to know to be fluent and ready for any Cyberethics challenge. How do I reduce the effort in the Cyberethics work to be done to get problems solved? How can I ensure that plans of action include every Cyberethics task and that every Cyberethics outcome is in place? How will I save time investigating strategic and tactical options and ensuring Cyberethics opportunity costs are low? How can I deliver tailored Cyberethics advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Cyberethics essentials are covered, from every angle: the Cyberethics self-assessment shows succinctly and clearly that what needs to be clarified to organize the business/project activities and processes so that Cyberethics outcomes are achieved. Contains extensive criteria grounded in past and current successful projects and activities by experienced Cyberethics practitioners. Their mastery, combined with the uncommon elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Cyberethics are maximized with professional results. Your purchase includes access details to the Cyberethics self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows your organization exactly what to do next. Your exclusive instant access details can be found in your book.

The penetration of computer technology in society has given rise to new moral dilemmas. The 26 ground-breaking essays in this insightful anthology define the nature of this new moral landscape and offer thoughtful answers to the ethical questions raised by the interaction of people and computers.

In its 4th edition, this book remains focused on increasing public awareness of the nature and motives of cyber vandalism and cybercriminals, the weaknesses inherent in cyberspace infrastructure, and the means available to protect ourselves and our society. This new edition aims to integrate security education and awareness with discussions of morality and ethics. The reader will gain an understanding of how the security of information in general and of computer networks in particular, on which our national critical infrastructure and, indeed, our lives depend, is based squarely on the individuals who build the hardware and design and develop the software that run the networks that store our vital information. Addressing security issues with ever-growing social networks are two new chapters: “Security of Mobile Systems” and “Security in the Cloud Infrastructure.” Instructors considering this book for use in a course may request an examination copy here.

Completely revised and updated, the new fourth edition of this popular text takes an in-depth look at the social costs and moral problems that have arisen by the ever expanded use of the internet, and offers up-to-date legal and philosophical perspectives. It focuses heavily on content control and free speech, intellectual property, privacy and security, and features new content on blogging and social networking. Case studies throughout offer real-life scenarios and include coverage of numerous hot topics. In the process of examinging current issues, the text identifies some of the legal disputes that will likely set the standard for future cases.

Ethics and Technology, 5th Edition, by Herman Tavani introduces students to issues and controversies that comprise the relatively new field of cyberethics. This text examines a wide range of cyberethics issues--from specific issues of moral responsibility that directly affect computer and information technology (IT) professionals to broader social and ethical concerns that affect each of us in our day-to-day lives. The 5th edition shows how modern day controversies created by emerging technologies can be analyzed from the perspective of standard ethical concepts and theories. -- Provided by publisher.

This fully revised and updated fifth edition offers an in-depth and comprehensive examination of the social costs and moral issues emerging from ever-expanding use of the Internet and new information technologies. Focusing heavily on content control, free speech, intellectual property, and security, this book provides legal and philosophical discussions of these critical issues. It includes new sections on Luciano Floridi's macroethics, gatekeepers and search engines, censorship, anti-piracy legislation, patents, and smartphones. Real-life case studies, including all-new examples focusing on Google, Facebook, video games, reader's rights, and the LulzSec Hackers, provide real-world context. --

Following an opening section that defines cyberethics, this anthology of 26 essays explores anonymity, personal identity, and the moral dimensions of creating new personalities; privacy; ownership of intellectual property and copyright law; and the impact of computers on democracy and community. Annotation copyrighted by Book News, Inc., Portland, OR

What are internal and external Cyberethics relations? What is our formula for success in Cyberethics ? What is Cyberethics's impact on utilizing the best solution(s)? How do we go about Comparing Cyberethics approaches/solutions? Will team members regularly document their Cyberethics work? This breakthrough Cyberethics self-assessment will make you the principal Cyberethics domain auditor by revealing just what you need to know to be fluent and ready for any Cyberethics challenge. How do I reduce the effort in the Cyberethics work to be done to get problems solved? How can I ensure that plans of action include every Cyberethics task and that every Cyberethics outcome is in place? How will I save time investigating strategic and tactical options and ensuring Cyberethics costs are low? How can I deliver tailored Cyberethics advice instantly with structured going-forward plans? There's no better guide through these mind-expanding questions than acclaimed best-selling author Gerard Blokdyk. Blokdyk ensures all Cyberethics essentials are covered, from every angle: the Cyberethics self-assessment shows succinctly and clearly that what needs to be clarified to organize the required activities and processes so that Cyberethics outcomes are achieved.

