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

The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

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).

CHAPTER TWO

An Ethical Compass for Global Information Technologies

§ 2.0: OVERVIEW OF CHAPTER & ROADMAP

[A] Overview of Computer Ethics

Advances in artificial intelligence (AI), drones, robotics, 3D printing, crypto currencies, the advent of the Internet of Things and other revolutionary breakthroughs continually alter daily life as we know it. Information technology is so transformative that the World Economic Forum declares that we are presently living in the "Fourth Industrial Revolution," creating the possibility of a far better future. This technological revolution is expected to "create an inclusive, human-centered future. The real opportunity is to look beyond technology, and find ways to give the greatest number of people the ability to positively impact their families, organisations and communities."[1]

Today's ABCs are Apple, Bluetooth and Chatting, followed by Downloads, Email, Facebook, Google, Home Pages and iPhones. Increasingly complex computer applications allow us to book airplane flights, connect with distant relatives, shop in virtual bookstores, watch videos and follow Pokémon characters. Computer professionals are forced to confront moral dilemmas as software increasingly reshapes every aspect of society.

Social media owners have a moral, but not necessarily a legal, duty to protect their users from a variety of online oppressions. Applied computer ethics are necessary to analyze rapidly evolving software developments. For example, social networks struggle to find the appropriate balance between free expression, spreading dangerous disinformation and protecting their users from third party civil and criminal wrongs.

The ACM Code of Ethics and Professional Conduct, reviewed in Chapter 1 is the equivalent of a moral compass, useful in analyzing ethical issues. Computer professionals who subordinate the public good for illegitimate personal gain, or some other immoral purpose, violate computer ethics. For example, the Commentary to Section 3.1 of the ACM Code of Ethics states that benefiting all parties, "including users, customers, colleagues, and others affected directly or indirectly—should always be the central concern in computing."[2] The public good must always be considered in every project.

The practical problem is how best to define and to achieve this ideal. What exactly is the "public good"? Since the first edition of this book "technologies like deep packet inspection have allowed ISPs to collect and sell details on every aspect of your online life, then, through obfuscation, proxies, and empty promises of 'anonymization,' insist they're not doing exactly that."[3] Does the development and implementation of these privacy invading technologies violate the ACM's admonition that "[p]eople . . . should always be the central concern in computing"?

The ACM Code requires computer professionals to obey the law, but simply avoiding illegal acts is not enough of an ethical guide. A Rice University professor notes that "[s]urveillance capitalism is perfectly legal, and enormously profitable, but it is unethical, many people believe, including me. . . . It would be extremely difficult to argue that surveillance capitalism supports the public good."[4]

Computer ethics are best developed in context and rarely through the articulation of abstract moral principles. For example, lawmakers deal with the innate uncertainly of how much security is necessary by using a "standard," in this case "reasonable security," rather than a clear-cut rule.[5] The law is uncertain as to what extent social media, websites and other online entities owe a duty to implement "reasonable" security, much less exactly how much security is required to meet the reasonableness standard.

Reasonable security is difficult for a software engineer to operationalize, much less for a lawmaker or regulator to clearly define. Releasing a product with clearly inadequate security is ethically wrong. On the other hand, requiring too high of a level of security in a smart device might deprive customers of an inexpensive and useful product when it is improbable that the item will be hacked.

This chapter introduces five major ethical approaches to evaluating a moral quandary. These ethical perspectives are designed to provide a road map for thinking about how to advance the public good, while avoiding doing harm. These five views of morality will be used throughout this book to provide practical guidance on how to apply ethics and the law to diverse activities such as negotiating or litigating computer contracts, introducing software products into the marketplace, protecting website users from crimes and torts, and safeguarding online intellectual property rights.

The coming age of autonomous vehicles (AV) illustrates the need to update laws and ethical codes to accommodate technological change. Modern cars have become mobile computers on wheels, with microprocessors regulating functions like brakes, traction control and cruise control. The 2016 Ford F150 requires over 150 million lines of code to be fully operational. Microsoft Windows, in contrast, needs only fifty million lines. "Some industry players estimate that the amount of code in fully self-driving vehicles will climb to as high as 500 million lines."[6] A Ford GT already operates more lines of code than a Boeing 787.[7]

Multiple companies are adding driver assistance features to their vehicles in a race to mass produce the first truly autonomous vehicles. In late 2019, Lyft rolled out a self-driving ride-hailing service in the Phoenix area. That same year, Russia's Yandex tested a fleet of 100 self-driving cars. Merchants Foodservice uses fleets of autonomous vehicles to deliver both perishable and nonperishable items to its 6,000 customers.

In 2020, Waymo received an Australian patent for "dynamic routing for autonomous vehicles."[8] By January of that year, Waymo's self-driving cars had logged "20 million miles on public roads—a major feat to say the least. Waymo's latest figures make it the de-facto leader in the self-driving car space, surpassing China's Baidu and Russia's Yandex."[9]

AV technology requires not only the development of sophisticated computer modules, but also years of road tests. Developers use a process called "deep learning" to teach autonomous vehicle systems how to maneuver without requiring a human driver. Cloud-connected vehicles need ethical guidelines for resolving issues such as the appropriate level of computer security to implement in self-driving cars. Rolling out code updates to these vehicles through the cloud gives cybercriminals new opportunities to create harm.[10]

New liability rules will be needed when driverless cars are deployed widely. The AV's software determines how the vehicle responds in an extreme situation. "When a driver slams on the brakes to avoid hitting a pedestrian crossing the road illegally, she is making a moral decision that shifts risk from the pedestrian to the people in the car. Self-driving cars might soon have to make such ethical judgments on their own."[11] The term "law as code" refers to situations in which the computer program takes the decision out of the hands of the people involved in the situation.

Legislatures and the courts will be struggling for decades over how to regulate AV's. Should the AV be programmed to swerve to run over a rule-abiding elderly pedestrian to avoid striking a toddler strolling into onrushing traffic? Should it be legal to program an automobile to prioritize a driver's life over those of pedestrians when a collision is unavoidable? Is it ethical? Can existing tort law be stretched to address these moral dilemmas?

Cloud-connected cars already collate extensive data about individual's travel-related habits. As of 2022, at least thirty-seven companies were "part of the rapidly growing connected vehicle data industry that seeks to monetize such data in an environment with few regulations governing its sale or use."[12] What geolocation data about a married person or an ex-spouse's travel will be available to opposing parties in divorce or child custody disputes?

Can courts require smart automobiles to monitor the sobriety of drivers and passengers as a condition of parole? Will manufacturers be liable if criminals use malware to exploit inadequate security in robotic vehicles? These legal and ethical dilemmas issues are only a small sample of the pressing quandaries raised by rapidly evolving AV technologies.

Legislating ethics raises divisive issues, particularly when political parties have sharply different views on basic moral issues such as individual privacy rights. For example, the Obama Administration enacted a rule demanding that Comcast, AT&T and other Internet Service Providers document users' specific consent before they can commodify customers' personal data.

In April 2017, a Republican-controlled Congress overturned the Obama Administration's broadband privacy rules. Trump's U.S. Department of Justice later attempted to further reduce online privacy rights, when it sought a warrant to force an anti-Trump website to reveal personally identifiable data about Trump critics posting on its website.

President Biden favors a reform of the broadband industry to make access a right, not a luxury. Biden is in the process of appointing a majority of the board of the Federal Communications Commission to advance his agenda, "which includes net neutrality and making broadband available to 100 percent of Americans."[13] This chapter focuses on the application of the five ethical perspectives to examine real-world dilemmas such as the proper balance between free expression and public safety or economic liberty versus the need to protect the vulnerable from exploitation.

[B] Roadmap to Chapter 2

Section 2.1 comprises the majority of this chapter. It provides a detailed analysis of five leading ethical perspectives: (1) Consequentialism, (2) Virtue and Duty Theory, (3) Conflict Perspective, (4) Social Contract Theory and (5) Libertarianism. Each moral paradigm is based upon fundamentally different assumptions about the nature of the "good society" and how best to achieve it. These viewpoints will be operationalized in subsequent chapters by applying each of them to legal developments in online torts, cybercrimes, contracts and intellectual property.

Section 2.2 evaluates the advantages and disadvantages of professionalizing the computer field. Unlike traditional professions, such as law and medicine, computer science does not have a prescribed curriculum, course of study, a legally enforced ethical code nor a disciplinary board that can impose sanctions. The ACM Code of Ethics and Professional Conduct is based upon general moral principles, as opposed to legally enforced ethical mandates such as in the American Medical Association's Code of Ethics and American Bar Association's Model of Professional Conduct.

Disbarment removes a lawyer from the practice of law in a given jurisdiction. A lawyer can be disbarred for willful disobedience of a court order or committing an act of moral turpitude, dishonesty or corruption. The most common grounds for disbarment are unethical conduct or criminal offenses. Lawyers also can lose their law license for gross incompetence or incapacity.

Doctors who discover dangerously shoddy hospital practices can file a complaint with the state medical association. A computer professional, in contrast, does not have a professional association that can protect her from retaliation for reporting substandard software. Similarly, patients harmed by substandard medicine, can file a complaint against a physician with the State Medical Board. If the Board investigates the matter and finds merit to a patient's complaint, it may suspend, temporarily revoke or permanently revoke a physician's license to practice medicine.

The National Practitioner Data Base "is a web-based repository of reports containing information on medical malpractice payments and certain adverse actions related to health care practitioners, providers, and suppliers."[14] This data base allows potential employers and the public to evaluate the competence of medical personnel. No comparable method of publicly exposing incompetent or unethical software developers exists.

A programmer who violates the Computer Fraud and Abuse Act by hacking into a computer system belonging to a bank cannot be punished by any computer professional entity, even though his actions constitute a felony. Nevertheless, computer professionals who design dangerously defective software are legally liable, even those there is no professional association that exposes them.

An increasing number of computer scientists are calling for greater professionalization of the field to safeguard practitioners from employers who engage in unscrupulous, or even illegal, behavior and to protect the public from the release of dangerously defective software products. This chapter is a close assessment of the ethical guideposts to assist computer professionals recognize, analyze and resolve difficult ethical dilemmas arising in their work, even though their field has not formalized an enforceable ethical code.

§ 2.1: COMPUTER ETHICS THEORIES

This section of the chapter will introduce the five most common perspectives on computer ethics used in each subsequent chapter: (1) Consequentialism, (2) Virtue and Duty Theory, (3) Conflict Perspective, (4) Social Contract Theory and (5) Libertarianism. These approaches assume divergent underlying assumptions about:

(1) The nature of justice;

(2) Basic assumptions of human nature;

(3) The conception of law and its role in resolving ethical dilemmas;

(4) The proper role for government and regulatory agencies; and

(5) The nature of good and evil.

Supporters of each of the five perspectives, for example, have profoundly different viewpoints about whether courts should be able to suppress hate speech or order the removal of other offensive postings from the Internet. The Libertarian policies of a social media site such as 4chan, differ considerably from more closely monitored websites such as Facebook or Instagram.

Is access to the Internet a basic human right that should be provided to all or is it a luxury reserved for those who pay for access? Do employees whose job is taken over by robots deserve compensation, retraining or even guaranteed employment at a comparable salary? Should employers have the right to dictate that job applicants provide them with passwords to their Facebook accounts so they can screen out candidates with undesirable values? The quest for the proper ways to use digital technology to produce a better society will be deeply influenced by a policymaker's own concept of social justice.

[A] The Ethics of Sexting Law

The relationship between the ethics and the law of sexting illustrates how paradigmatic views of justice can lead to differing legal policies. Sexting, a portmanteau of "sex" and "texting," is commonly defined as sharing sexually explicit images, videos or other images with members of their peer group. Sexting is criminalized in many states if one of the parties is a minor. Forty-eight states have criminalized the sharing of nonconsensual pornography.[15] "Only two states—New Mexico and Maine—completely decriminalize teenage sexting."[16] Kentucky has made sexting a felony: "If a juvenile transmits a nude image of (him or her)self via a cell phone or a computer, that by law is a crime, but it's only punishable by being convicted of a felony."[17]

Sexting subdivides into two broad categories: "experimental" and "aggravated."[18] "Experimental" sexting is defined as youth-produced images sent "to established boy-or-girlfriends, to create romantic interest in other youth, or for other reasons such as attention-seeking."[19] Experimental sexting does not involve "malice or misuse or other criminal use of the image."[20]

Aggravated sexting, in contrast, "involve[s] criminal or abusive elements beyond the creation, sending or possession of youth-produced sexual images."[21] It requires an "additional act beyond what was anticipated or consented to by the person producing th[e] photograph" to become an aggravated sext.[22] When the original sext "is disseminated beyond its intended recipient, it becomes nonconsensual and can be a form of cyber bullying or revenge pornography. Such aggravated or nonconsensual sexting includes sexts exchanged between a teen and an adult."[23]

Other examples of aggravated sexting include "sharing a sext with the intent to cause harm and obtaining sexts via coercion or other non-consensual means."[24] The Internet Watch Foundation (IWF) report "shows almost 20,000 webpages of child sexual abuse imagery in the first half of 2022 [that] included 'self-generated' content of 7- to 10-year-old children."[25]

A federal statute prohibits "the coercion and attempted coercion of a minor to engage in sexually explicit conduct for the purpose of producing a visual depiction of such conduct applies to purely intra-teenage 'sexting,' provided that the 'sext' depicts a minor engaging in sexually explicit conduct."[26] A sext can be criminalized as child pornography and regulated under 18 U.S.C. § 2251(a) if it contains "sexually explicit conduct," which is defined as "actual or simulated—(i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (ii) bestiality; (iii) masturbation; (iv) sadistic or masochistic abuse; or (v) lascivious exhibition of the genitals or pubic area of any person."[27]

"[M]any states have laws that make sexting a crime—mainly due to concerns about the risks to safety and privacy."[28] Using criminal statutes to punish sexting minors is highly controversial because "[t]eenagers who are prosecuted for sexting are 'no longer going to school' and 'are shunned by their peers,' meaning that they are 'locked out of normal adolescence.' "[29] Juveniles' fear of a criminal record can lead to the sexting teen being further victimized through "sextortion," which is exploitation of the person sending sexual material. "Sextortion is a serious crime that occurs when someone threatens to distribute your private and sensitive material if you don't provide them images of a sexual nature, sexual favors, or money."[30]

Massachusetts, one of the outlier states without a criminal statute, is considering a law that would minimize the harms of prosecuting minors for sexting. "The proposal would divert minors who share explicit images of themselves or their peers into an 'educational diversion program' developed by the state attorney general, instead of automatically charging them with crimes."[31]

The argument over whether sexting should be criminalized illustrates the interrelatedness between ethics and law. Are sexting teenagers just participating in risqué flirtations via a modernized dating ritual or should these salacious communications be criminalized? Law enforcement personnel have wide discretion in translating and enforcing existing statutes. Colorado law, for example, categorizes the possession of any explicit pictures of underage persons as a felony, even if exchanged between consenting minors.

