GLOBAL INFORMATION TECHNOLOGIES

ETHICS AND THE LAW

Second Edition

THOMAS H. KOENIG
PROFESSOR EMERITUS OF SOCIOLOGY
NORTHEASTERN UNIVERSITY

MICHAEL L. RUSTAD
THOMAS F. LAMBERT PROFESSOR OF LAW AND CO-DIRECTOR
INTELLECTUAL PROPERTY LAW CONCENTRATION
SUFFOLK UNIVERSITY LAW SCHOOL

WEST ACADEMIC PUBLISHING

860 Blue Gentian Road, Suite 350
Eagan, MN 55121
1-877-888-1330

Printed in the United States of America

ISBN: 978-1-68561-570-3

Preface

This book explains the most critical ethical, social, and legal issues arising from advances in computer technology. The chapters apply law and ethical principles to information technology contracts, Internet torts, cybercrimes, global information privacy, global patents, copyrights, trademarks and trade secrets. Both of us have taught, published and consulted in this field for decades.

This textbook is appropriate for law school classes in computer law, Internet Law and Introduction to U.S. Law classes for international students. This book can also be assigned in computers and society courses in social science departments. Business school professors can adopt this text for courses in computers and business or electives in computer ethics.

We frequently receive telephone calls or emails from individuals and businesses, seeking practical advice about computer ethics or legal issues such as the following: "My daughter has a learning disability and is being bullied on a social media site. What can I do about it?" "When is copying software illegal?" "What should I do if get a copyright infringement notice?" "Our business computer system has been locked by people who are demanding payment in Bitcoin to unencrypt it. Should I call the local police or the FBI? Should I pay the ransom?"

Legal and ethical issues arise out of all-too-common, deeply troubling privacy violations. "A mortifying picture of me has been posted on a revenge porn website by an ex-lover. The website owner and owner of the domain name will not remove it. Does the website have a legal duty to take down posts violating my privacy? Can I force them?" "An ex-boyfriend is posting menacing rap lyrics that reference the breakup of our relationship on Snapchat. I am scared. Should I report it to Snapchat and how should I document the post?" "Is my business liable for misappropriation of a customer's trade secrets if our computer system enabled the intrusion by failing to employ adequate security?"

Workplace ethical and legal quandaries often arise out of Internet misuse and abuse. "I work in IT and my boss demands that I set up monitoring software that secretly records and stores all keyboard strokes for all employees. Can I refuse to install this software, which secretly invades workers' privacy? If my employer terminates me for refusing to comply with his demand, do I have legal recourse?"

"Some of the workers are forwarding inappropriate jokes through our email system. Can they be fired for distributing these offensive jokes on our company

computer system?" "My employer is just about to release poorly tested software into the marketplace. Many of our customers are health care facilities so the software has a high probability of compromising medical information and third-party data. How secure does a computer program need to be and what are my responsibilities if our computer security falls short of industry standards for health care providers?"

Disputes over one-sided computer clauses such as warranty disclaimers, caps on damages and predispute arbitration clauses create further ethical and legal difficulties. "My company just added language to the terms of service agreement of their website that gives it the right to terminate employees or customers who post anything negative about the company. Is this an enforceable provision?"

Increasingly, we are asked about how to use intellectual property to protect software, websites and other intangible information assets. "I have invented a new software application that I believe can be very profitable. How do I protect it?" "Can I prevent someone from using my trademark in his or her domain name?" "What is the process by which I can get patent protection for my newly developed software application?"

Why the Intersection of Computer Ethics & the Law?

Daily headlines describe high-stakes conflicts over disruptive information technologies. The rapidly evolving ethical dilemmas arising from the Internet of Things (IoT), which refers to things connected to the Internet, illustrates the increasing need for developing clearer legal and moral rules. 'Smart Mobiles, smart refrigerators, smartwatches, smart fire alarms, smart door locks, smart bicycles, medical sensors, fitness trackers, smart security system, etc., are few examples of IoT products."[1] Internet connected devices, artificial intelligence and surveillance applications are reshaping business models, digital intelligence, and daily life.

Prior to the development of the Internet and the World Wide Web, computer science departments did not teach courses on computer ethics. Today, however, in addition to an understanding of software architecture, coding and design, computer professionals are expected to play a significant role in avoiding legal liabilities and ethical lapses. Rapidly evolving information technologies require computer professionals—and their attorneys—to be highly imaginative and extremely flexible.