Contains extensive criteria grounded in past and current successful projects and activities by experienced Cyberethics practitioners. Their mastery, combined with the easy elegance of the self-assessment, provides its superior value to you in knowing how to ensure the outcome of any efforts in Cyberethics are maximized with professional results. Your purchase includes access details to the Cyberethics self-assessment dashboard download which gives you your dynamically prioritized projects-ready tool and shows you exactly what to do next. Your exclusive instant access details can be found in your book.

Provides a framework for discussing ethical dilemmas related to today's computer technology and the Internet. This title contains chapters, each of which begins with a case study, based on an actual legal or business scenario. Interdisciplinary readings, questions, and exercises, help students develop a more complete understanding of the material.

Ethical values in computing are essential for understanding and maintaining the relationship between computing professionals and researchers and the users of their applications and programs. While concerns about cyber ethics and cyber law are constantly changing as technology changes, the intersections of cyber ethics and cyber law are still underexplored. Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices discusses the impact of cyber ethics and cyber law on information technologies and society. Featuring current research, theoretical frameworks, and case studies, the book will highlight the ethical and legal practices used in computing technologies, increase the effectiveness of computing students and professionals in applying ethical values and legal statues, and provide insight on ethical and legal discussions of real-world applications.

The Sixth Edition of CyberEthics: Morality and Law in Cyberspace provides a comprehensive examination of the social costs and moral issues emerging from the ever-expanding use of the internet and new information technologies. Focusing heavily on content control, free speech, intellectual property, and security, the sixth edition offers a legal and philosophical discussion of these critical issues.

Rapid technological advancement has given rise to new ethical dilemmas and security threats, while the development of appropriate ethical codes and security measures fail to keep pace, which makes the education of computer users and professionals crucial. The Encyclopedia of Information Ethics and Security is an original, comprehensive reference source on ethical and security issues relating to the latest technologies. Covering a wide range of themes, this valuable reference tool includes topics such as computer crime, information warfare, privacy, surveillance, intellectual property and education. This encyclopedia is a useful tool for students, academics, and professionals.

In today?s globalized world, businesses and governments rely heavily on technology for storing and protecting essential information and data. Despite the benefits that computing systems offer, there remains an assortment of issues and challenges in maintaining the integrity and confidentiality of these databases. As professionals become more dependent cyberspace, there is a need for research on modern strategies and concepts for improving the security and safety of these technologies. Modern Theories and Practices for Cyber Ethics and Security Compliance is a collection of innovative research on the concepts, models, issues, challenges, innovations, and mitigation strategies needed to improve cyber protection. While highlighting topics including database governance, cryptography, and intrusion detection, this book provides guidelines for the protection, safety, and security of business data and national infrastructure from cyber-attacks. It is ideally designed for security analysts, law enforcement, researchers, legal practitioners, policymakers, business professionals, governments, strategists, educators, and students seeking current research on combative solutions for cyber threats and attacks.

Offers a practical guide on cyber ethics that can help students become safe, smart cyber citizens.

Unified Philosophy: Interdisciplinary Metaphysics, Ethics, and Liberal Arts demonstrates how an integrated vision of metaphysics, ethics, and hermeneutics can serve as an underlying philosophy for general education or liberal arts courses and programs. Its unique approach elevates such courses to orientation and reorientation courses and seminars within higher education. The book introduces and reintroduces concepts in philosophy in ethics for students and faculty. It underscores that philosophy is theoretical and applied metaphysics; metaphysics is applied ethics and hermeneutics; and ethics and hermeneutics are applied metaphysics. The opening chapter explores metaphysics: inquiry into reality. It consists of two sections: part and whole; and change and stability. Part and whole involve four positions about reality: part-alone, holistic or limited part, part-whole dualism, or whole-alone. Change and stability also entail four positions about reality: change-alone, holistic or directed change, change-stability dualism, or stability-alone. In turn, each of the eight positions integrates the apparently unrelated languages of game theory, mereology, functions, sets, virtue ethics, phenomenology, cybernetics, and ergonomics/human factors. Chapter One forms the model of which the remaining chapters are applications. The third edition expands Alphonse Chapanis' environment-user interface to four interfaces: environment-environment, environment-person, person-environment, and person-person interfaces. New chapters include Chapter One, Chapter Two, and Chapter Seven. Chapter Two examines positivism through subjectivity spectrum. Chapter Seven examines management reality including authority. Written in recognition of ethics and metaphysics as fundamental components of philosophy and the quest for wisdom, Unified Philosophy is a thought-provoking text for students of theology, ethics, law, medicine, and engineering, education, and city planning/environmental science.