A severe penalty would technically comply with the letter of the Colorado law but, arguably, violates its statutory purpose. Legislators initially passed harsh child pornography statutes to punish the exploitation of vulnerable children by adults. The legislators probably never considered that this statute would also apply to sexting teenagers.

District attorneys (DAs) have filed child pornography charges against consensually sexting adolescents, noting that "when a minor takes and sends a lascivious picture of his or herself, the sexted image easily amounts to self-produced child pornography. As a result, the child can effortlessly be charged with violating child pornography laws."[32]

However, in Canon City, Colorado, the district attorney's office declined to prosecute a case against more than one hundred teenagers caught sharing sexually charged photos. Convictions for violating child pornography laws would stigmatize these teenagers for life because they would be required to register as sex offenders.[33]

In the judgment of the more aggressive DAs, to disregard criminal violations by these sexting teenagers would violate the prosecutors' ethical duty to enforce the law. These prosecutors seek not only to punish the direct perpetrators of these crimes ("specific deterrence"), but also to send a message of deterrence to the larger community ("general deterrence"). Libertarians, in contrast, contend that these overly zealous prosecutors are misusing their prosecutorial discretion. This viewpoint asserts that it is a waste of prosecutorial resources to criminalize the voluntary sending of risqué photos between youngsters.

Some states require schools to report any sexting activities to their local law enforcement office. While this is a legal duty, is it ethical? Schools may suspend the teens pending the outcome of such investigations and the investigation itself may cause humiliation for the teen. Is it ethical to publicize the punishing of consensual sexters "in an attempt to control the growing practice of sexting," even if the criminal sanction might be excessive?[34] Pragmatists argue that this "problem may be best handled as part of education and mentoring."[35]

[B] The Morality of Winning at All Costs

In his book, *The Art of the Deal*, Donald Trump brags about hoodwinking Holiday Inn executives into financing his Atlantic City casino project in 1982 by renting bulldozers to stand by, creating the impression that a new construction project was underway. This type of strategic decision-making reflects "poker game ethics." Bluffing in poker uses deceptive techniques such as betting or raising aggressively to fool your opponent into folding a hand incorrectly.[36] A skilled poker player uses trickery as a legitimate tactic to win the game.

Many venture capitalists are proud of their poker playing skills, considering their talents in reading other' motivations, tricking the opposition, estimating the odds of success and conquering misfortune to be very useful to succeed in the hypercompetitive environment of Silicon Valley.[37] Salespersons often guarantee that new computer applications will be highly reliable, even though most features have not yet been fully developed or tested.

Is offering "vaporware" (i.e., software or hardware that has been advertised but is not yet available for purchase) ethical? Is this acceptable "growth-hacking" or is this immoral behavior? Should Internet Service Providers be allowed to throttle information from one source at the expense of one that pays more for speedy transmissions? The five primary theories of computer ethics and law can be applied to these, and many other, dilemmas raised throughout the book.

[C] Computer Ethics Theories as Ideal Types

The five ethical vantage points used throughout this book demonstrate what German sociologist Max Weber (1864–1920) called ideal types, which "are constructs or concepts which are used as methodological devices in our understanding and analysis of any social problem."[38] The social scientist utilizes the ideal type as a construct for understanding complicated social realities. Weber used the German phrase, "Idealtypus" to indicate:

> A common mental construct in the social sciences derived from observable reality although not conforming to it in detail because of deliberate simplification and exaggeration. It is not ideal in the sense that it is excellent, nor is it an average; it is, rather, a constructed ideal used to approximate reality by selecting and accentuating certain elements.[39]

This investigative device stresses polarities as opposed to shared aims of seemingly incongruent theories.[40] One should seldom look at a moral dilemma from a single ethical perspective. When faced with a challenging moral impasse, it is often most productive to consider insights from several approaches.

(1) Deontological Ethics: Moral Rights & Wrongs

Moral philosophy may be divided into deontological and teleological approaches. The term "deontology" originates from the Greek words for duty ("deon") and science ("logos"). For deontological ethics, the focus is on the character of the moral agent and actions are demarcated as either right or wrong without considering the social context.

Deontologists place he emphasis on performing actions because they are virtuous and avoiding actions that are morally wrong. "In deontological ethics, an action is deemed morally right because of some aspect of the action itself, not because the totality of the action is morally right."[41]

Policymakers frequently incorporate deontological concerns in drafting and enforcing legal statutes. Criminal law classically describes offenses as having two elements: the "mens rea" and the "actus reus." The mens rea is the state of mind, while the actus reus is the act. Mens rea includes states of mind, such as whether an act is done with malice, purposely, knowingly, recklessly or negligently.

The mens rea for involuntary manslaughter is vastly different from first-degree murder, even though both are criminal sanctions for causing a death. Manslaughter is homicide committed negligently or recklessly. First degree murder, in contrast, requires a mens rea of malice and will be punished far more severely.[42]

Hacking into someone's computer system is illegal, but the computer intrusion may be done for virtuous motives, such as to foil a criminal or to expose government or corporate misdeeds. Should criminal penalties for Internet-related crimes vary depending upon the degree of immorality of the cybercriminal's actions?

For example, should a court distinguish between punishing a computer for a playful script kiddie versus a profit-seeking, black hat hacker, even though both released malware that caused equivalent harm? Should legislators draft criminal statutes to consider the motives of teenage pranksters as opposed to organized criminal gangs? A deontologist considers the degree of virtue underlying a cybercriminal's actions versus a focus on the consequences, which is the teleological approach.

(2) Teleological Ethics as an Ideal Type

Teleological ethics, in contrast to deontological perspectives, evaluate moral goodness or badness by the consequences, rather than the fundamental virtue of the actor. Jeremy Bentham (1747–1832), the father of Utilitarianism, denounced rights-based ethical theories as "nonsense on stilts." Moral behavior, for utilitarians, is producing the greatest overall amount of societal happiness. Utilitarianism aligns with Law and Economics in its support of free market economics.[43]

The five leading computer ethics theories will be applied to each hot button issue in this book. Mechanically utilizing one specific ethical perspective for every situation is an untrustworthy moral compass for resolving complex computer dilemmas. The five most important ethical perspectives are delineated in the chart below.

FIVE LEADING THEORIES OF COMPUTER ETHICS

Computer Ethics Theories	**Subtypes**	**Principal Focus**
Consequentialism	Utilitarianism, Pragmatism, Law and Economics	Are the outcomes good, even though the motives may not be?

		The objective of any public policy is to maximize overall societal happiness.
Virtue and Moral Duties	Aristotelians, Kantian Categorical Imperatives	Is the action moral in itself? What we ought to do without concern for the consequences?
Conflict Perspective	Marxism, Elite Theory, Critical Feminism, Critical Race Theory, Intersectionality of race, sex, class, age and disability	"Conflict theory states that tensions and conflicts arise when resources, status, and power are unevenly distributed between groups in society."[44] How can legislation be drafted to reduce societal inequities? Are societal inequities worsened by global information technologies such as the Internet?
Social Contract Theory	Hobbes, Locke and Rousseau's State of Nature, Rawlsian Social Justice	The goal is to achieve a stable social order without violating fundamental human rights such as free expression. A core dispute is over what rights must not be violated.
Libertarianism	Traditional Libertarianism, Cyberlibertarians	How can we increase human freedom, while preserving social order? Nation states have no authority to enact

		statutes governing cyberspace.

[D] Consequentialist Ethical Theories

(1) The Canons of Consequentialism

"Consequentialism is a theory that says whether something is good or bad depends on its outcomes."[45] Consequentialists assess positive consequences against harms created by the technological innovation. Jeremy Bentham favored a close analysis of positive and negative consequences of proposed legislation. "The correct statutory balance produces the greatest utility for the greatest number. Bentham's views are most closely aligned with 'act utilitarianism.' This basic form of consequentialism holds an action as ethical if, and only if, it produces more beneficial/pleasure-causing outcomes than negative/pain-causing ones."[46]

Bentham's student, John Stuart Mill, found Bentham's formulation to be impractical. Mill "believed it was too difficult for a society to run if it had to consider the specific costs/benefits of every single action. How could we have speeding laws, for example, if it would sometimes be ethical to break the speed limit?"[47] Users will differ on whether the convenience of allowing cookies to be placed on your computer is worth the sacrifice of privacy.

Mill articulated the Greatest Happiness Principle, that "actions are right in proportion as they tend to promote happiness, wrong as they tend to produce the reverse of happiness."[48] "Of all the things a person might do at any given moment, the morally right action is the one with the best overall consequences."[49] Most digital advances have increased human happiness, although sometimes at a significant cost.

(2) Applying Consequentialism to Killer Drones

A U.S.-centric consequentialist approach appraises the ethical issues raised by military drones in terms of whether they accomplish their assigned goals at an acceptable cost. The U.S. Department of Defense endorses the use of drones based on their effectiveness: "Now they're pretty much integrated into our standard operating procedure for response because they're so useful both for fire mapping and damage assessment."[50]

Consequentialists purposely remove emotion from the cost-benefit equation by using terminology such as "collateral damage," to describe civilian deaths caused by wayward drones. Diplomats at a 2022 United Nations conference on whether the use of robots designed to kill without direct human oversight should be banned as a war crime, referred to these devises with the relatively neutral term, "lethal autonomous weapons systems."[51] This moral framework may lead military strategists to ignore the sacrifice of innocent lives for America's greater good.

A deontological perspective, in contrast, begins with a deep concern with creating amoral killing machines. Leaders from the world's top AI and robotics companies issued a 2017 letter warning of the dangers of military drones and other killer robots. The letter states that these technologies "will permit armed conflict to be fought on a scale . . . faster than humans can comprehend."[52] The founder of Clearpath Robotics cautions that: "The development of lethal autonomous weapons systems is unwise, unethical and should be banned on an international scale."[53]

Human Rights Watch takes the same deontological stance, stating that:

> Weapons systems that select and engage targets without meaningful human control are unacceptable and need to be prevented. All countries have a duty to protect humanity from this dangerous development by banning fully autonomous weapons. Retaining meaningful human control over the use of force is an ethical imperative, a legal necessity, and a moral obligation.[54]

A United Nations panel in Geneva is split on the issue of autonomous killing machines. "If an autonomous weapon makes a mistake and possibly commits a war crime, who's responsible?"[55]

Legislators have yet to draft statutes addressing the privacy concerns raised by the widespread deployment of drones in the civilian economy. Should it be illegal to take pictures of celebrities through the windows of their private dwellings? Should jealous husbands be legally permitted to deploy drones to document their spouse's infidelity? Transportation workers may be displaced by drone package deliveries, potentially instigating a "jobs apocalypse." Should governments allocate tax dollars to comprehensive programs to retrain transportation sector workers displaced by drones?[56]

Computer professionals may play a pivotal role in developing code that can enforce ethical drone regulations. It might be possible, for example, to implement software that will employ AI to block the drone user's ability to take intrusive photographs. Similarly, drone software could override any command that would endanger commercial or military flights.

An obvious weakness of this perspective is its lack of consideration of basic human rights and social justice.[57] In addition, it is impractical to research the benefits and costs of every act. While consequentialism "sounds attractive in theory, it's a very difficult system to apply to real life moral decisions because every moral decision is a completely separate case that must be fully evaluated."[58]

[E] Virtue & Duty Ethics

(1) Kant's Duty Theory

Virtue and Duty ethicists, adopting deontological logic, regard the amoral emphasis on efficiency in consequential models to be deeply objectionable. Immanuel Kant, the founding father of duty ethics, denounced consequentialism, stating that: "Morality is not the doctrine of how we may make ourselves happy, but how we may make ourselves worthy of happiness." In Kant's words, "a good will is not good because of what it effects or accomplishes, but rather because it is one's duty."

Consequentialists criticize Kant's rigid definition of correct behavior as inimical to the practical necessity of compromise.[59] To a utilitarian, "when lying is necessary to maximize benefit or minimize harm, it may be immoral not to lie."[60] In contrast, Kant's moral duties must be fulfilled no matter what the consequences, a very abstract notion, which lacks social context:

> For example, we must always tell the truth no matter what. Suppose a German SS officer knocked on my door, asking me whether I had any Jews. And suppose further that I had two Jews in a secret compartment in the attic that he'd never be able to find. Everybody will agree that I must lie and say I haven't any Jews in my house. But I'd have to disobey Kant's categorical imperative "do not lie," because I felt obliged to not betray innocent people leading to their death.[61]

Virtue and Duty theorists find this accusation to be imbalanced, arguing that a more generous reading of Kant's essential point is that wrongs, even when done in a virtuous cause, are still deeply problematic.[62]

Immanuel Kant (1724–1804)
Father of Secular Duty Ethics
"Always recognize that human individuals are ends, and do not use them as means to your end."
Source: Government Document, U.S. Library of Congress.

Ethicists approaching computer technology dilemmas from a Kantian perspective believe that morality is not pursued "for the sake of anything else: it does not owe its value to anything outside itself."[63] Kantians would follow their ideals and refuse to design a manipulative website, because such work would not produce a product of the highest moral worth. Deceiving consumers violates a moral duty, even if the designer technically complies with contract law.

Kantianism was prefigured by Aristotelian ethics, which emphasized that law should reward virtue and punish vice. Like many classical Greek thinkers, Aristotle (384–322 B.C.), the tutor of Alexander the Great, believed that the goal of government is to cultivate good character. Nevertheless, Aristotle acknowledged that law is always subject to revision when conditions change. The Aristotelian conceptions of nature, justice and equity still shape contemporary views of right behavior.[64]

(2) Applying Virtue Theory to the Ashley Madison Breach

Ashley Madison is a website that, at its core, violates the moral imperative that honesty is the best policy. Virtue and Duty ethicists would probably find the cheating website morally repugnant simply because it promotes extramarital affairs. Worse, the site deployed bots impersonating sexually available females calculated to coax male customers into sending gifts to win the affections of eligible women.

This behavior would certainly fail any test of compliance with virtue ethics. As part of case's settlement, Ashley Madison's parent company agreed to provide a refund of up to $500 to members who spent money to communicate with an estimated 70,000 "engagers" that were actually bots with bogus female profiles.[65]

Violating Kantian ideals of honesty, however, can be the most effective approach in catching and prosecuting cybercriminals. In computer security parlance, a "honey pot" is a trap set to detect, deflect, or in some manner neutralize attempts at unauthorized use of information systems. The computer security administrator uses the honey pot to understand more about how cybercriminals take advantage of any vulnerability in their system, and then redesigns the system to eliminate these flaws.