This book introduces computer law and ethical dilemmas in an applied format, using concrete legal issues, regulatory actions and court decisions to illustrate the global consequences of unethical computing. Practitioners who are

not reflective and who take the approach that they should only "do what they are told" will not serve their clients well. They may expose themselves and their employers to professional malpractice for their failure to comply with ethics or the law:

> In fact, unethical behavior of an employee can be very serious for a company and can be cause for dismissal. In order to understand professional and ethical behavior, it is necessary to go beyond an understanding of personal morality. You need to understand the kinds of situations that can and frequently do occur in the conduct of business that can have a serious negative impact on companies and their employees if these situations are not handled correctly.[2]

Each chapter considers how other countries, particularly the twenty-seven nations of the European Union, evaluate and resolve these issues. App developers marketing their product in Europe must comply with European Union (EU) privacy regulations such as the General Data Protection Regulation and the EU/USA Privacy Shield that governs data transfers outside the European Union. The European Commission has filed actions against Facebook, Google, Microsoft, Twitter and many other U.S. companies that did not adequately revise their contracting practices for the European consumer market.

Students who view computer science as an exclusively technical field are missing the big picture. Apple's career page, for example, boasts:

> For everything we create, we consider its impact—on our customers, our colleagues, and our planet. The same innovation that goes into making our products goes into taking on issues we care about deeply, such as accessibility, equity, privacy, and the environment. Everyone joins Apple for a reason. Often it's because they found a company that aligns with their own values.[3]

"Developers are often natural problem solvers who possess strong analytical skills and the ability to think outside the box,"[4] but more is required to reach the top ranks of the profession. Computer science accreditors require that programs help students gain "an understanding of professional, ethical, legal, security and social issues and responsibilities."[5]

Computer science degrees that are accredited by the Accreditation Board for Engineering and Technology (ABET) require students to have training in the ethical aspects of computing. For example, for Student Outcome (4) of the Computing Accreditation Commission (CAC), a part of ABET accreditation standards for computer science programs, states that "the Graduates of the

program will have an ability to: 'Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.' "[6]

The Accreditation Board of Engineering and Technology, which accredits Engineering, Computer Science, and Information Systems educational programs, specifies six essential skills that are often imperative to career success. These non-technical qualifications include:

(1) The ability to communicate effectively.

(2) The ability to understand professional, ethical responsibility.

(3) The ability to function on multi-disciplinary teams.

(4) Broad education necessary to understand the impact of engineering solutions in a global and societal context.

(5) Recognition of the need for, and an ability to engage in, life-long learning.

(6) Knowledge of contemporary issues.[7]

Computer forensics provides an example of a high-demand, fast-growing field that requires a cross-disciplinary approach.[8] These professionals need a basic knowledge of criminal statutes, cybercrime fighting techniques and a familiarity with hacker culture as well as high-level programming skills. Digital forensics experts uncover "smoking gun" evidence of cybercrimes such as trade secret theft, computer system intrusions and insider hackings. These experts catch cybercriminals threatening U.S. companies and national security.

Firms on the cutting edge of technology are devising new methods of bypassing traditional recruiting channels to locate employees who are skilled, imaginative and self-motivated. AI programs increasing screen potential employees. Google famously experimented with using brainteasers that required applicants to show that they were imaginative and resourceful, but this method of testing applicants was abandoned several years ago.

A Georgia Tech graduate reports that he was recruited through a Google search that he initiated:

> One morning, while working on a project, I Googled "python lambda function list comprehension." The familiar blue links appeared, and I started to look for the most relevant one. But then something unusual happened. The search results split and folded back to reveal a box that said "You're speaking our language. Up for a challenge?" I stared at the

> screen. What? After a moment, I decided yes, I was most definitely up for a challenge. I clicked through and landed on a page that called itself "foo.bar." The page resembled a UNIX interface, so I typed the command to see the list of files. There was a single one called "start_here.txt." I opened it and saw two sentences:
>
> *"Type request to request a challenge. Type help for a list of commands."*
>
> I typed "request" and half expected to see "Follow the white rabbit, Max." Instead, the screen displayed a paragraph outlining a programming challenge and gave instructions on how to submit my solution. I had 48 hours to solve it, and the timer was ticking.[9]

The recent graduate was intrigued by the task and solved the problem for fun:

> I set to work and solved the first problem in a couple hours. Each time I submitted a solution, foo.bar tested my code against five hidden test cases. Once my solution passed all of those tests, I could submit it and request a new challenge. Over the next two weeks, I solved five more problems. After I solved the sixth problem, foo.bar gave me the option to submit my contact information. I typed in my phone number and email address, fully expecting that to be the end of things. Much to my surprise, a recruiter emailed me a couple days later asking for a copy of my resume. I emailed it to him, and we set up a phone call. Overall, I enjoyed the puzzles that they gave me to solve, and I'm excited for my first day as a Googler.[10]

Similarly, Apple has attempted to bypass traditional hiring channels through innovative tactics such as placing covert job advertisements where skilled and imaginative programmers are likely to run across them.[11] Energy, aptitude and inquisitiveness are important qualifications in addition to paper credentials by computer companies at the forefront of the IT revolution.