An international journal of theology; a catholic journal in the widest sense: rooted in Roman Catholicism yet open to other

Christian traditions and the worlds faiths. Promotes discussion in the spirit of Vatican II. Annual subscriptions available.
Teenagers in the cyberworld, the subject is worth to be nown by teenagers, parents, and educators, is the theme selected by the writers as the response to the involvement of teenagers in the cyberworld. This book portrays the particular behavior of teenagers while interacting in cyber-society in contrast to the life of traditional society. The discussions are very interesting because what has been done in ‘traditional society’ is transformed into the cyberworld; where computer ability acts as the main vehicle to surf it. Problems endured by teenagers as ‘personal beings’, who are very active in cyberworld, tend to disadvantage themselves. This is proven from the existing cases presented in this book. It is the responsibility of parents and educators as the representation of society to give full attention in creating a better cyberworld for the teenagers. Further, society, in this context represented by parents and educators, should have correct understanding of cyberworld and its impacts towards the lives of teenagers in particular. The discussions in this book are some samples of many Internet contents which related mostly to the life of teenagers in the cyberspace. The topics described inside it based on the recent cases happened and are explained briefly and concisely. Therefore, they are up-to-date as well as educative. Moreover, it is hoped that its presence gives practical values for teenagers, educators, and parents. This book is suitable for teachers, lecturers, and societies as a whole because it illustrates the real problems and their solutions happened in foreign countries and Indonesia as well.

Computer crimes and the invasion of privacy by electronics means are major concerns. They threaten the future of access to information. This book comprehensicely covers these subjects. Chapter one explains both the infrastructure and communication protocols to help in understanding computer crimes. Chapter two addresses the motives for cyber attacks-- personal, pleasure seeking, attention seeking, revenge or even vendetta, financial escapades, and raw hate. Likely targets and security issues in computer augmented settings are discussed in chapter three. Chapter four addresses the costs of computer crimes-- to individuals, to the nation and to businesses. The crime prevention efforts of individuals, civic groups, institutions, nations, and multinational bodies are described in chapter five. Chapter six assesses the future of cyber attacks by looking at the changing technology, access to computers by criminals, and education and crime prevention measures. The mind of the computer hacker is also explored at length.

This collection of papers, articles, and monographs details the ethical landscape as it exists for the distinct areas of Internet and network security, including moral justification of hacker attacks, the ethics behind the freedom of information which contributes to hacking, and the role of the law in policing cyberspace.

In its 4th edition, this book remains focused on increasing public awareness of nature and motives of cyber vandalism, the weaknesses inherent in cyberspace infrastructure, and the means available to protect ourselves and our society. The new addition aims to integrate security education and awareness with morality and ethics. In all, the security of information in general and of computer networks in particular, on which our national critical infrastructure and, indeed, our lives depend, is based squarely on the individuals who build the hardware and design and develop the software that run the networks that store our vital information. Addressing security issues with ever-growing social networks are two new chapters: "Security of Mobile Systems" and "Security in the Cloud Infrastructure."

A primer on legal issues relating to cyberspace, this textbook introduces business, policy and ethical considerations raised by our use of information technology. With a focus on the most significant issues impacting internet users and businesses in the United States of America, the book provides coverage of key topics such as social media, online privacy, artificial intelligence and cybercrime as well as emerging themes such as doxing, ransomware, revenge porn, data-mining, e-sports and fake news. The authors, experienced in journalism, technology and legal practice, provide readers with expert insights into the nuts and bolts of cyber law. Cyber Law and Ethics: Regulation of the Connected World provides a practical presentation of legal principles, and is essential reading for non-specialist students dealing with the intersection of the internet and the law.

Ethics and Technology, 5th Edition, by Herman Tavani introduces students to issues and controversies that comprise the relatively new field of cyberethics. This text examines a wide range of cyberethics issues - from specific issues of moral responsibility that directly affect computer and information technology (IT) professionals to broader social and ethical concerns that affect each of us in our day-to-day lives. The 5th edition shows how modern day controversies created by emerging technologies can be analyzed from the perspective of standard ethical concepts and theories.

Offering insights and coverage of the field of cyberethics, this book introduces readers to issues in computer ethics. The author combines his years of experience in the field with coverage of concepts and real-world case studies.

This anthology hopes to contribute, in particular, to the analysis of the mutually constitutive interaction of the use of cyberspace and Asian cultures, with particular attention to ethical, feminist, and religious perspectives especially within Catholic Christianity.