Online pedophiles may be identified and apprehended through honey pots created by FBI agents posing as adolescents. This type of duplicity can be viewed from a virtue perspective as an unethical form of entrapment, where a person may be tempted into perpetrating a crime that they would not have otherwise committed. Consequentialists support this law enforcement strategy because it works.

[F] Conflict Theory Ethical Perspectives

(1) Applying Conflict Theory to New Technologies

Conflict Theory evaluates novel technologies in terms of how they increase or decrease social equality. Conflict theorists contend that the widespread use of artificial intelligence will result in greater inequality over time unless capitalism's profit-motive is replaced by considerations of social justice. Under capitalism, the leaders and financiers of a small number of high technology companies unjustly become immensely wealthy, while robots and other innovative technologies displace increasing numbers of workers. A more just social order would provide a guaranteed income for everyone:

> Robotization, like past technological changes, can be a very good thing, relieving the workload of humans while helping overcome the many challenges the world faces. But it could also affect humans disastrously, dividing societies between the owners of the robots on one side, and the workers who compete with the robots on the other. We should worry less about the potential displacement of human labor by robots than about how to share fairly across society the prosperity that the robots produce. Today, gains accrue disproportionately to the wealthy—who are the principal owners of capital.[66]

Critics of conflict theory argue that technological advances create a better world, even if some lives are disrupted in the short run. It is unlikely, for example, that robots using artificial intelligence will replace lawyers. "From typewriters to computers and from fax machines to email, each advance has been transformative in the law. Lawyers have accepted and adopted each of these evolutions. AI is the next frontier."[67]

Artificial Intelligence "is helping lawyers automate repetitive types of tasks—like drafting lower-exposure or lower-liability agreements like NDAs. AI is also empowering in-house counsel in areas such as predictive coding, by saving attorneys' time by using samples of data to identify relevant documents in connection with e-discovery requests."[68] AI enables lawyers to make better decisions and to give advice more efficiently.

(2) The Computer Industry & Social Inequalities

Conflict perspectives focus upon the constraints of "sex, gender, race, sexual orientation and class that shape individuals' knowledge, experience and opportunities."[69] These theorists assert that the field of computer science is marked by increasing gender injustice. The percentage of computer science degrees granted to women by American colleges has dropped from 37% in 1985 to only 18% in 2014.[70]

In top-ranked universities, the percentage of female computer science graduates has decreased even further, to 14%. The computing industry is creating jobs at three times the national average, but one study concludes that women will hold only a fifth of computing jobs by 2025.[71] Melinda Gates, a computer science major and former technology company executive, has pledged $80 million to help recruit more women into high tech jobs.

Sexism is widespread in high technology fields. A former employee of Upload VR contended "that the company created a hostile work environment by making offensive sexual comments, discussing details about their sexual encounters, and even engaging in sexual intercourse in the office."[72] A 21-year-old researcher reports being sexually assaulted in Meta's virtual reality platform, "Horizon Worlds, when a male avatar led her into a private room and raped her avatar. The researcher also said she witnessed homophobic slurs and virtual gun violence. Her case seems to be one of many."[73]

As an example of how computer science's "bro culture" discourages women from remaining in the computer science field, one female computer scientist observes:

> On Sunday, after an all-night hackathon at TechCrunch Disrupt, Australian programmers presented Titstare. 'Titstare is an app where you take photos of yourself staring at tits,' Jethro Batts explained. He went on to say, 'I think this is the breast hack ever.' The app was

> dreamed up during an overnight hackathon and presented to an audience of 500.[74]

The Gamergate controversy arose out of a series of threats and other hostile actions against women who criticized sexism in the gaming industry. In August 2014, a group of mostly young men launched a vitriolic attack on Zoie Quinn, a female game developer. She became the target of trolls and stalkers after "she began trying to publish *Depression Quest,* a text-based game partially based on her own experience with depression."[75]

Anonymous misogynists who "sent images showing video-game characters raping her harassed Anita Sarkeesian, a prominent media critic. Sarkeesian's Wikipedia entry was repeatedly vandalized" after she won a Game Developer Choice Award.[76] She contends that online gaming has a deeply sexist history:

> The gaming industry has been male dominated ever since its inception, but over the last several years there has been an increase in women's voices challenging the sexist status quo. We are witnessing a very slow and painful cultural shift. Some male gamers with a deep sense of entitlement are terrified of change.[77]

The attacks on Zoie Quinn, Anita Sarkeesian and other leading women in the gaming field is said to stem from a misogynistic subculture dominated by young, white, heterosexual males:

> Campaigns of personal harassment aimed at game developers are nothing new. They are dismayingly common among those who happen to be women, or not white straight men, and doubly so if they also happen to make the sort of game that in any way challenge the status quo, even if that challenge is only made through their very existence. The viciousness and ferocity with which this campaign occurred, however, was shocking, and certainly out of the ordinary. This was something more than routine misogyny (and in games, it often is routine, shockingly). It was an ugly spectacle that should haunt and shame those involved for the rest of their lives.[78]

Previous research documented that 28% of female users of virtual reality games have experienced sexual harassment. "There is racism, sexism, and anti-LGBTQ sentiments that are definitely happening now."[79] Meta is struggling "to combat hate speech and harassment on its popular social media platforms, where people leave behind a record of their remarks."[80]

(3) Updating Marxism for the Information Age

(a) Karl Marx's Theory of Class Conflict

Marxism is named after Karl Marx (1818–1883). The term "Marxist" refers to those who believe that the economic structure plays a key role in shaping social reality. Marxism is the antithesis of capitalism, as "an economic system based on the private ownership of the means of production and distribution of goods, characterized by a free competitive market and motivation by profit. Marxism is the system of socialism of which the dominant feature is public ownership of the means of production, distribution, and exchange."[81]

Karl Marx predicted continual class conflict between wealthy capitalists, who control the means of production, and the proletariat, who are increasingly deskilled wage laborers, lacking control over their work product.[82] In the *Manifesto of the Communist Party*, Marx and Engels wrote that "society as a whole is more and more splitting up into two great hostile camps, into two great classes, directly clashes with each other: Bourgeoisie and Proletariat."[83] "The proletariat is without property. . . . Law, morality, religion is to him so many bourgeoisie prejudices, behind which lurk in ambush just as many bourgeois interests."[84] "The present youth rebellion," he writes, by "helping to change the workers of tomorrow" will, along with other factors, make possible a socialist revolution.[85]

The central tenets of Marxism are to:

(1) See the character of economic organization as the basic factor in shaping a society's value system, social class structure and political institutions and practices.

(2) See a capitalist economy as creating profit-oriented, materialistic values and a class structure in which wealthy owners constitute a ruling class that uses the power of the state, both at home and abroad, in exploitative and selfish ways; and

(3) Believe that such a social system is unjust, unnecessary, inconsistent with man's nature and should be eliminated—peacefully or, if necessary, by force.[86]

Marxists argue that most people are oppressed under capitalism because this economic system clashes with the basic human desire to be cooperative. Gender inequality, racial inequality, militarism, imperialism and other social problems are viewed as being, at least partially, created by class conflict.

(b) Marxism in the Age of the Internet

Cyberspace is a modern arena of struggle between the capitalist class's desire to maximize their power and the desires of the great majority to use the Internet to create a more just society. "The Marxist revolution for the 21st century will not need guerrilla warfare, but better coding and UX design. Fighting for equality is helping build the p2p platforms and fostering user adoption. This time, the revolution will reconcile freedom and equality."[87]

In a post-capitalist society, technological and cultural progress will be far more rapid because, without the profit motive, software advances would be freely available. Frederico Ast calls for a Marxist revolution for the Internet:

> The fall of Siren Servers (Facebook, YouTube, Uber, Airbnb, Twitter, Medium, etc.) and the rise of blockchain [decentralized autonomous organizations] will usher a new revenue model for the Internet, and higher equality in income distribution for the world at large. Wealth that is today accumulated in the few hands of founders and early investors of the mega intermediaries will go to all users. This, I believe, will create a new middle class for the Internet Age.[88]

(4) An IT Labor Aristocracy?

If Marx was alive today, he might be startled by how well workers are treated in the information technology sector. "There's no shortage of perks at the world's best tech employers—free food, massages, on site medical centers—the industry is jam-packed with employers who offer lucrative pay and enviable extras."[89] Google has become one of the best places to work in the country:

> Attracting high-achieving talent with endless perks and bonuses, the media giant aims to make employees' lives easier with meditation facilities and free meals. Googlers are a proud lot. Scoring 98 percent in Great Rated!'s "Great Pride" category overall, employees say they often or almost always carry meaningful responsibilities with the organization. And Googlers share that pride in giving back to the community: the company donated more than a billion dollars to charity last year. Says one employee: 'I have never worked in any place like this. It feels like working at a cross between Harvard, Hogwarts and NASA. The atmosphere and culture is truly unique and unlike anything I've ever experienced elsewhere.'[90]

Eighty-seven percent of Twitter's employees agreed that "they often or almost always experience a free and transparent exchange of ideas within the organization."[91] Twitter hosts special Global Tea Times where executives and staff socialize:

> Twitter keeps the conversation going between staff members. Offices feature on-tap kombucha and iced coffee and employees have access to training and improvisation courses and receive a $100 fitness reimbursement. Says one employee: 'Between celebrities coming into work on a regular basis, the relaxed vacation policy and the genuine friendship I have with co-workers is unlike anything I've experienced before. I work my ass off and get a lot done, but the ability to take breaks in the game room, or take the day off when necessary, provides for a really relaxed while upbeat work environment.'[92]

Contemporary Marxists charge that these luxurious working conditions are actually a way to encourage high tech workers to spend more hours on the job. Marxists argue that the profit motive will eventually lead to widespread cutbacks on worker benefits.

(5) Profit-Sharing as a Refutation of Marxist Theory?

Eugene Debs, a pioneering American labor leader, argued that profit sharing, if done fairly, would prevent a Marxist revolution.[93] "It is possible that profit sharing, if conducted honestly, would do away with the more serious labor troubles which afflict the industrial world."[94] Many high technology companies give their employees a share of the profits in the form of direct grants or stock options:

> Every Intuit employee is eligible for some kind of equity grant, whether it be stock option or restricted stock units. Those in vice president positions or higher receive non-qualified stock options upon being hired, while those in lower positions are offered RSUs. Either way, the equity grant vests over a period of three years. The information technology company also offers an employee stock purchase plan. Workers have the option to contribute up to 15% of their eligible pay to purchase stock at a discount of at least 15%, an option that more than two-thirds of employees choose.[95]

GoDaddy Inc., a publicly traded Internet domain registrar and web hosting company, gave its nearly 5,000 employees non-qualified stock options when it went public in 2015. "The technology provider also offers a stock purchase plan that offers employees the opportunity to buy and sell stock every six months at a discounted rate of 15%."[96]

Huawei, the Chinese telecommunications giant is owned by its employees. At Huawei's inception, the company designed an Employee Stock Ownership Plan (ESOP).[97] "Furthermore, because Huawei is not a public company and owned by its employees, employees take a large share from the company's earnings. In the case of Huawei the total net profit that was earned over the last twenty years is considerably smaller than the total net profit that was paid out to its employees."[98]

Employees working in the top rungs of the information industry are hardly an oppressed proletariat. However, profits are not equally apportioned. In 2002, nine of the ten wealthiest persons in the U.S. were founders of leading information technology companies.[99] "As of August 2022, Mark Zuckerberg's net worth is estimated to be $70 Billion."[100] The 400 wealthiest Americans had a total net worth of $4 trillion.[101] The Forbes 400 Report found that:

> Elon Musk tops The Forbes 400 for the first time. Despite all the turmoil in both his professional and personal lives, Musk is an estimated $60.5 billion richer this year, thanks to an 11% jump in Tesla stock and fresh new rounds of funding for SpaceX. He unseats Jeff Bezos, now No. 2, who was hit by a 27% drop in Amazon shares. Bill Gates moved up a spot, to No. 3.[102]

The economic gap between the privileged elites and a much larger group that labors in disrupted industries such as retail sales, transportation and food services continues to widen. Third World temporary computer employees often toil long hours in oppressive workplace conditions at low pay. Marxists argue that the most severe contemporary class struggle is between workers remotely working in Third World countries and their privileged, First World employers.

(6) How Free & Open Source Blurs the Worker/Owner Divide

Open Source Software (OSS) is defined as "software for which the human-readable source code is available for use, reuse, modification, enhancement and redistribution by the users of that software."[103] Under the traditional proprietary license, source code is kept secret and the program is only made available in object form. In contrast, open source license agreements do not restrict anyone from selling, or even giving away the software.

Yochai Benkler, a Harvard law professor, argues that information technology companies have softened the sharp division between the owners and workers by changing the meaning of property ownership. "Property in open source is configured fundamentally around the right to distribute, not the right to exclude."[104] Open source license agreements enable the sharing of source code with greater collaboration and less inequality. The Open Source Initiative explains this principle:

> In order to get the maximum benefit from the process, the maximum diversity of persons and groups should be equally eligible to contribute to open sources. Therefore, we forbid any open-source license from locking anybody out of the process.[105]

In the information-age economy, everyone can be a producer as well as a consumer, so the means of production are not solely in the hands of the capitalist class. Benkler sees the open source movement and the rise of the Internet as key to democratizing the means of production. He conceptualizes three layers of Internet governance: the "physical infrastructure" layer, the "content" layer and the "logical" layer. Benkler writes:

> We are making regulatory choices at all layers of the information environment—the physical infrastructure, logical infrastructure and content layers—that threaten to concentrate the digital environment as it becomes more central to our social conversation. These include decisions about intellectual property law, which can make ownership of content a point of reconcentration, decisions about the design of software and its standards, and the regulation of physical infrastructure available to Internet communications, like cable broadband services.[106]

Free and open source software is generative, continually being improved by the programmers who produce, distribute and modify it. In contrast, proprietary software reflects a pro-capitalist model, where the software publishers own the code and control the means of production.

Open source licensing allows a community of downstream users to look under the hood and improve the code. An intellectual commons is a core component of a free-networked society. Hollywood, the recording industry and other large proprietors of intellectual property, are seen as systematically undermining the innovations of the collaborative-networked economy.

Yochai Benkler concludes that we should not let "yesterday's winners dictate the terms of tomorrow's economic competition." Peer-to-peer production, Benkler argues, is creating a new order where collective efforts contribute to the common goal of better software. Benkler cites the triumph of user-driven innovation, such as the General Public License version 3 (GPL/V3), which requires licensees to return modifications to the public under the same terms.