State-of-the-art information technology companies are aware that they need employees who keep pace with the rapidly evolving digital environment. Innovative computer professionals who can learn from diverse fields, including the liberal arts, and who are intrigued by other cultures, will be competitive in an increasingly globalized field. Even small, highly specialized technology start-ups need to implement funding, employment and hiring practices that comply with the highest ethical standards and the law.

Computer professionals need to know how to protect their company's legal rights and avoid protecting the rights of others. Cybertort liability may result from

entangling your organization too closely with third party content that creates liability for the wrongdoing of others. Even if a company has its own corporate counsel, computer professionals need to know when to recognize potential legal exposures before a risk evolves into a full-blown catastrophe.

Many of the costly and time-consuming lawsuits discussed in this book could have been avoided through preventive law. Intellectual property, such as trademarks, copyrights, patents and trade secrets must be protected, while avoiding infringing the rights of others. Computer professionals need to know when they must consult with legal counsel to prevent problems dealing with software licensing, data protection, tax law, securities regulation, products liability, environmental law, financial services, patent infringement, discrimination complaints and other specialized workplace regulations, where there are often national law differences. This book gives the computer professional guidance on all of these issues.

Privacy issues will become even more significant as Internet of Things devices harvest, process, and share personal information. Should insurance policyholders waive their privacy rights in return for the benefits of insurers collecting data about their activities? What security systems are sufficient to prevent paparazzi from spying on celebrities through Internet connected devices?

Should electronic agents using blockchain technology be able to form legally enforceable "smart contracts"?[12] Electronic payment systems will compile extensive data about your financial behavior. Who will have access to this valuable information? Is consumer consent required for third parties to access this personally identifiable information?

The GE Profile Series French-Door Refrigerator can be Wi-Fi enabled "so after you download the app you can adjust settings, preheat water for coffee and get alerts if the door is open. It works with Amazon Echo, too. Smart refrigerators connected to the Internet via Wi-Fi often with a large touchscreen interface."[13] The consumer can "interact with your fridge from your smartphone or tablet. Some smart refrigerators can even communicate with other smart devices in your home, such as speakers, TVs, dishwashers, and microwaves."[14] Smart refrigerators enable the consumer to "view a live feed from the interior camera while you're grocery shopping to see if you need milk, eggs, or other essentials."[15]

Issues of information privacy are raised by such useful machines. Will these appliances be permitted to transfer information on eating habits to the consumer's physician, health insurer, spouse, grocery provider or other specified parties?

Samsung's Family Hub Refrigerator, for example, is a kitchen command center where a consumer:

> can use the screen to draw, leave messages, share pictures, sync calendars and even check who's at your front door or adjust your thermometer with compatible smart devices. You can also use it to stream music or television shows while you're cooking. When you're not home, you can peek inside to see what you need from the supermarket, or, while you are home, you can use it to browse recipes and even order the groceries you need right from the door. Plus, Alexa's built into it so you can operate many of the apps without touching the screen. Our littlest testers (ages five and under) confirmed that the screen is highly responsive and fun to draw on, while our previous tests confirmed that the brand is great at maintaining super steady temperatures, which is a must to keep foods fresh.[16]

The determination of who has access to data documenting a consumer's late night raids of the refrigerator raises legal and ethical dilemmas. Advertisers would pay well for such information. A property owner may be interested in IoT data to assess the number and behaviors of the apartment's tenants.

New forms of targeted advertising are evolving as smart devices compile and integrate information from a wide variety of sources. In a famous example, software began directing advertisements for pregnancy products to a woman before she even realized that she was pregnant. Are we entering an era in which traditional notions of privacy become obsolete?

Can your probation officer use big data to monitor your behavior? New Jersey police are being sued by a public defender's office and a newspaper for using a decade old mandatory blood draw from a new-born to bolster a sexual assault case against the father.[17] Is this an illegal search or just high quality law enforcement?