To qualify as a GPL, the license must permit users to redistribute software so that other licensees have access to source code. Linus Torvalds, the developer of the "Linux kernel," famously quipped that "Software is like sex; it's better when it is free."[107]

[G] Social Contract Ethical Perspectives

(1) History of Social Contract Theory

Social contract theory assumes that a person's moral and political obligations stem from a contract to form a society. "Social contract theory says that people live together in society in accordance with an agreement that establishes moral and political rules of behavior. Some people believe that if we live according to a social contract, we can live morally by our own choice and not because a divine being requires it."[108]

Social Contract Theory is predicated upon the philosophical assumption that we must surrender individual freedoms for the privilege of living in a civilized society. However, certain basic human rights are guaranteed by the social contract to be protected at all costs. "Social contracts can be explicit, such as laws, or implicit, such as raising one's hand in class to speak. The U.S. Constitution is often cited as an explicit example of part of America's social contract. It sets out what the government can and cannot do."[109]

The ethical questions for social contract theory center on how to determine fundamental rights in cyberspace. The right to physical security often clashes with free expression rights. Monitoring and suppressing Internet communications violates the fundamental rights guaranteed in the Bill of Rights of the U.S. Constitution. Social contract theorists seek to balance privacy and security in a world in which "hackers can take control of cars or shut down an electric grid."[110] To what degree is it ethical to limit online expression to clamp down on immoral cyberspace activities?

Different social contract-inspired theories do not agree on what rights are fundamental. A United Nations report declared "that disconnecting people from the Internet is a human rights violation and against international law."[111] Several nations, "including Costa Rica, Estonia, Finland, France, Greece and Spain, have asserted some right of access in their constitutions or legal codes, or via judicial rulings."[112]

President Biden describes his Administration's Affordable Connectivity Program as vital to providing low priced, high speed Internet service to the vast majority of Americans. A quality Internet connection, Biden argues, is now "a necessity, analogous to the need to have a telephone":

> [T]hat's why, in November, when we passed the Bipartisan Infrastructure Bill, we also created something called the Affordable Connectivity Program. . . . Here's how it works: If your household income is twice the federal poverty level or less—that's about $55,000 per year for a family of four or $27,000 for an individual—or a member of your household is on Medicaid or Supplemental Security Income or a number of other programs, you're eligible to—for affordably connect—the Affordable Connectivity Program.[113]

Classical Greek philosophers advocated social contract theories long before the birth of Christ. In Plato's *Crito*, Socrates laid the foundation for social contract theory, which states that there is an unspoken agreement between the individual and the state. Socrates explains that he must accept the Athenian government's death sentence because society requires cooperation with mutually agreed upon rules.

Classical social contract theorists, such as Seventeenth and Eighteenth Century political philosophers Thomas Hobbes, John Locke and Jean-Jacques Rousseau, further developed the idea that all humans live under an implied covenant.[114] John Rawls' Kantian version of social contract theory posits that people who did not know their eventual fate would voluntarily choose an extensive social safety net.[115]

The social contract philosophers depicted in the chart below each promoted different versions of the argument that society is based on an implicit contract by which individuals voluntarily surrender their non-essential freedoms in return for the advantages of living in society. Throughout history, people have exchanged certain freedoms for the protection and other benefits of society.

Certain freedoms were not surrendered in joining society and people have the right to reject any law or policy that violates these natural rights. The United States Constitution's Bill of Rights is a literal social contract that delineates essential human rights the U.S. government is forbidden to violate. The basic dispute among the major social contract theorists lies in what essential rights are too important to be debased.

THREE VARIETIES OF SOCIAL CONTRACT THEORY

Key Concept	**Thomas Hobbes**	**John Locke**	**John Rawls**
Human Nature	Selfish; Can be vicious	Selfish, but restrained by common sense	Seeks equality if outcomes are concealed by a "veil of ignorance"
State of Nature	Life is "solitary, nasty, brutish and short"	Inefficient cooperation	Cooperative because fate is unknown
Role of Government	Necessary	Useful	Useful
Social Contract Rights	Life	Life, liberty, and property rights	Strong social safety net to protect the weak

(2) Thomas Hobbes' Leviathan

Thomas Hobbes (1588–1679) developed a version of social contract theory in his 1661 book, *The Leviathan,* written during the English Civil War of 1642 to 1651. The thesis of *The Leviathan* is that we surrender power to the state as the price for our collective security. Hobbes argued that a strong central state or sovereign was necessary to prevent returning to the state of nature, which is a time of an intolerable war of all against all:

> In the State of Nature, which is purely hypothetical, men are naturally and exclusively self-interested, they are equal to one another, (even the strongest man can be killed in his sleep), there are limited resources, and yet there is no power able to force men to cooperate. Given Hobbes' reasonable assumption that most people want first to avoid their own deaths, he concludes that the State of Nature is the worst possible situation in which men can find themselves. It is the state of perpetual and unavoidable war. The situation is not, however, hopeless. Because men are reasonable, they can see their way out of such a state by recognizing the laws of nature, which show them the means by which to escape the State of Nature and create a civil society.[116]

Under a Hobbesian model, the government's basic duty is to protect the lives and safety of the citizenry. Applying this perspective to modern issues, violations of Internet freedom would be permissible if the alternative would be to let terrorists destabilize society.

(3) John Locke's State of Nature

John Locke (1632–1704) challenged Thomas Hobbes' "nasty, brutish and short" view of human life without a strong sovereign. Instead, Locke described the state of nature "as a state of perfect and complete liberty to conduct one's life as one best sees fit, free from the interference of others."[117] "The Law of Nature, which is in Locke's view the basis of all morality, and given to us by God, commands that we not harm others with regards to their 'life, health, liberty, or possessions.' "[118]

John Locke highlighted the role of government in protecting property, liberty and life as the basis of the social contract, arguing; "That the obligation to obey civil government under the social contract was conditional upon the protection not only of the person, but also of private property. If a sovereign violated these terms, he could be justifiably overthrown."[119]

(4) Jean-Jacques Rousseau's Social Contract

Jean-Jacques Rousseau (1712–1778), who lived and wrote during the Enlightenment in eighteenth century France, described his version of social contract theory in his 1762 work entitled *Social Contract*. Rousseau's central question was "how can we live together without succumbing to the force and coercion of others?" We can do so, Rousseau maintains, by submitting our individual wills to the collective or general will, created through agreement with other free and equal persons.

Like Hobbes and Locke before him, Rousseau contended that all men are created to be equals. These philosophers maintain that no person has a natural right to govern others. The "only justified authority is the authority that is generated out of agreements or covenants."[120] People have the right to revolt against a government that sufficiently violates this basic morality.

Rousseau's political philosophy was a major influence in the French Revolution and on modern political thought. The Declaration of the Rights of Man and of the Citizen, enacted by France's National Constituent Assembly in August 1789, was the most important document of the French Revolution. This Declaration was shaped in large part by the theory of natural rights, maintaining that the rights of man are universally valid.

In September 2016, the Internet Security Alliance proposed a social contract to provide a coherent framework to create a "sustainable system of cybersecurity."[121] Cybersecurity Social Contract 2.0 posits two key elements:

> First is the realization that cyber security is not a purely technical problem. Rather, cyber security is an enterprise-wide risk management problem which must be understood as much for its economic perspectives as for its technical issues. The second key element is that, at this point, government's primary role ought to be to encourage the investment required to implement the standards, practices and technologies that have already been shown to be effective in improving cyber security.[122]

(5) John Rawls' Veil of Ignorance

John Rawls (1921–2002) was a twentieth century social contract theorist who employed the thought experiment of asking what social order people would choose if they did not know what body, nationality and social status they would be born into.[123] Rawls' "veil of ignorance" was presented as a hypothetical about a situation in which: "No one knows his place in society, his class position or social status; nor does he know his fortune in the distribution of natural assets and abilities, his intelligence and strength, and the like."[124]

Rawls contended that in this "veil of ignorance," people would overwhelmingly support an eclectic position in which there is a faithfulness to the social contract rather than libertarian or utilitarian positions. Their fear of being born with few resources, or being cut off from the connected society, would trump any desire to gamble on being born into a privileged position.

This logic led Rawls to argue that morality requires helping the downtrodden. He advocated for the "difference principle," under which "only those social and economic inequalities are permitted that work to the benefit of the least advantaged members of society."[125] No one in their original position would choose to implement a digital divide, where a relative lack of access to information technologies undermines the life chances of the underprivileged.

Rawls' argument applies equally well to the social impact of computing. Section 3.3 of the ACM Code states that professionals must: "Manage personnel and resources to enhance the quality of working life."[126] The Commentary to Section 3.3 of the ACM Code of Ethics reflects a Rawlsian position:

> Leaders should ensure that they enhance, not degrade, the quality of working life. Leaders should consider the personal and professional

> development, accessibility requirements, physical safety, psychological well-being, and human dignity of all workers. Appropriate human-computer ergonomic standards should be used in the workplace.[127]

Section 3.5 imposes a duty on computer professionals to foster leadership in the persons they supervise. The section states that computer professionals must "Create opportunities for members of the organization or group to grow as professionals."[128] The Commentary to Section 3.5 explains that leaders are to help others improve their position, which is also a Rawlsian precept:

> Educational opportunities are essential for all organization and group members. Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties. These opportunities should include experiences that familiarize computing professionals with the consequences and limitations of particular types of systems. Computing professionals should be fully aware of the dangers of oversimplified approaches, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and their contexts, and other issues related to the complexity of their profession—and thus be confident in taking on responsibilities for the work that they do.[129]

Similarly, it is a Rawlsian ideal to consider the impact of a computer professional's work on society. Section 3.7 explicitly imposes a professional obligation to: "Recognize and take special care of systems that become integrated into the infrastructure of society." The Commentary of Section 3.7 explains:

> When organizations and groups develop systems that become an important part of the infrastructure of society, their leaders have an added responsibility to be good stewards of these systems. Part of that stewardship requires establishing policies for fair system access, including for those who may have been excluded. That stewardship also requires that computing professionals monitor the level of integration of their systems into the infrastructure of society.[130]

Social justice would involve using the Internet to disproportionately benefit the disadvantaged, which brings Rawls' implied policies much closer to those of conflict theorists than other social contract theorists. Nevertheless, conflict theorists are far more likely to believe that society is so deeply stratified and imbalanced that the idea of a social contract is a fiction. For many conflict theorists, the legal system itself needs to be radically revised or even overthrown, which is a goal that Rawlsians would not favor.

One of the main defects of social contract theory is that there is no empirical support for the historical explanation of how the State evolved:

> It claims to be a historical explanation of the origin of the State, but it has no foundation in history. In the whole range of human history we do not find men living in a State of nature without social relationships, nor do we find any evidence of a social contract which created the society and the State. In short, there is no historical evidence of a social contract in human past It is historically impossible to believe that men living in the State of nature, and knowing nothing about political institutions and organisations, should suddenly and deliberately agree to set up a State.[131]

Feminists and critical race theorists "have argued that social contract theory is at least an incomplete picture of our moral and political lives, and may in fact camouflage some of the ways in which the contract is itself parasitical upon the subjugations of classes of persons."[132]

[H] Libertarianism & Cyberlibertarian Ethics

(1) The Traditional Libertarian Approach

Libertarianism, which draws upon nineteenth-century laissez faire capitalism, argues, "so long as we do not violate others' rights, we should each be free to live as we choose."[133] Central to this ideology is the belief that the free market is an important source of economic and political freedoms.[134]

The total satisfaction is greater in a free market than in any collectivistic alternative because there is no coercion of the individual. Libertarians maintain that private contracts, with government intervention only to ensure that both parties live up to their agreements, maximizes freedom. Traditional libertarians also assume that the parties would not enter an agreement unless it was mutually beneficial.

Andrew Grove, a co-founder and CEO of the semiconductor manufacturer Intel, characterized the intense competition among high technology entrepreneurs in a book entitled *Only the Paranoid Survive*.[135] Libertarians believe that customers benefit greatly from the ceaseless competitive struggle to gain an advantage over rivals.

Consumers have the responsibility to read and understand these terms rather than relying on government oversight. If the terms of use are not to the consumer's liking, he or she has the freedom to boycott the website and to use (or profit from establishing) one that offers more satisfactory terms.

The legal invention of licensing protects the underlying intellectual property rights of software, trade secrets, patents and derivative works through private contracts, which is an alternative to heavy-handed government regulation. Software licensing contracts are used to advance intellectual property rights, limit liability, earn royalties and commodify the product.

The licensor and licensee voluntarily enter into a contract, even if they check "I agree" without actually reading the terms. Given that almost no consumer reads the terms of use, should the government police these agreements for clauses such as caps on damages, arbitration clauses and class action waivers that eliminate any meaningful remedy? Should the government protect consumers from unfair and deceptive consumer contracts or should it be limited to being a mere "night-watchman," a minimal state that only protects individuals from clear-cut aggression, theft and fraud?[136]

The software industry adopts a libertarian position when it opposes activist courts that invalidate one-sided terms, such as anti-class action waivers, caps on damages or mandatory predispute arbitration. The industry argues that paternalistic courts foster a nanny state when they refuse to enforce anti-consumer clauses.

Software providers contend that, in a free market, rivals will displace companies that do not serve consumers well. In the words of Amazon CEO, Jeff Bezos, "Your profit margin is my opportunity." Netflix was setting its prices higher than was necessary, which motivated Amazon, and then several others, to enter the market with competing film streaming services.

Libertarians contend that established interest groups attempt to block potential competitors by lobbying for laws that ostensibly are enacted for the common good, but actually protect the proposers' privileged position. For example, the hotel industry encourages governments to pursue policies that would undermine Airbnb, under the guise of protecting consumers.

Taxicab companies are lobbying cities to regulate Uber, Lyft and other ride-sharing businesses in ways designed to cripple e-riding services. "The taxi industry has donated $3,500 to state legislators for every dollar that Uber, Lyft and their smaller competitor Sidecar have given, according to an analysis by the Sunlight Foundation."[137] Uber removed its services from Denmark after April 2017 "when fare meters and seat occupancy sensors became mandatory for all taxi services."[138] "A number of destinations have banned UberPop—a service that allows non-professional drivers to pick up paying customers using their own vehicles. Italy, France, the Netherlands and Finland have all banned UberPop."[139]

Brick and mortar liquor stores seek to stifle potentially disruptive rivals by mounting legal challenges to online wine sellers, resorting to the rationale that virtual sellers cannot sufficiently prevent minors from purchasing alcoholic beverages. Open competition, not governmental regulation, should determine which online services flourish and which ones go out of business.

Other ethical theorists disagree with the Libertarians, noting that mass-market software licenses impose terms on a "take it or leave it" basis, which is inconsistent with the libertarian assertion that these are truly voluntary agreements. In a *South Park* episode entitled "HUMANCENTiPAD," one character, Kyle, failed to read his iTunes terms of service and agreed to become a component in a web browser and emailing device that is part human and part centipede. The *South Park* episode parodies U.S. courts that mechanically uphold one-sided website terms.

(2) Cyberlibertarians

(a) Protecting the Free Flow of Information

A central tenet of traditional libertarianism is respect for private property. In contrast, cyberlibertarians take freedom one step further by arguing, "Information wants to be free." They are sympathetic to the anarchist motto that "property is robbery."[140] Activist hackers often "liberate" information that private organizations or governments wish to keep secret.

Cyberlibertarians agree with the traditional libertarian values of maximizing individual freedom and distrusting government. Like the traditional libertarians, they strongly support undermining established organizations through websites such as Kickstarter, which allows individuals and small entities to voluntarily fund startups without the need for government or venture capitalist financing. The website GoFundMe permits those in need of funding to make their case and gather voluntary contributions by posting an explanation of why donors should contribute to them.

Similarly, Lending Club, an online organization that enables individuals to borrow money from other individuals without the need for banks and other traditional lenders, is a free-market mechanism where willing borrowers and lenders reach voluntary agreements to lend money. Lending Club is now being accused of financial irregularities and inadequate security.[141] In August of 2022, the Federal Trade Commission returned $9.7 million as a second payment to 61,990 consumers harmed by the company's deceptive hidden fees.[142] A variety of rivals will emerge if this company fails to effectively exploit its first mover advantage.

Cyberlibertarians champion crowd sourcing of social control, instead of government actions, to police the Internet. Clay Shirky's 2008 cyberlibertarian book, *Here Comes Everybody: The Power of Organizing Without Organizations*,[143] explores "what happens when people are given the tools to do things together, without needing traditional organizational structures."[144] Netizens themselves should employ vigilante justice to punish online oppression. Predicting a future of "mass amateurization," Shirky uses the example of getting a lost cell phone returned by exposing the personal information of the unrepentant thief.[145]

Both types of libertarians support Bitcoin and other cryptocurrencies that shield individual privacy from governmental and corporate intrusion. Ross Ulbricht, the former owner of Silk Road, a DarkNet marketplace for the buying and selling of illicit goods, authored cyberlibertarian manifestos. Before Ulbricht was arrested and the Silk Road shuttered:

> There were 10,000 products for sale in the spring of 2013, 70% of which were drugs. But there were also 159 listings for "services," most of which were for hacking into social network accounts like Twitter or Facebook and more than 800 listings for digital goods such as pirated content, or hacked Amazon and Netflix accounts, according to the FBI indictment. Fake drivers' licenses, fake passports, fake utility bills and fake credit card statements.[146]

Merchants on the Silk Road website and its many successors are constrained by an evaluation system by which customers report on the quality of the providers' goods. The higher a seller's ratings, the more it can charge. Amazon, eBay and hosts of other legal companies use the same seller rating method. A seller with a record of reliably providing quality goods can profit from its sterling reputation. A provider without an established record of dependability may need to sell at a loss to build up its online reputation. Meanwhile, websites such as *RipOff Report* publish complaints that can constrain the sales of unethical online sellers.

(b) Cyberlibertarian Utopianism

In his article, *Cyberlibertarians' Digital Deletion of the Left*, David Golumba writes that:

> There are overt libertarians who are also digital utopians—figures like Jimmy Wales, Eric Raymond, John Perry Barlow, Kevin Kelly, Peter Thiel, Elon Musk, Julian Assange, Dread Pirate Roberts, and Sergey Brin and the members of the Technology Liberation Front who explicitly describe themselves as cyberlibertarians.[147]

Cyberlibertarian John Perry Barlow thundered, "On behalf of the future, I ask you of the past to leave us alone."[148] His utopian vision is an Internet free from censorship: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind." Barlow proclaimed that governments have no legitimate authority in cyberspace:

> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.[149]

Barlow's argument is that legitimate authority must come from the consent of Internet users around the world, not from legislators, judges or corporate giants. He wrote his famous Manifesto in response to the German government's prosecution of a Bavarian Internet service provider that enabled users to access Nazi memorabilia. By what authority can a Bavarian court order a U.S. service provider to block content to German citizens?

Barlow is also critical of governmental content regulations that constrain online political expression. Authoritarian regimes view the Internet as an existential threat and are quick to erect roadblocks and access controls to censor subversive content.

Libertarian-influenced privacy advocates, such as the Electronic Frontier Foundation, worry about the potential for widespread surveillance and the emergence of a new form of Jeremy Bentham's *Panopticon*. The design of the *Panopticon* was such that a single guard could watch the inmates without the inmates themselves knowing whether they were being watched. Cyberlibertarians fear that the Internet could become a similar total-controlling institution, used by elites to violate basic human freedoms.

(c) Cyberlibertarian Ethics

The cyberlibertarian perspective is seen in the hacker community's view of computer ethics, as illustrated in the chart below. In sharp contrast to computer industry ethical codes, which emphasize respect for intellectual property rights, the cyberlibertarian view is that property is communal, and information should be freely shared. Traditional libertarians see humans as naturally self-interested and are therefore skeptical of extreme cyberlibertarianism, believing that private property and the profit motive are the best defenses for individual freedom.

CYBER-LIBERTARIAN CODE OF ETHICS

The hacker community's computer ethics commandments challenge computer professional's core values:

(1) We believe: That every individual should have the right to free speech in cyberspace.

(2) We believe: That every individual should be free of worry when pertaining to oppressive governments that control cyberspace.

(3) We believe: That democracy should exist in cyberspace to set a clear example as to how a functioning element of society can prosper with equal rights and free speech to all.

(4) We believe: That hacking is a tool that should and is used to test the integrity of networks that hold and safe guard our valuable information.

(5) We believe: Those sovereign countries in the world community that do not respect democracy should be punished.

(6) We believe: That art, music, politics and crucial social elements of all world societies can be achieved on the computer and in cyberspace.

(7) We believe: That hacking, cracking, and phreaking [1970s practice of hacking telephone systems in order to get free long distance calls] are instruments that can achieve three crucial goals: (a) Direct Democracy in cyberspace; (b) The belief that information should be free to all; and (c) The idea that one can test and know the dangers and exploits of systems that store the individual's information.

(8) We believe: That cyberspace should be a governing body in the world community, where people of all nations and cultures can express their ideas and beliefs has to how our world politics should be played.

(9) We believe: That there should be no governing social or political class or party in cyberspace.

(10) We believe: That the current status of the Internet is a clear example as to how many races, cultures and peoples can communicate freely and without friction or conflict.

(11) We believe: In free enterprise and friction-free capitalism.

(12) We believe: In the open source movement fully, as no government should adopt commercial or priced software for it shows that a government may be biased to something that does not prompt the general welfare of the technology market and slows or stops the innovation of other smaller company's products.

(13) We believe: That technology can be wielded for the better placement of man kind and the environment we live in.

(14) We believe: That all sovereign countries in the world community should respect these principles and ideas released in this constitution.[150]

Lawrence Lessig charges cyberlibertarians with extreme naiveté: "Cyberspace, it is said, cannot be regulated. It 'cannot be governed;' its 'innate ability' is to resist regulation. In its essence, cyberspace is a space of no control."[151] A change in the architecture of the Internet could radically restrict the freedoms of users. For example, message content can be scanned to increase social control or to manipulate customers.

The potential of the Internet to become a technology of social control, disinformation and oppression is the great fear of both traditional and cyberlibertarians. All authority is distrusted, even when it claims to be benevolent, which is inconsistent with clauses in the ACM Code of Ethics. Principle 1.6, for example, requires professionals to "Respect privacy" and Principle 1.7, which mandates "Honor confidentiality." Cyberlibertarians have no problem with people who illegally break into corporate and governmental data bases to expose wrongdoing by the powerful.

The hacktivist group, Anonymous, for example, is aggressively attacking Russian websites to sabotage that nation's invasion of Ukraine. Anonymous posted a tweet calling for hackers around the world to target Russia. "Subsequent posts claimed the group was responsible for pulling down websites of the Russian oil giant Gazprom, the state-controlled Russian news agency RT and numerous

Russian and Belarusian government agencies."[152] "Anonymous also took credit for disrupting Russian internet service providers, leaking documents and emails from the Belarusian weapons manufacturer Tetraedr, and shutting down a gas supply provided by the Russian telecommunications service Tvingo Telecom."[153]

[I] Learning from Multiple Perspectives

Science fiction writer James Gunn wrote *The Immortals* in which an impoverished drifter has a uniquely valuable blood variation that can temporarily cure any illness in those who receive a transfusion.[154] The ideal type of consequentialist would favor capturing him for study and extracting his blood for the greater good because his plasma would save thousands of lives. His sperm might be extracted to maximally breed him in the hope that his offspring would inherit the same ability to produce this invaluable blood.

The other four perspectives, in contrast, would reject this extreme violation of the drifter's rights, no matter what the social benefits, as it is morally wrong to use another human being as merely a means to a broader societal end. The conflict perspective would abhor solutions that would allow the rich to live for centuries, while the poor die early deaths.

All five of the ethical perspectives agree that powerful corporations must be opposed when they seek to illegitimately stifle critics of their products and services. However, where the line is drawn depends on the ethical perspective of the decision maker. One prominent example of this is when copyright owners representing the film and music industries aggressively seek to unveil anonymous file sharers. Courts issuing these subpoenas to reveal posters' identities must balance the privacy rights of anonymous speakers against the right of owners to protect their intellectual property.

Except for the libertarians, the great majority of computer ethicists would agree that society must deter and punish certain bad behaviors, which may call for suppressing the worst excesses of free expression. Most Americans recognize that even though free expression is both useful and a core societal value, too much Internet freedom can be socially costly. Terrorists, state-sponsored criminals, brutal racists and sexual predators exploit online anonymity to spread hate speech and undermine legitimate governments.

Particularly ironic is the fact that the U.S. Navy invented and protects Tor (a name taken from the initials of "The Onion Router"), which is the preeminent anonymizing software. At the same time, the U.S. National Security Agency and its UK counterpart are attempting to de-anonymize Tor because the service enables illicit messaging by terrorists and other cybercriminals. Illegal online marketplaces thrive because Tor allows them to operate beyond the reach of any nation's law.

Some computer professionals contend that all laws should be obeyed, regardless of a programmer's opinion about their reasonableness. Other information ethicists, especially the cyberlibertarians, contend that a principled programmer must use her professional judgment and, if necessary, resist immoral laws. Computer professionals, like any other group, have the right to call for law reform, but they must obey the law or face potential punishment.

The ACM Code of Ethics & Professional Conduct recognizes this duty to obey the law. The ACM Code of Ethics requires computer professionals to know and comply with applicable local, regional, national, and international laws and regulations, as well as any policies and procedures of the organizations to which the professional belongs.[155]

§ 2.2: THE FUTURE OF COMPUTER ETHICS

[A] Martin's Programmer's Oath

Professional associations often play a key role in providing guidance to practitioners faced with ethical challenges and to lawmakers attempting to regulate controversial practices. The computer profession will not become a true profession without a code of ethics, a professional association that enforces them, and a certification system for qualified members. Canada is the first country to certify information professionals:

> A local and national association of Computer Scientists needs to be established consisting of a well-organized group of people who follow codes of ethics and standards created and maintained by the professional association. An example of a professional association is Canada's Association of I.T. Professionals that provide certification like Information Systems Professional (ISP) and Information Technology Certified Professional (ITCP) for I.T. professionals.[156]

Robert Martin, popularly known in computer circles as "Uncle Bob," in a November 2016 episode of his "The Future of Programming" series, argued for the necessity of computer professionals organizing into a formal profession.[157] Martin has proposed a nine-element Programmer's Oath to "defend and preserve the honor of the profession of computer programmers."[158] Martin's aspirational code of conduct for programmers written in the form of commandments is reprinted below:

ROBERT MARTIN'S PROGRAMMER'S OATH

In order to defend and preserve the honor of the profession of computer programmers,

I Promise that, to the best of my ability and judgment:

(1) I will not produce harmful code.

(2) The code that I produce will always be my best work. I will not knowingly allow code that is defective either in behavior or structure to accumulate.

(3) I will produce, with each release, a quick, sure and repeatable proof that every element of the code works as it should.

(4) I will make frequent, small releases so that I do not impede the progress of others.

(5) I will fearlessly and relentlessly improve my creations at every opportunity. I will never degrade them.

(6) I will do all that I can to keep the productivity of myself, and others, as high as possible. I will do nothing that decreases that productivity.

(7) I will continuously ensure that others can cover for me, and that I can cover for them.

(8) I will produce estimates that are honest both in magnitude and precision. I will not make promises without certainty.

(9) I will never stop learning and improving my craft.

To qualify as a profession, the computer field needs a code of ethics with an enforcement mechanism, not just broad aspirational principles as in the programmers' oath. In March 2022, Robert Martin updated his demand for a professional code of ethics, predicting that a major software defect causing widespread damage will lead to pressure for legislators to hastily enact legislation:

> Currently, software developers carry the lifeblood of civilization. Nothing can function without software, and developers' behavior isn't in line with that responsibility. I want us programmers to behave in a stalwart way, and acknowledge our responsibility, which is likely to keep growing. There have been high-profile calamities caused by software

> over the past decades. Software developers need to start discussions about what may be done before a disaster happens that takes control out of our hands. For example, most modern cars have some level of automatic control. There are computers exerting that control over the head of the driver or in response to the driver. This level of control raises ethical questions even before we build fully autonomous cars. I expect a disaster to happen eventually that overtakes politics and causes legislation to constrain the software industry. We need to get ahead of this and be ready with a code of ethics and a set of standards by the time the politicians come to regulate us.[159]

A coding error, like the one alleged in Toyota's class action litigation over the sudden, unintended acceleration of its cars, could result in a substantial number of fatal crashes. Toyota Motors of North America later settled the class action for an estimated $1.2 to $1.4 billion.[160] Toyota's Chief Legal Officer claimed that "reliable scientific evidence and multiple independent evaluations have confirmed the safety of Toyota's electronic throttle control systems."[161] The company settled the case, he stated, only because "we concluded that turning the page on this legacy legal issue through the positive steps we are taking is in the best interests of the company, our employees, our dealers and, most of all, our customers."[162]

In 2014, emergency dispatch centers serving eleven million Americans in six states were disabled by a coding error. Programmers had capped the number of 911 calls at an arbitrary number in the millions, which was reached, shutting down the system.[163] Key systems that formerly were controlled by humans are now software-driven. On a single day in 2015:

> United Airlines grounded its fleet because of a problem with its departure-management system; trading was suspended on the New York Stock Exchange after an upgrade; the front page of *The Wall Street Journal's* website crashed; and Seattle's 911 system went down again, this time because a different router failed.[164]

[B] The Need for Computer Professional Ethics

Computer professionals must adopt high ethical standards, Bob Martin argues, or face having lawmakers impose rules upon them when, inevitably, a serious software error results in widespread injuries or serious economic damages:

> Other people think they write the rules; but then they hand those rules to us, and we actually write the rules that make the machines work. We rule the world. With that great power ought to come great responsibility.