Will law enforcement be permitted to view personal information to document plans to receive an abortion in a neighboring state?[18] The search engine, Mozilla, questions the privacy protections of most reproductive health tracking devices in the wake of the recent Supreme Court decision overturning *Rowe v. Wade*. Mozilla concluded that eighteen of the top twenty-five reproductive health apps have opaque policies about sharing information with law enforcement agencies:

> "Overnight, apps and devices that millions of people trust have the potential to be used to prosecute people seeking abortions," Ashley

> Boyd, Mozilla's vice president of advocacy, said in a 2022 statement: "Our research confirms that users should think twice before using most reproductive health apps."[19]

Computing's worldwide impact on daily life requires an assessment of its complex impact on diverse stakeholders. Globalized Internet communications lead to increased international understanding and harmonization, but also engender new forms of crime, oppression and social friction. An information technology company doing business in Sweden, Brazil, Malaysia and South Africa must comply with cultural, ethical and legal norms in each of these countries.

Requirements to store information such as users' social media posts, private messages and online articles threatens freedom of expression:

> A record number of governments prosecuted users for nonviolent political, social, and religious posts in 2019, signaling a greater willingness and capacity to target individuals for their online expression. An increase in data localization would likely exacerbate this trend by providing authorities with a more extensive dataset of the populations' written opinions.[20]

Commentators call for international limitations on some cyberspace freedoms to undermine cybercriminals, deter mass tax evasion, prevent state-sponsored espionage and foil international terrorists, while others argue that online free expression is an inalienable human right. Will hate groups be allowed to incite religious strife through postings depicting the mass burnings of copies of the Qur'an; an action protected under the First Amendment of the U.S. Constitution, but that also is likely to cause significant harm to American interests throughout the Middle East? The United Nations is concerned about the increasing use of the Internet for terroristic purposes.

Social media websites, such as Twitter, have implemented "report buttons," allowing users to alert monitors to objectionable postings. Some users have objected to this, contending that it violates freedom of expression and robust discussion.[21] Donald Trump has launched his own social media platform, Truth Social, declaring "I created Truth Social. . . to stand up to the tyranny of big tech. . . . We live in a world where the Taliban has a huge presence on Twitter yet your favourite [sic] American president has been silenced."[22]

Facebook replaced its trending news topics curators with "objective" algorithms because of complaints that conservative media was being screened out.[23] However, eliminating human judgment led to an explosion of fake news stories, which now is being countered by linking these stories to fact-checking

organizations. This book is designed to provide conceptual tools and insights to help future leaders approach such inevitable dilemmas in a systematic and principled way.

How This Book Teaches About Law & Ethics

Each chapter of this book considers emerging predicaments of the information age, such as whether individuals should have the right to erase demeaning postings, whether copyright law should protect tweets, how much cybersecurity should be required for cloud computing and how the ownership of software is established. Workplace rights, cybercrimes, Internet security, civil lawsuits, intellectual property rights, Internet-enabled devices, online privacy and social media terms of use are among the rapidly evolving issues addressed.

The global focus of this book is one of its strongest features. Computer professionals, and the lawyers that represent them, must stop being U.S. centric in activities such as website design, competition law and cross-border data transfers to avoid legal trouble. Both European Union and Chinese law, for example, provide consumers with mandatory rights that are not available to U.S. website users.

In September 2022, South Korea levied large fines against both Google ($50 million) and Meta ($2 million) because these companies "did not clearly inform users or obtain their consent as they collected information about their online activities when they used other websites and apps outside their own platforms."[24] Two weeks earlier, Instagram was fined €403 million by European Union regulators for failing to properly protect the privacy of children.[25]

At the end of each chapter, there are practical problems operationalizing legal and ethical issues such as the protection of personal data, preventing cybercrime, avoiding cybertort liability, implementing reasonable security, adapting electronic contracting and protecting intellectual property rights. As these questions describe real world legal struggles, rather than abstract hypotheticals, students can look online for the most recent developments in similar disputes. Our overall goal is for students to learn to apply the principles of moral and legal reasoning to concrete problems arising from digital technologies.

Computer scientists are the architects of the Internet, designing new applications and implementing operations on a global basis. Every chapter of this book stresses the need to develop a personal sense of right and wrong and an understanding of what laws, if any, punish unethical online behavior. Medical doctors and U.S. attorneys have formal codes of enforceable ethics, which practitioners must follow or be subject to professional discipline. A computer

scientist, in contrast, cannot lose their license for violating a standard of care or be disbarred for ethical lapses.