> And, indeed, society will hold us responsible when our actions result in disaster. And yet nothing binds us together as a profession. We share no ethics. We share no discipline. We share no standards. We are viewed, by our employers, as laborers. We are tools for others to command and use. We have no profession. This cannot continue. If we do not form a profession on our own, then society will force it upon us—and define it for us. And that will be good neither for society, nor for us. We must get there first.[165]

Several U.S. engineering associations, which include software professionals among their membership, have aspirational, though not legally binding, codes of ethics. The National Society of Professional Engineers (NSPE) is an American group representing licensed professional engineers. Engineering.com describes NSPE as "the recognized voice and advocate of licensed Professional Engineers," represented in 52 state (and territorial) organizations and over 400 local chapters.

The NSPE Code is standards-based rather than rules-based. Its ethical code draws from the Virtue and Duty perspective, calling for its membership to exhibit "honesty, impartiality, fairness and equity, and must be dedicated to the protection of the public health, safety, and welfare."[166]

The province of Ontario, Canada recognizes legally enforceable ethical codes that parallel the practices of the medical and legal professions. The Professional Engineers Ontario (PEO) has been empowered for more than ninety years by the province's Professional Engineer Act[167] to license and discipline engineers. Only those licensed by the PEO can offer engineering services and take responsibility for professional engineering work in the province.

In addition to educational requirements, applicants for an Ontario Engineering License, the candidate must pass the Professional Practice Examination (PPE), "a three-hour, closed-book exam on ethics, professional practice, engineering law and professional liability."[168] The PEO's Code of Ethics requires that engineers demonstrate fairness and loyalty to "associates, employers, clients, subordinates and employees" and "fidelity to public needs."[169]

The high ethical standards expected of engineers are reinforced by universities throughout Canada, whose graduates participate in a symbolic Ritual of the Calling of the Engineer, a private ritual written by Rudyard Kipling. All Canadian engineering graduates receive an iron ring, which symbolizes their commitment to a high standard of professional ethics.

The iron ring is the new engineering graduate's reminder of their duty to conduct themselves ethically in their professional and personal life. Unethical behavior will be investigated by the PEO and can result in the temporary or permanent withdrawal of the right to practice engineering in Ontario, in a monetary fine, and/or the publication of the engineer's failings, among other possible punishments.[170]

Some commentators argue that programming is essentially different from traditional engineering. New regulatory models need to be devised for this unique profession. Perhaps the label "software developers" is better than "software engineers" because it suggests the need for a fresh look at how the law should operate.

A discussion about whether U.S. software engineers should form a strong professional organization went viral on *Hacker News* in the wake of a November 2016 essay by Bill Sourour, entitled, "The Code I'm Still Ashamed of."[171] Sourour regrets an online questionnaire he programmed more than a decade earlier, which appeared to be an informative diagnostic tool, but was actually designed to promote the financial interests of a pharmaceutical company. Respondents received a recommendation that they should be taking his client's powerful antidepressant in response to almost any possible combination of answers to the questionnaire.

The covert goal was to boost sales of a profitable anti-depressant drug, even though it had potentially fatal side effects. Sourour concluded, "The more software continues to take over every aspect of our lives, the more important it will be for us to take a stand and ensure that our ethics are ever-present in our code."[172] Computing boot camps should expand their mission beyond straightforward technical training to a discussion of ethical issues. Sourour later authored The Trustworthy Coder's Pledge,[173] as a set of ethical touchstones. Most of his ideas are incorporated into the far more comprehensive ACM Code of Ethics and Professional Conduct.

The Trustworthy Coder's Pledge

I do hereby pledge to only produce trustworthy software that respects its users.

Such software will:

- be transparent, honest, and accountable in all user communication;
- function exactly as described;
- seek explicit user consent prior to collecting any user information; including both user-provided information and

information collected from a user's device or through integration with other services;

- seek explicit user consent prior to sharing any and all user information;
- use clear and plain language when seeking user consent;
- describe in clear and plain language what user information is collected and how;
- describe in clear and plain language where, when, and how any user information will be used;
- make it easy for users to withdraw consent at any time;
- make any user-generated content available for download by the user who generated it, free of charge, any time, with no restrictions;
- clearly identify any advertising or sponsored content;
- provide a simple, easy-to-use, and easy-to-find mechanism for users to opt out of any advertising or marketing;
- completely delete any and all user information upon request by the user; and, clearly and explicitly disclose any and all potential conflicts of interest including both conflicts that may arise through commercial interests and conflicts that may arise through political affiliation.

Some computer scientists believe that without a professional organization that can assert moral or disciplinary authority, ethical software engineers are disempowered because unscrupulous employers can easily find a less ethical replacement for those not following company orders. Without legal enforcement, the ethical code is ineffective because it's easy to fall into the trap of thinking that just because a job is legal and has a steady paycheck, the company is ethical.

One commentator echoed the Conflict perspective when he stated: "The most effective way to change the world, in my opinion, is to push for political and social changes that change incentives in a manner that reduces the number of unethical economic niches that exist for the necessity of social change."[174] This raises a much larger issue, to be discussed in subsequent chapters, of whether recent advances in artificial intelligence and the Internet of Things require significant modifications of contemporary society to avoid creating a large class of permanently disempowered individuals.

Libertarian-style resistance to the establishment of legally enforceable codes of ethics reflects an individualistic streak possessed by many programmers, who want no oversight by a professional organization. One commentator argued that, in reality, the Ontario board acts to limit competition by artificially restricting the number of engineers who can work in the province.

Milton Friedman, a free market economist, criticized laws controlling who can practice in a profession as the "tyranny of the status quo."[175] Friedman believed that established special interest groups protect their privileged status—and generous paychecks—by using legal restrictions to block innovations that threaten the profession's profits.

[C] ACM Code of Ethics Provisions Applied

Section 2.8 of the ACM Code of Computer Ethics and Professional Conduct (ACM Code of Ethics) requires computer professionals to deploy their computing skills for the public good, which clashes with libertarian freedoms. Section 2.8 states: "Access computing and communication resources only when authorized or when compelled by the public good."[176] Computer professionals need to balance profit motives with the public good to comply with this admonition.

Computer professionals must: "Design and implement systems that are robustly and usably secure."[177] A programmer has an ethical responsibility not to engage in cover-ups of malfunctioning software and a duty as a whistleblower to minimize harm to the public of defective software. Because the cover-up of defective software is hard to discover, perhaps enhanced financial awards for whistleblowing would be particularly effective.

Section 2.7 of the ACM Code of Ethics imposes a duty to foster public understanding of computing. This section requires computer professionals to: "Foster public awareness and understanding of computing, related technologies, and their consequences."[178] This ethical duty would require a computer professional to be forthcoming about defects in software. Writing a list of vague admonitions suggesting that programmers should pursue a variety of virtues, such as "protecting the public interest," "refusing unethical assignments," "acting with honor and integrity," and "promoting fairness," is easy.

Producing laws that will punish those who violate these aspirational principles is extremely difficult. The following chapters of this book will discuss how the legal system is evolving to advance the public interest, regulate unethical online behavior and control the misdeeds of cybercriminals.

As societal dependence on reliable computer systems advances at an ever-increasing pace, the legal order will require the continuous updating of computer ethics to operationalize new dilemmas. This book is designed to provide a survey of the existing legal structure so that practitioners will know what they are allowed to do, victims will understand what defenses are available and policymakers will understand the successes and shortcomings of the current legal code.

CONCLUSION

Computer ethics is an applied field that examines moral and legal issues raised by advances in computers, software and information technologies. This chapter introduced five leading theories of ethics: (1) Consequentialism; (2) Virtue and Duty Ethics; (3) Conflict Perspective; (4) Social Contract Theory; and (5) Libertarianism. These ethical perspectives embody divergent ways of conceptualizing and resolving moral dilemmas. The contemporary debates discussed in subsequent chapters will demonstrate the value of approaching ethical problems from multiple vantage points. Our overarching argument is that the most useful insights often arise from combining the most relevant features of several perspectives.

This book is designed to help develop and refine your critical thinking skills and your ability to make persuasive arguments about the best approaches to the ethical quandaries that will inevitably arise as the digital era progresses. Radical advances in information technology are continuously producing unique moral challenges that will require the rethinking of the laws and regulations governing knotty topics such as online privacy, Internet security, intellectual property and computer contracts.

In the following chapters, you will learn about applying independent judgment and complying with the ethical and legal dimensions of issues such as peer-to-peer file sharing, Internet crime, employee surveillance, human rights and the hazards of simultaneously operating under the laws of multiple nations. The phenomenal growth in traffic on the Internet requires that all branches of the law be adapted to globalized cyberspace.

Information professionals, lawyers and informed citizens will be called upon to determine how to maximize the benefits that can arise from the Fourth Industrial Revolution. Section 2.5 of the ACM Code requires computer professionals to exercise their independent professional judgment using objective standards to serve their clients. Computer professionals are to: "Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks."[179]

Everyone will need to become increasingly globally minded. Information technology has a great potential to increase international cooperation, coordination and mutual prosperity. However, to achieve this goal, Internet governance must agree on the basic ethical and legal rules that will apply in the information age. A leading online privacy advocate makes the case for greater transparency by U.S. companies because data on the Internet crosses national borders:

> The continued sale of sensitive data could present its own privacy and security concerns, and the news highlights that ISPs are providing this data at scale to third parties likely without the informed consent of their own users. But it remains entirely possible to craft comprehensive, basic federal rules that, at the very least, mandate absolute transparency with the end user. Instead of doing what we've created with a wild west-like ecosystem of app makers, phone makers, software giants, telecoms and others, selling every shred of data they can find, often failing to adequately secure it, and with consumer protection (or even awareness) a distant, belated afterthought.[180]

Legal developments in one nation have cascading effects worldwide. For example, the "current U.S. regulatory landscape hinders the competitiveness of U.S. digital asset businesses' due to the uncertain application and incompatibility of existing laws and regulations to digital assets and their underlying infrastructure."[181] The danger is that financial and intellectual capital will "be disproportionately driven to other jurisdictions."[182] The weak U.S. tradition of protecting data privacy will increasingly become a global trade barrier. To transfer or not transfer personal data to the U.S., that is the question.[183]

The question set at the end of this, and all subsequent chapters, are designed to help you operationalize ethical principles such as the ACM Code of Ethics to real world dilemmas. In answering these questions, consider how the public good would be impacted by your decisions. To quote prolific inventor and head of research for General Motors, Charles Kettering, "we should all be concerned about the future because we will have to live the rest of our lives there."[184]

CHAPTER TWO: REVIEW EXERCISES

2.1: "In the classic science-fiction film '2001,' the ship's computer, HAL, faces a dilemma. His instructions require him both to fulfill the ship's mission (investigating an artifact near Jupiter) and to conceal the mission's true purpose from the ship's crew. To resolve the contradiction, he tries to kill the crew. As robots become more autonomous, the notion of computer-controlled machines facing ethical decisions is moving out of the realm of science fiction and into the real world. Society needs to find ways to ensure that they are better equipped to make moral judgments than HAL was."[185] What would a duty-based deontologist, a consequentialist and a libertarian say about HAL's actions? How much autonomy should computers be allowed to make life and death choices? Please explain.

2.2: Armed drones were deployed in Afghanistan to attack Taliban and Al Qaeda leaders.[186] From each of the five ethical perspectives, what factors should be considered for the deployment of autonomous drones in warfare?

2.3: Consider the computer game, Fallout 3. In the Tenpenny Tower quest, players "find a building in which the dream of a time past is preserved. The dominant cast keeps the population happy but scared. They prevent riots by presenting the ghouls that roam just outside the residence as the enemy. Throughout the game, however, ghouls are presented as mostly pacific denizens. In this quest, players face a dilemma: They can eliminate all ghouls in the proximity of the Tower, help the ghouls kill the humans, or negotiate peace between both."[187] How would supporters of the five ethical perspectives approach this issue in a real-life scenario? How can it best be resolved? Please explain.

2.4: Should game designers and software engineers have a higher duty to produce ethical software products that teach lessons in morality? In Gamergate, women were harassed with violent threats for suggesting that online games should be more socially complex and contextual.[188] Conflict theory would see this as suppression of females at the hands of privileged males. How might this be approached from the other four perspectives?

2.5: "While ethics courses have become a staple of physical-world engineering degrees, they remain a begrudging anomaly in computer science pedagogy."[189] Should all Computer Science Departments require a course that applies ethical principles to real-life dilemmas they will face in their professional life?

2.6: "On the Internet, 'free' services abound. The question of where the money will come from is often put off, being off-putting. We just build the amazingness, keep an eye on the adoption metrics, and figure someone else will take care of the dirty work of keeping the server lights on. Worst case, there are always ads."[190] Do software developers have any ethical obligations in creating "free services" that are not really free? Do developers have any obligation to provide users with minimum mandatory disclosures about how they make their profits? What would the ethics theorists say about companies that trick consumers into downloading software, a practice called drive-by downloads?

2.7: In his science fiction story, *I Robot*, Isaac Asimov created three laws of robotics. The Three Laws from Asimov's "Handbook of Robotics, 56th Edition, 2058 A.D." are:

> (1) A robot may not injure a human being or, through inaction, allow a human being to come to harm.
>
> (2) A robot must obey the orders given it by human beings except where such orders would conflict with the First Law.
>
> (3) A robot must protect its own existence as long as such protection does not conflict with the First or Second Laws.

Fast forward six decades after Asimov wrote *I Robot*. Now, "ethical subroutines may sound like science fiction, but once upon a time, so did self-driving cars."[191] What ethical rules apply to the following scenario? "Your car is speeding along a bridge at fifty miles per hour when an errant school bus carrying forty innocent children crosses its path. Should your car swerve, possibly risking the life of its owner (you), to save the children, or should it keep going, putting all forty kids at risk? If the decision must be made in milliseconds, the computer will have to make the call."[192] Do you believe that people will buy vehicles programmed to sacrifice passengers over bystanders?

2.8: We are far from programming a robot that would refuse to harm humans. Is it even desirable to program a robot to never harm a human? Would a virtue theorist prevent a robotic sniper from killing a terrorist who has taken a group of preschoolers hostage? In Isaac Asimov's short story, "Liar," a robot lies to protect its programmer from psychological harm that would come from knowing the truth. What are the ethical issues raised by this hypothetical?

2.9: What rules need to be formulated to prevent journalists from violating the privacy of celebrities? Should there be different rules for using drones to follow public officials who are suspected of corruption or treason? Does your answer change if an investigative journalist uses drones to learn about the illegal activities of a toxic waste recovery company? Suppose this is a contested divorce case, in which a spouse wishes to prove her spouse's secret liaisons. Should a court allow evidence collected by a drone documenting a spouse's illicit affair? Please explain.

2.10: In the 1950s and 1960s, the American automobile industry blamed the epidemic of car accidents on driver error and bad roads to deflect attention away from design defects that created excessive, preventable dangers. Automobiles in this era were not even equipped with safety glass, let alone seatbelts. Today's automobiles are much safer because products liability exposed such flaws and encouraged the auto industry to adopt improved designs. Is it now time to extend products liability to include insecure or dangerously defective software?[193] Will greater liability have a negative impact on new software products? What would a libertarian and a consequentialist say about imposing products liability on software programmers, developers, and intermediaries in the stream of distribution?

2.11: California was the first state to enact a statute requiring companies to notify consumers of computer security breaches. The Business Roundtable opposes "breach notification laws requiring companies to report computer security breaches or implement minimum security standards because these obligations may lead to greater litigation costs." Some consumers, particularly those who know little about computers, may be needlessly alarmed by such a notification. What are the ethical issues in imposing an obligation to notify consumers of any breach of the security of their data?

2.12: A leading commentator wrote: "the software industry is no longer in its infancy. Its development has moved out of garages and into corporate offices. It has matured to become a dominant sector of the economy. Consequently, it is appropriate to consider liability for defective software in the same light as liability for defective automobiles, pharmaceuticals and other products."[194] What is the case for and against imposing greater liability on software makers when they market defective products? Are there any reasons to shield the software industry, while holding other manufacturers accountable, when defectively designed software causes injury or death?

2.13: Chapter 1 argued that law and medicine are professions because of having implemented a standard curriculum of study, post-graduate certification tests and enforceable model rules of discipline. Do you think that computer professionals' codes of ethics will be recognized by the courts in the near future? Should computer scientists organize themselves into a traditional profession? Why or why not?

2.14: Should there be a legal duty requiring that Internet Service Providers (ISPs) help trace the true identity of anonymous posters of hate speech? What would the five perspectives say about this issue? As the next chapter will explain, U.S. ISPs and other intermediaries have no legal duty to unveil anonymous posters for any reason? ISPs are shielded from liability by Section 230 of the Communication Decency Act. Should Congress amend CDA Section 230 to impose a duty to unveil anonymous individuals who post hate speech? What would be the practical problems for the ISP responding to a subpoena to unveil a poster of hate speech or other illegal content?

2.15: A John Doe, or anonymous poster, described a Dunkin Donuts shop the plaintiff owned as one "of the most dirty and unsanitary-looking food-service places he had ever seen." The owner of the franchise wishes to file a subpoena to the news website where the statement was posted to unveil the identity of the anonymous critic. A subpoena is a request to produce documents, or a request to appear in court or other legal proceeding. In this case, the subpoena would be issued to the news group, requiring it to reveal the identity of the poster of the derogatory statements about the plaintiff's shop. The franchise operator suspects that the owner of a rival coffee shop posted the message. What factors should courts consider in deciding whether to issue the subpoena to unmask the anonymous poster?

2.16: Frank Fortran, a computer professional, was assigned to evaluate a computer program that the company was considering purchasing. His supervisor had no knowledge that Carl's brother-in-law was the program designer. Does Frank owe an ethical duty to reveal his conflicts of interest? Please discuss any ethical principles that might apply.

2.17: Please respond to the following statement: "People who think about machine ethics make it sound like you can come up with a perfect set of rules for robots, and what we show here with data is that there are no universal rules." Please critically evaluate this statement giving examples. Do any of the principles of the ACM Code of Ethics apply?

2.18: Big Computer Company (BCC) has no female, minority or disabled programmers. BMC claims that they hire computer programmers solely on their experience and skill set. They also claim that their hiring decisions do not discriminate against anyone based on age, color, disability, ethnicity, family status, gender identity, labor union membership, military status, national origin, race, religion or belief, sex, sexual orientation or any other inappropriate factor. How should a court determine whether BCC discriminates given empirical evidence of an all-male work force?

2.19: Big Computer Company requires all its software engineers and programmers to assign authorship, copyrights, patents, trade secrets and other intellectual property rights to the company. BMC places its name on all patent and trademark applications and the creators are given no credit. The company's view is that they it owns all intellectual property created by its employees. Has BMC violated the ACM Code of Ethics discussed in Chapter 1? If so, what provision of the ACM Code of Ethics has the company violated in asserting that it owns all rights to intellectual property created by employees? Would it make a difference if the intellectual property were conceived during an employee's free time weekends? Please explain.

2.20: Big Computer Company (BCC) has created computer software that enables the compilation of personal information instantly, inexpensively, and without the knowledge of its employees. BCC's software surreptitiously captures each key stroke of all employees, supposedly to prevent the theft of intellectual property. The retention and disposal periods for stored keystrokes is not clearly defined, enforced, nor communicated to data subjects. Has BMC violated the ACM Code of Ethics by its keystroke monitoring of its employees?

2:21: Frank Fortran is working on a software project financed by the Department of Defense. Frank signed a nondisclosure agreement (NDA) that precluding him from disclosing anything he has learned on this project to anyone other than his governmental client. One day he detected that another programmer was using an unlicensed software program. Neither the company nor the employee had an express or implied license to use this software. Is Frank bound by the NDA he signed to not report his co-employee's copyright infringement? Would making a disclosure to appropriate authorities be in harmony with the ACM Code of Ethics? Consider thoughtfully whether such disclosures will violate his ethical duties.

2.22: Section 2.3 of the ACM Code of Ethics states that computer professionals must: "Know and respect existing rules pertaining to professional work." One of the norms of Big Computer Company is to meet all project deadlines "come hell or high water." Due to the illness of a key software engineer, the company was way behind and was going to miss an important benchmark. Frank Fortran was told to "chance it" rather than to adequately test the application in its environment of use. BCC met the benchmark by cutting corners with the result that the released software product had a serious design defect that would have been uncovered with adequate testing. Should Frank have spoken up challenging management's decision to "chance it" that resulted in the company releasing dangerously defective code into the marketplace. Should Frank have taken the time to adequately test the software, even if it cost him his job?

2.23: "What technological breakthrough has enabled this huge increase in performance?" The CEO replies, "We have created a new biological chip with lab-grown human neurons. These biological chips are better than silicon chips because they can change their internal structure, adapting to the user's usage pattern and resulting in huge efficiency gains."[195] What ethical and legal concerns apply to computers using human brain matter?

2.24: Koniku, another company that makes computers from lab-grown neurons, believes its technology will revolutionize several sectors, including agriculture, healthcare, military technology and airport security.[196] What would a consequentialist, libertarian, and a conflict theorist say about this development? Please explain.

2.25: "Scientists can create cells from blood samples or skin biopsies into a type of stem cell that can become any type of cell in the human body. However, this raises questions about donor consent. Do people who provide tissue samples for research and technology development know that they could be used to make neural computers? Must information be disclosed for their consent to be valid?"[197] What ethical or legal issues apply to using human cells to make neural networks?

2.26: Target suffered a computer intrusion in 2013 that exposed 110 million sets of credit/debit card details. Should a software designer be liable for design flaws that enabled the cybercriminals to steal the data of millions of consumers? Should software products liability address substandard software security, where there is no personal injury or death.

REFERENCES FOR CHAPTER TWO

[1] *Fourth Industrial Revolution,* WORLD ECONOMIC FORUM (2022), https://www.weforum.org/focus/fourth-industrial-revolution?page=185.

[2] *ACM Code of Ethics & Professional Conduct*, Commentary to § 3.1.

[3] Karl Bode, *ISPs Give 'Netflow Data' To Third Parties, Who Sell It Without User Awareness or Consent*, TECHDIRT (Aug. 25, 2021).

[4] Moshe Y. Vardi, *ACM, Ethics, and Corporate Behavior,* COMMUNICATIONS OF THE ACM, Vol. 65 No. 3, Page 5 (March 2022).

[5] Louis Kaplow*, Rules Versus Standards: An Economic Analysis*, 42 DUKE LAW JOURNAL 557–629 (1992).

[6] Hans Greimel, *Automakers Rush to Take Back Their Software Codes*, AUTOMOTIVE NEWS (Oct. 12, 2020).

[7] Stephen Edelstein, *Ford's New GT Has More Lines of Code Than a Boeing Jet Airliner,* DIGITAL TRENDS (May 21, 2015), https://www.digitaltrends.com/cars/the-ford-gt-uses-more-lines-of-code-than-a-boeing-787/.

[8] *Australia: Waymo Receives Patent for 'Dynamic Routing for Autonomous Vehicles'*, GOV AUSTRALIA LIVE (Apr. 25, 2020) (available on WESTLAW NEWS).

[9] Baystreet Staff, *6 Players Shaping the Future of Transportation*, BAYSTREET WIRE (Apr. 22, 2020) (available on WESTLAW' NEWS).

[10] Shannon Flynn, *What Are the Risks of Cloud-Connected Vehicles*, MUO (Sept. 28, 2021).

[11] *Id.*

[12] John Keenan and Alfred Ng, *Who Is Collecting Data from Your Car?*, THE MARKUP (July 27, 2002).

[13] Marguerite Reardon, *Why Biden's Broadband Agenda Is at a Do-or-Die Moment*, CNET (July 16, 2022).

[14] NPDB: National Practitioner Data Base, *About Us*, U.S. DEP'T OF HEALTH & HUMAN SERVICES (2022).

[15] Matt Stout, *Stalled 'Revenge Porn' Bill Keeps Mass. an Outlier on Law,* BOSTON GLOBE (Aug. 6, 2022).

[16] *United States v. Streatt*, 434 F. Supp. 3d 1125, 1142 (D. N.M. 2020).

[17] *Felony Charge for Sexting Unfair* Teens, UNIVERSITY WIRE (Sept. 16, 2020) (quoting Kentucky's sexting statute drafter Sen. Joe Bowen, R-Owensboro).

[18] *United States v. Streatt, Id.* at 1142.

[19] *Id.*

[20] *Id.* at 1132.

[21] *Id.*

[22] *Id.*

[23] *Id.*

[24] *Id.*

[25] *20,000 Reports of Coerced 'Self-Generated' Sexual Abuse Imagery Seen in First Half of 2022 Show 7- to 10-year-olds—Internet Watch Foundation*, WOMEN'S NEWS (Aug. 15, 2022).

[26] 18 U.S.C. § 2251(a).

[27] 18 U.S.C. § 2256(2)(A).

[28] *Why Is Sexting Illegal*, LEGAL MATCH (2022).

[29] *United States v. Streatt*, 434 F. Supp. 3d 1125, 1142 (D. N.M. 2020).

[30] *What Is Sextortion?,* FBI.

[31] *Id.*

[32] Matthew H. Birkhold, *Freud on the Court: Re-interpreting Sexting & Child Pornography Laws*, 23 FORDHAM INTELLECTUAL PROPERTY, MEDIA, AND ENTERTAINMENT LAW JOURNAL 897, 905 (2013).

[33] Kiley Crossland, *Should Sexting Teens Be Charged with Child Pornography?*, WORLD (Nov. 18, 2015).

[34] *United States v. Streatt*, 434 F. Supp. 3d 1125, 1142 (D. N.M. 2020).

[35] *Id.* at 1143.

[36] See generally, *Poker Bluffing*, RED SHARK POKER (2021).

[37] Eugene Kim, *Why Silicon Valley's Elites Are Obsessed with Poker*, BUSINESS INSIDER (Nov. 2, 2014).

[38] Sabla Priyadarshini, *Weber's Ideal Types: Definition, Meaning, Purpose, and Use* (2016).

[39] *Ideal Type*, ENCYCLOPEDIA BRITANNICA (2016).

[40] *Id.*

[41] Editors of the Encyclopedia Britannica, *Deontological Ethics*, Encyclopedia Britannica.

[42] *Slaughterbutler v. Horton*, No. 2:18–cv–24, 2022 U.S. Dist. LEXIS 118073 (W.D. Mich. July 6, 2022).

[43] Johnathan Riley, *Utilitarianism and Economic Theory*, THE NEW PALGRAVE DICTIONARY OF ECONOMICS (Feb. 15, 2018).

[44] Ashley Crossman, *Understanding Conflict Theory,* THOUGHT COMPANY (July 3, 2019).

[45] *Ethics Explainer: Consequentialism,* THE ETHICS CENTER (Feb. 15, 2016).

[46] *Id.*

[47] *Id.*

[48] JOHN STUART MILL, UTILITARIANISM (1863) at Chapter Two.

[49] *Id.*

[50] Haye Kesteloo, *Department of Defense Supports Use of Drones to Map California Wildfires,* DRONEDJ.COM (June 2, 2019) (quoting Adj. Gen. David Baldwi).

[51] DW Bureau. *Killer Robots: Will They Be Banned?*, DTNEXT (July 26, 2022).

[52] Chris Pash, *The World's Top Artificial Intelligence Companies Are Pleading for a Ban on Killer Robots*, BUSINESS INSIDER (Aug. 21, 2017).

[53] *Id.*

[54] John Stauffer, *Stopping Killer Robots: Country Positions on Banning Fully Autonomous Weapons and Retaining Human Control*, HUMAN RIGHTS WATCH (2020).

[55] *Killer Robots: Will They be Banned?,* DW.COM (July 26, 2022).

[56] JOHN MARKOFF, MACHINES OF LOVING GRACE: THE QUEST FOR COMMON GROUND BETWEEN HUMANS AND ROBOTS (New York, New York: Harper/Collins Publishers 2015) at 327.

[57] *Utilitarianism*, *Ethics Unwrapped*, MCCOMBS SCHOOL OF BUSINESS (2022).

[58] BBC, *About Consequentialism*, *Id.*

[59] PETER K. MCINERNEY & GEORGE W. RAINBOLT, ETHICS (New York, New York: Harper Perennial, 1994) at 90.

[60] Tim C. Mazur, *Lying*, MARKKULA CENTER FOR APPLIED ETHICS, SANTA CLARA, CALIFORNIA: SANTA CLARA UNIVERSITY (2016).

[61] *What Would Kant Do When Two Categorical Imperatives Conflict? Could He Ever Justify Lying?*, http://philosophy.stackexchange.com/questions/259/what-would-kant-do-when-two-categorical-imperatives-conflict-could-he-ever-just.

[62] Helga Vardon, *Kant and Lying to the Murderer at the Door. . . One More Time: Kant's Legal Philosophy and Lies to Murderers and Nazis*, 41 JOURNAL OF SOCIAL PHILOSOPHY 403 (Winter 2010).