At the end of each chapter there are practical problems that operationalize legal and ethical issues in context. As these examples describe real world legal struggles, rather than abstract hypotheticals, students can look online for the most recent developments in similar disputes. Our overall goal is for students to learn to apply the principles of moral and legal reasoning to concrete problems arising from digital technologies.

Roadmap of the Chapters

Chapter 1: Basic Concepts in Computer Ethics & the Law

Chapter 1 demonstrates that studying the intersection of law and ethics is the most practical approach to studying Computer Ethics. Nearly every ethical lapse raises the specter of litigation. This chapter introduces the concept of professionalization, describing the Association for Computing Machinery's (ACM) Code of Ethics and Professional Conduct and other proposed ethical guidelines in depth. The ACM Code of Ethics will be applied in a globalized setting in subsequent chapters.

Computer professionals need to anticipate and help resolve legal dilemmas resulting from the interaction between technological developments and new market conditions.[26] At the upper branches of the information technology field, computer experts are working with legislators and regulators in testifying about the new ethical and legal issues raised by the ubiquitous applications of novel information technologies. Computer professionals often take the initiative in advocating for new legal rules on topics such as enhanced database security and more effective intellectual property protection.

Chapter 2: Applying Ethical Perspectives and the Law

Laws, both in the U.S. and globally, draw heavily from moral underpinnings. Chapter 2 provides a summary of the five principal ethical perspectives used to analyze and resolve the many ethical dilemmas raised by emerging information and communications technologies. These five perspectives are: (1) Consequentialism; (2) Virtue and Duty Ethics; (3) Conflict Perspectives; (4) Social Contract Theory; and (5) Libertarianism. We focus on identifying the greatest strengths of each philosophical approach and how these perspectives are embodied in both technology law and personal moral codes.

Resolving ethical questions requires a balancing of costs and benefits of different courses of action. The Ryan Haight Online Pharmacy Consumer

Protection Act of 2008, for example, prohibits Internet medical consultations from supplying controlled prescription drugs. The U.S. Attorney for Florida successfully prosecuted the leader of an online pharmacy that illegally distributed hundreds of thousands of narcotic and other prescription pills.

The great benefit of online pharmacies is their convenience and lower costs for consumers, which must be balanced against potential dangers to the public's health. The U.S. Department of Justice has sanctioned several online pharmacies for selling fraudulent COVID-19 products.[27] Each subsequent chapter applies the five ethical perspectives introduced in this chapter to such substantive dilemmas.

Chapter 3: Cybertorts for the Information Age

Chapter 3 emphasizes the role of private litigation in supplementing criminal law. Many cybertorts parallel civil actions in the brick-and-mortar world, but often contain a digital twist. A company or individual, for example, may be held liable for defamation after publishing or repeating false accusations in a blog, a tweet or a website posting. However, newspapers are held to a higher standard than websites in some situations because, under the Communications Decency Act, websites are immunized from any legal responsibility for third party postings.

Because of gaps in the criminal law and inadequate enforcement mechanisms, cyberspace injuries resulting from revenge pornography, online stalking, dark-side hackings and other socially harmful behavior would go unpunished if it were not for the tort system. Punitive damages are an example of a cybertort remedy that punishes and deters these types of malicious misconduct on the Internet.

This cybertort chapter is organized around the three branches of tort law: (1) Intentional Torts, (2) Negligence, and (3) Strict Liability. Intentional cybertorts were the first to develop and dominate the Internet legal landscape. The tort of outrage is often deployed against online stalkers and egregious postings. Negligent cybertorts are beginning to deal with lapses by web designers and substandard cybersecurity. Strict liability is in an early stage of evolving to address injuries from defective software such as crashes caused by poorly programed self-driving vehicles.

Chapter 4: Cybercrimes: Ethics and the Law

Chapter 4 reviews extant criminal law statutes deployed against cybercrimes such as the Computer Fraud and Abuse Act (computer trespass statute), the Electronic Communications Privacy Act (federal wiretap act) and the Economic Espionage Act. Computer professionals need to be able to recognize if a crime has been committed and know which law enforcement authorities to contact,

especially when dealing with cross-border law breaking. Preventing insider crimes requires monitoring of employee access to sensitive information.

This chapter, like all the others, discusses global developments, which include attempts to coordinate international enforcement through the Cybercrime Convention. New statutes and criminal justice techniques are emerging to deter and punish international cybercriminals and state-sponsored spies. Whether to enforce online enablement of "crimes without victims," such as carrying transparently coded advertisements for prostitution, is controversial because of sharp divergences between the major ethical perspectives about morality laws. Finally, Chapter 4 discusses the controversy over when to reveal confidential information in order to protect the public.

Chapter 5: Information Privacy

What does the right to be left alone mean in a world when we are connected to the Internet 24/7? Teens and young adults are increasingly "living their lives as if in a fishbowl." Chapter 5 contrasts the U.S. piecemeal privacy approach to the European Union's treatment of privacy as a fundamental right. Questions such as whether the U.S. should adopt Europe's "right to be forgotten" or maintain its current marketplace approach to online privacy are being fought out in state and federal legislatures. In February 2016, the EU and the U.S. agreed to a temporary Privacy Shield, which requires U.S. companies to self-certify that data entrusted to them is secure.

Web security, anonymity, censorship, human-computer interactions and many other Internet topics raise troublesome privacy-related issues. Should the FBI be able to order Apple to create a means to decrypt iPhone messages? When can stingrays be used to capture personal communications? When can cell phones of criminal suspects be searched without a warrant?

Chapter 6: Information Technology Contracts

Chapter 6 contrasts U.S. and European consumer contract rules. The enforceability of sales, leases and licenses used in the information-based economy differ dramatically between these two legal systems. U.S. consumers are frequently surprised to discover that when they clicked "yes" to a hyperlink they may have waived their right to a jury trial or to join a class action and can be forced to arbitrate disputes in distant venues. European consumer law, in contrast, prohibits anti-class action waivers, predispute forced arbitration, disclaimers of warranties and caps on damages.

The chapter examines the major contracting forms used in the information-based economy: sales, leases and licenses. The First Sale Rule gives purchasers

control over any product that they buy. For this reason, software is licensed rather than sold so computer companies can control the use of their applications after delivery to their customers. Licenses protect intellectual property by using contract law to prevent unauthorized distribution and copying.

Chapter 7: Patents, Copyrights & Computers

Chapter 7 applies legal and ethical perspectives to disputes over the best balance between the rights of intellectual property owners and the larger public interest. This chapter focuses on the two purely federal branches of intellectual property law: patents and copyrights. The U.S. patent system has been significantly revised by the passage of the America Invents Act of 2011. Similarly, federal copyright law has been significantly updated for the digital age.

Topics such as the patenting and copyrighting of software, the rights of employers to control code written by consultants and other employees, and the operation of the free software movement are examined. European statutory and case law developments covering topics such as moral rights, database protection and secondary infringement are compared to recent U.S. legal developments.

Chapter 8: Trademarks, Trade Secrets & Computers

Chapter 8 examines the ethical and legal issues underlying trademark and trade secret protection. Software publishers seek trademark protection for their logos, trade names, products and even their websites. The trademarks of Apple, IBM, Google and Microsoft need to be aggressively defended to prevent them from losing their legal protection by becoming everyday words, as happened to former trademarks such as "zipper" or "thermos."

Software companies use trade secrets to protect their source code, customer lists and other intangible assets that have an economic value if kept secret. High tech companies generally require their employees, joint venture partners, consultants and others to sign nondisclosure agreements to protect their secrets. Increasingly, the U.S. is including trade secret protection in international trade treaties such as TRIPS and NAFTA. In late 2016, Congress enacted the Defend Trade Secrets Act that gives trade secret owners a private remedy under the federal Economic Espionage Act.

About Us: Why We Wrote This Book

Both authors of this book have had a longstanding interest in ethical computing issues for more than four decades. When we first started working with computers in the early 1970s, keypunch cards were physically fed into a card reader. Mainframe computers were so heavy that they had to be kept in basements

so that they would not crash through the floor. Tom Koenig was an undergraduate student at the University of California, Santa Cruz, which was just beginning to be impacted by the emergence of what would later be labeled Silicon Valley.

Computer access was so expensive that every program needed to specify a maximum amount of run time because a mistake would result in an "infinite loop" that would burn up the employers' annual budget. Software came pre-installed as part of the computer system, which was leased from a few large suppliers such as IBM and Hewlett-Packard. System crashes were generally attributed to hardware failures, such as a burned-out component, rather than defective software. We were college sophomores in December 1968 when IBM made the monumental decision to unbundle software from hardware, which led to the emergence of an independent software industry.

Tom Koenig did his Ph.D. work at the University of California, Santa Barbara, where he studied under the guidance of the former head of the University of Michigan's Institute for Social Research's computer center. The late Professor John Sonquist, his mentor and dissertation chair, was a Quaker pacifist who was deeply distressed by the irony that the software code he had designed was deployed to guide intercontinental nuclear missiles. One of Professor Sonquist's major priorities was to make the ARPANET, the predecessor to the Internet, a mechanism to democratize information rather than to increase the centralized power of the military-industrial complex.