[63] RALPH C.S. WALKER, KANT: THE ARGUMENT OF THE PHILOSOPHERS (London, Henley and Boston: Routledge and Kegan Paul, 1978) at 151.

[64] EDWIN PATTERSON, JURISPRUDENCE: MEAN AND IDEAS OF THE LAW (Brooklyn, New York: The Foundation Press, Inc., 1953) at 341 (discussing Aristotle's ethics and law and influence upon later developments in law and legal philosophy).

[65] David Kravets, *Lawyers Score Big in Settlement for Ashley Madison Cheating Site Data Breach*, ARC TECHNICAL (July 17, 2017).

[66] Richard B. Freeman, *Who Owns the Robots Rules the World*, HARVARD MAGAZINE (May–June 2016).

[67] *Ready or Not: Artificial Intelligence and Corporate Legal Departments,* THOMPSON-REUTERS (2022).

[68] *Id.*

[69] JULIA T. WOOD, GENDERED LIVES: COMMUNICATION, GENDER & CULTURE (New York, New York: Thomson, Wadsworth, 2005) at 2.

[70] Selena Larson, *Why So Few Women Are Studying Computer Science*, READWRITE (Sept. 2, 2014).

[71] Gaby Galvin, *Middle School Is Key to Girls' Coding Interest*, U.S. NEWS & WORLD REPORT (Oct. 20, 2016).

[72] *Attorney Carney Shegerian Comments on Sexual Harassment and Discrimination Allegations Against UploadVR*, PLUS COMPANY UPDATES(PCU) (June 15, 2017).

[73] Sanika Karandikar, *The Risks of Sexual Harassment in the Metaverse*, PERSONNEL TODAY (July 14, 2022).

[74] Elise Hu, *Sexism in the Tech Industry Takes Center Stage*, NATIONAL PUBLIC RADIO: ALL THINGS CONSIDERED (Sept. 11, 2013).

[75] Jay Hathaway, *What is Gamergate, and Why? An Explainer for Non-Geeks*, GAWKER.COM (Oct. 10, 2014).

[76] Simon Parkin, *Gamergate: A Scandal Erupts in the Video-Game Community*, NEW YORKER (Oct. 17, 2014).

[77] *Id.*

[78] Dan Golding, *The End of Gamers*, DANGOLDING.TUMBLR.COM (Aug. 28, 2014).

[79] *Fast Rise in Social Virtual Reality Stirs Harassment Concerns*, CLEMSON NEWS (Sept. 17, 2021).

[80] Queenie Wong, *Facebook, Now Meta, Struggles to Combat Harassment in Virtual Reality*, CNET NEWS.COM (Dec. 9, 2020).

[81] *What Is Marxism?*, ALL ABOUT PHILOSOPHY.ORG (2022).

[82] HARRY BRAVERMAN, LABOR AND MONOPOLY CAPITAL: THE DEGRADATION OF WORK IN THE TWENTIETH CENTURY (New York, New York, Monthly Review Press, 1974).

[83] Karl Marx & Frederick Engels, *Manifesto of the Communist Party* (New York, New York: Cosimo Classics 2009) (1848) at 49.

[84] *Id.*

[85] *Id.*

[86] PAUL BARAN & PAUL M. SWEEZY, MONOPOLY CAPITAL (New York, New York: Modern Reader Paperbacks, 1966) at 6.

[87] Frederico Ast, *The Marxist Revolution for the Internet Age*, MEDIUM.COM (June 6, 2016).

[88] *Id.*

[89] Robert Hackett, *20 Great Workplaces in Tech*, FORTUNE (Oct. 8, 2014).

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] Eugene Debs, *Profit Sharing,* 16(12) LOCOMOTIVE FIREMEN'S MAGAZINE (Dec. 1892).

[94] *Id.*

[95] Michael Addady, *These 10 Companies Are Generous with Stock Options,* FORTUNE (Mar. 11, 2016).

[96] *Id.*

[97] David De Cremer and Tian Tao, *Huawei: A Case Study of When Profit Sharing Works,* HARV. BUS. REV. (Sept. 24, 2015).

[98] *Id.*

[99] Kerry Dolan and Chase Peterson-Withorn, *Forbes World's Billionaire List*, FORBES (2022), https://www.forbes.com/billionaires/.

[100] Dan Western, *Mark Zuckerberg Net Worth*, WEALTHY GORILLA (Aug. 1, 2022).

[101] Chase Peterson-Withorn, *The 2022 Forbes 400 List Of Richest Americans: Facts And Figures,* FORBES (Sept. 27, 2022).

[102] *Id.*

[103] Amicus Brief of Software Freedom Law Center in *Microsoft Corp. v. AT & T Corp.*, 2005 U.S. Briefs 1056 (Dec. 15, 2005).

[104] STEPHEN WEBER, THE SUCCESS OF SOURCE CODE (Cambridge, Massachusetts: Harvard University Press, 2004) at 1.

[105] *Id.*

[106] Yochai Benkler, *From Consumers to Users: Shifting Deeper Structures of Regulation: Toward Sustainable Commons and User Access*, 52 FEDERAL COMMUNICATIONS LAW JOURNAL 561, 562 (2000).

[107] Linus Torvalds, @Linus__Torvalds, Tweet, 2:05 PM Jan 29, 2013 (Twitter Web Client).

[108] *Social Contract Theory: Ethics Defined,* ETHICS UNWRAPPED, McCombs School of Business, University of Texas Austin.

[109] *Id.*

[110] Chris Willentz, *The Dark Side of Technology*, 53 FINANCE & DEVELOPMENT 1 (INTERNATIONAL MONETARY FUND) (Sept. 2016).

[111] David Kravits, *U.N. Declares Access to the Internet as a Human Right*, Wired (June 3, 2011).

[112] David Rothkopf, *Is Unrestricted Access to the Internet a Modern Human Right?*, FP (Feb. 2, 2015).

[113] *Remarks By President Biden on the Affordable Connectivity Program*, THE WHITE HOUSE (May 9, 2022).

[114] STEVEN N. DURLAUF AND LAWRENCE E. BLUME, THE NEW PALGRAVE DICTIONARY OF ECONOMICS (New York, New York: Palgrave, MacMillan, 2d ed. 2008).

[115] "After Hobbes, John Locke and Jean-Jacques Rousseau are the best known proponents of this enormously influential theory, which has been one of the most dominant theories within moral and political theory throughout the history of the modern West. In the twentieth century, moral and political theory regained philosophical momentum as a result of John Rawls' Kantian version of social contract theory, and was followed by new analyses of the subject by David Gauthier and others." INTERNATIONAL ENCYCLOPEDIA OF PHILOSOPHY, *Social Contract Theory* (1995).

[116] *Id.*

[117] *Id.*

[118] *Id.* at ¶ 6.

[119] ENCYCLOPEDIA BRITANNICA, *Social Contract* (2016).

[120] *Social Contract Theory*, entry in INTERNATIONAL ENCYCLOPEDIA OF PHILOSOPHY (2016).

[121] INTERNET SECURITY ALLIANCE, SOCIAL CONTRACT 2.0: A 21ST CENTURY PROGRAM FOR EFFECTIVE CYBER SECURITY (Sept. 2016).

[122] *Id.* at 4.

[123] INTERNATIONAL ENCYCLOPEDIA OF PHILOSOPHY, *Social Contract Theory* (1995).

[124] JOHN RAWLS, A THEORY OF JUSTICE (Cambridge, Massachusetts: Harvard University Press, 1999).

[125] MICHAEL SANDEL, JUSTICE: WHAT'S THE RIGHT THING TO DO (New York, New York: Farrar, Straus and Giroux, 2009) at 151–152.

[126] *Id.* at § 3.3.

[127] *Id.* at Commentary to § 3.3.

[128] *Id.* at § 3.5.

[129] *Id.* at Commentary to § 3.5.

[130] *Id.*

[131] Awami Politics, *Criticism of the Social Contract Theory* (July 21, 2012).

[132] *Social Contract Theory,* entry in INTERNATIONAL ENCYCLOPEDIA OF PHILOSOPHY (1995).

[133] JASON BRENNAN, LIBERTARIANISM: WHAT EVERYONE NEEDS TO KNOW (New York, New York: Oxford University Press, 2012) at 1.

[134] MILTON FRIEDMAN, CAPITALISM AND FREEDOM (Chicago, Illinois: University of Chicago Press, 1962) at 7–21.

[135] ANDREW S. GROVE, ONLY THE PARANOID SURVIVE: HOW TO EXPLOIT THE CRISIS POINTS THAT CHALLENGE EVERY COMPANY (New York, New York: Crown Business Group, 1999).

[136] "The night-watchman state or minarchy is a model of a state that is limited and minimal, whose only functions are to act as an enforcer of the non-aggression principle by providing citizens with the military, the police and courts, thereby protecting them from aggression, theft, breach of contract, fraud and enforcing property laws." Nightwatchman States, LIBERTARIAN WIKI.

[137] Emily Badger, *The Taxi Industry is Crushing Uber and Lyft on the Lobbying Front, 3,500 to 1,* WASH. POST (July 31, 2014).

[138] Greg Dickinson, *How the World is Going to War with Uber,* THE TELEGRAPH (June 26, 2018).

[139] *Id.*

[140] Pierre-Joseph Proudhon, *No Gods, No Masters: An Anthology of Anarchism* (Chico, California: AK Press, 2005) at 55–56.

[141] *Abraham Jewett, LendingTree Class Action Alleges Data Breach Exposed Data of 200K Customers*, Top Class Actions (July 14, 2022).

[142] Federal Trade Commission, *Federal Trade Commission Returns More Than $9.7 Million To Consumers Harmed by LendingClub's Deceptive Hidden Fees* (Aug. 11, 2022).

[143] CLAY SHIRKY, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS, Penguin Random House (New York: New York; 2008).

[144] Video Interview, *Clay Shirky on Here Comes Everybody*, P2PF Foundation (2019).

[145] CLAY SHIRKY, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS, Penguin Random House (New York: New York; 2008) at 1.

[146] Parmy Olson, *The Man Behind Silk Road—The Internet's Biggest Market for Illegal Drugs*, THE GUARDIAN (Nov. 10, 2013).

[147] David Golumba, *Cyberlibertarians' Digital Deletion of the Left*, JACOBIN MAGAZINE (Dec. 13, 2013).

[148] John Perry Barlow, *A Declaration of Independence of Cyberspace*, Davos Switzerland (1996).

[149] *Id.*

[150] This email message, written by the hacking group Xanatomy, was sent to a Computer Ethics instructor as a response to the Ten Commandments mentioned in Chapter 1.

[151] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 24 (1999).

[152] Monica Buchanan Pitrelli, *Global Hacking Group Anonymous Launches 'Cyber War' Against Russia*, CNBC (Mar. 1, 2022).

[153] *Id.*

[154] JAMES GUNN, THE IMMORTALS (New York, New York: Simon & Schuster; 2005).

[155] *Id.* at Commentary to § 2.3.

[156] Ebun Oke, *Professionalism in Computer Science,* MEDIUM.COM (June 26, 2019).

[157] Robert C. Martin, *The Future of Programming*, https://www.youtube.com/watch?v=ecIWPzGEbFc&feature=youtu.be&t=1h9m49s.

[158] Robert C. Martin, *The Clean Code Blog* (Nov. 18, 2015).

[159] Gábor Zöld, *Software Engineering Ethics Manifesto by Uncle Bob Martin,* CODINGSANS (Mar. 15, 2022).

[160] Bill Chappell, *Toyota Moves To Settle 'Sudden Acceleration' Lawsuits For More Than $1 Billion*, NATIONAL PUBLIC RADIO (Dec. 26, 2012).

[161] *Id.*

[162] *Id.*

[163] James Somers, *The Coming Software Apocalypse*, THE ATLANTIC (Sept. 26, 2017).

[164] *Id.*

[165] Robert C. Martin, *The Clean Code Blog, Id.*

[166] NSPE Code of Ethics for Engineers (revised July 2007).

[167] Professional Engineers Act, R.S.O. 1990, c. P.28.

[168] *Id.*

[169] Professional Engineers Ontario, *Code of Ethics* (2017).

[170] Professional Engineers Ontario, Discipline (2017).

[171] Bill Sourour, *The Code I'm Still Ashamed of*, DevMastery.com (Nov. 13, 2016).

[172] *Id.*

[173] Bill Sourour, *The Trustworthy Coder's Pledge* (Oct. 9, 2017).

[174] *Id.*

[175] MILTON FRIEDMAN & ROSE FRIEDMAN, THE TYRANNY OF THE STATUS QUO, Houghton Mifflin Harcourt (Boston, Mass. 1984).

[176] *ACM Code of Ethics and Professional Conduct*. at § 2.8.

[177] *Id.* at § 2.9.

[178] *Id.* at § 2.7.

[179] *Id.* at § 2.5.

[180] *Id.*

[181] *Hedera Council Issues Public Comment to Commerce Dept.*, TARGETED NEWS SERVICE (US) (July 11, 2022).

[182] *Id.*

[183] Morgan Jones, *To Transfer, Or Not to Transfer, That Is the Question*, MONDAQ (July 11, 2022).

[184] Charles Kettering (1876–1958), Quoted in Robert Andrews, THE CONCISE COLUMBIA DICTIONARY OF QUOTATIONS (Columbia University Press, New York, New York 1989) at 105.

[185] Stephen DeAngelis, *Artificial Intelligence and Moral Dilemmas*, ENTERRO (June 29, 2012).

[186] *Id.*

[187] Miguel Sicart, *Moral Dilemmas in Computer Games*, 29 MIT: DESIGNER ISSUES 28, 32 (2013).

[188] Caitlin Dewey, *The Only Guide to Gamergate You'll Ever Need to Read*, WASH. POST (Oct. 14, 2014).

[189] Peter Waynor, *12 Ethical Dilemmas Gnawing at Developers Today*, INFOWORLD (April 21, 2014).

[190] *Id.*

[191] Gary Marcus, *Moral Machines*, NEW YORKER (Nov. 24, 2012).

[192] *Id.*

[193] Some commentators have urged extending strict products liability principles to software. See e.g., Lori A. Weber, *Bad Bytes: The Application of Strict Products Liability to Computer Software*, 66 ST. JOHN'S L. REV. 469 (1992); see generally, Diane Savage, *Avoiding Tort Claims for Defective Hardware and Software Strategies for Dealing with Potential Liability Woes*, 15 COMPUTER LAW STRATEGIES 1 (1998).

[194] Frances E. Zollers et al., *No More Soft Landings for Software, Liability for Defects in an Industry That Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 746 (2005).

[195] *Nothing Like it Has Ever Existed Before": Tech Companies Make Computer Chips from Human Cells, but is it Ethical?*, CE NOTICIAS FINANCIERAS (June 7, 2022).

[196] *Id.*

[197] *Id.*