In 1969, UCLA's Network Measurement Center, Stanford's Research Institute (SRI) and the Universities of Utah and California, Santa Barbara established the first nodes for what would later be called the Internet.[28] While at Santa Barbara, Tom was one of the first sociologists to access the ARAPANET, which was "slow, sluggish, and unreliable."[29] Remote connections were made through telephone modems, which would erase unsaved work whenever there was a glitch in the telephone line. During this era, there were no online "browsers." The term was applied to impoverished students who might browse books in bookstores to save money.

Tom's dissertation modified a networking program to examine how interlocking directorships among the 500 largest U.S. corporations correlated with their financial and political policies. His teaching career took him to Brown University in the mid-1970s and then to Boston's Northeastern University. Tom studied computer law as a Fellow at Harvard Law School and later taught computer policy as a Fulbright Scholar at the University of Belgrade Law School in Serbia. Tom has placed many of his Northeastern University students in a variety of high technology firms.

Michael Rustad's first position after completing his master's degree in Sociology was in the Computer Information and Systems Division of the National Institute of Education (NIE) in 1973. Like the University of California, NIE used mainframe computers weighing many tons and contained thousands of vacuum tubes. When Michael moved to Massachusetts in 1978 to begin his Ph.D. program, his first job was at a startup called Optimum Computers in Auburndale, Massachusetts.

During his time at Optimum Computers, there were no sophisticated software applications or personal computers. Michael wrote some of the first user manuals for computer-based statistics with Sheldon Laube, who later became the first CIO of Innovation at PricewaterhouseCooper. Laube was ranked as one of the twenty-five most influential pioneers of Silicon Valley after founding "USWeb which was the world's largest Internet consulting firm during the Internet boom. That company grew from five people to 2,500 in more than 23 countries in fewer than 25 months."[30]

Michael completed his Ph.D. thesis and first book, *Women in Khaki: A Study of the American Enlisted Woman*, on an IBM Selectric typewriter. This IBM typewriter was then state of the art, although it had no spell-check or word processing capabilities. He used "white-out," a small bottle of white paint, to cover up typing errors. He did not use a personal computer until 1985 when Charles Nesson, his LL.M. advisor at Harvard Law School, suggested that he invest in one. Professor Rustad taught one of the first computer law courses at an East Coast law school, beginning in 1993.

Our goal in writing this book is to produce the first text that focuses on the intersection between computer ethics and the law in a globalized setting. The book provides compelling examples from the European Union, China, the former Russian Republics and other countries. Computer professionals need to comply with the legal system in every country where they render services.

Class Activities: Note for Instructors

Both of us favor an active and participatory teaching style, requiring students to give oral presentations and to participate actively in classroom group exercises. We have designed interesting and provocative end-of-chapter exercises that can be used for class discussion, take-home assignments, or in-class presentations. Professor Rustad finds that these exercises work well when they are pre-assigned to students who are on-call to be experts on particular questions. Professor Koenig often divided his class into research groups who were each responsible for presenting reports that explained specialized issues.

Michael Rustad preassigns two law students to represent the plaintiff and defendant in featured cases, giving each team ten minutes to do a closing argument. The rest of the class is assigned as jurors who will deliberate briefly and announce a verdict. He also does a debriefing, asking jurors about what arguments were (or were not) persuasive.

We both find these exercises raise the level of class discussion and that students enjoy debating these contentious topics. Students who use these materials become more enthusiastic about understanding computer law, both to chart an ethical path and to avoid legal troubles when they become computer industry professionals.

This book presents a snapshot of a complex and rapidly changing field. We have tried to be as timely as possible and would greatly appreciate your feedback. Professors adopting this book can email either of us for access to a website where we update cases, discuss technological and legal developments, and do our best to keep the information in this book exciting and contemporary. Our website also contains ideas for examination questions, tips for teaching, PowerPoints, as well as links to interesting articles and legal developments. Whether you are a new instructor or an experienced professor, we would like to work with you to make adopting this book a great experience.

Acknowledgments to the Second Edition

We would like to give special thanks to Suffolk University Law School Librarian and Professor Richard Buckingham for his ongoing support of this edition. Librarian Diane D'Angelo's research and insightful comments have been extremely valuable. Research assistants Ivette Cuenod Lorenzo and Layth H. Hert provided very helpful research, proofreading and editorial suggestions. Finally, we would like to acknowledge the support of Suffolk University Law School Deans Andrew Perlman, Rebecca Curtin, and Pat Shin for this edition. Professor Rustad would like to thank his wife Chryss Knowles for her editing and insightful suggestions.

Thomas H. Koenig
Michael L. Rustad

January 15, 2023

---

1 *18 Most Popular IoT Devices in 2022 (Only Noteworthy IoT Products)*, SOFTWARE TESTING HELP (Oct. 25, 2022).

2 University of Maryland, Baltimore, *What Do Graduates of Engineering, Computer Science, and Information Systems Programs Need to Know Beyond Their Technical Courses?* (2016).

3 CAREERS AT APPLE, https://www.apple.com/careers/us/index.html.

4 U.S. NEWS & WORLD REPORT, *Software Developer Overview: #2 in Best Technology Job* (2016).

[5] Accreditation Board of Engineering and Technology (ABET), *Criteria for Accrediting Computing Programs*, 2016–2017.

[6] Matthew Hertz & Atri Rudra, *Teaching Responsible Computing Playbook Accreditation and Ethics* (2022).

[7] University of Maryland, Baltimore, *What Do Graduates of Engineering, Computer Science, and Information Systems Programs Need to Know Beyond Their Technical Courses?* (2016).

[8] Computer Science Degree Hub, *Can I Get a Job in Forensics with a Computer Science Degree?* (2022).

[9] Max Rosett, *Google Has a Secret Interview Process. . . And It Landed Me a Job* (Aug. 24, 2015).

[10] *Id.*

[11] Kif Leswing, *Apple Hid a Job Listing on Its Website That You Need Serious Computer Skills to Find*, Business Insider (Aug. 19, 2017).

[12] Jake Epstein and Haven Orecchio-Egresitz, *Police Used a NJ Baby's Mandatory Blood Sample to Pursue a Criminal Case. Public Defenders and a Newspaper Are Now Teaming Up to Sue Over Privacy Concerns*, INSIDER (Aug. 16, 2022).

[13] Nicole Papantoniou & Betty Gold, *Best Refrigerators to Buy in 2022, According to Kitchen Appliance Experts,* GOOD HOUSEKEEPING REVIEWS, (July 6, 2022).

[14] *What a Smart Refrigerator Could Do for Your Kitchen*, MR. APPLIANCE (Nov. 5, 2019).

[15] *Id.*

[16] *Id.*

[17] Jake Epstein & Haven Orecchio-Egresitz, *Police Used a NJ Baby's Mandatory Blood Sample to Pursue a Criminal Case. Public Defenders and a Newspaper Are Now Teaming Up to Sue Over Privacy Concerns*, MSN (Aug. 16, 2022).

[18] Debra Cassens Weiss, *Mom Is Charged with Aiding Daughter's Illegal Abortion After Prosecution Obtains Facebook Messages*, ABA JOURNAL (Aug. 12, 2022).

[19] Jordan Parker Erb, *Mozilla Slaps 18 Period and Pregnancy Tracking Apps and Devices with a 'Privacy Not Included' Warning Label*, INSIDER (Aug. 17, 2022).

[20] Adrian Shahbaz & Allie Funk, *Special Report 2020: User Privacy or Cyber Sovereignty?*, FREEDOM HOUSE (2020).

[21] *Twitter Adds In-Tweet "Report" Button After Cyber Threats*, MASHABLE (Aug. 1, 2013).

[22] James Clayton, *Trump's Truth Social app branded a disaster,* BBC NEWS (Apr. 4, 2022).

[23] Emily Schultheis, Top Senate Republican Calls on Facebook to Respond to Censorship Accusations, CBS News (May 10, 2016).

[24] *South Korea Issues Google and Meta Largest Ever Privacy Fines*, ALM LAW.COM (Sept. 15, 2022).

[25] Natasha Lomas, *Instagram Fined €405M in EU Over Children's Privacy*, TECHCRUNCH (Sept. 2, 2022).

[26] Cyberinstitute.com, *How to Use Preventive Law Principles to Develop New Preventive Law* (2016).

[27] Vera Bergengruen, *How an Online Pharmacy Sold Millions Worth of Dubious COVID-19 Drugs—While Patients Paid the Price*, TIME (Oct. 20, 2021).

[28] Kim Anne Zimmerman, *Internet History Timeline: Arpanet to the World Wide Web* (June 4, 2012).

[29] *Id.*

[30] Michael Gordon, *Perennial Entrepreneur: Sheldon Laube Launches Artkick*, THE SUIT: PROMOTING ENTERPRISE THROUGH INFORMATION (Mar. 12, 2014).