

# Computer Ethics & the Law

---

## § 1.0: WHY STUDY COMPUTER ETHICS?

I think it's fair to say that personal computers have become the most empowering tool we've ever created. They're tools of communication, they're tools of creativity, and they can be shaped by their user.

—Bill Gates

### [A] How Computers Impact Our Daily Lives

The word ethics comes from the Greek word *ethos* (character), and the Latin word *mores* (norms or customs). Ethics is a branch of philosophy that studies the nature and development of good character. Computer ethics applies moral reasoning to resolve dilemmas created by a plethora of rapidly evolving information age technologies. As recently as 1994, there were only 150 websites in the entire world. Google did not open its first office until 1998 and Apple launched the iPhone in 2007. Internet hardware such as routers, hubs, servers, cell phone towers, satellites, radios, smartphones and countless other devices have become ubiquitous.

A world without email (first created in 1971), text-messages (1992), Skype (2003), Facebook (2004), YouTube (2005), Twitter (2006), Instagram (2010) and Tinder (2012) is difficult to imagine for today's "digital natives," who grew up after the widespread availability of the Internet. The term "digital immigrant," in contrast, refers to an individual who was not exposed to the World Wide Web until adulthood. Both of this book's authors are digital immigrants, who remember when making a long-distance telephone call was an expensive luxury, which was reserved only for important communications. Both of us began using the Internet in the 1970s, when almost all users were military, governmental or educational researchers.

Advertisers have a marketing category called “digital resisters” for digital immigrants who still fax documents, write physical checks and refuse to use email or social networks. Michael Rustad often chides Tom Koenig for wearing a wristwatch and using landlines for most telephone calls. Michael’s daughter Erica, who is a digital native raised in a media-rich world, criticizes him for rarely sending text messages and never using emojis. Digital natives casually send emails, update their calendars, check the weather forecast, access databases, play games, get traveling directions, make financial transactions and perform countless other everyday tasks online.

When Psion Corporation released the first Personal Digital Assistants (PDAs) in 1984, only a few visionaries could foresee the smartphone applications that would become omnipresent three decades later. The first mobile telephones with Internet connectivity did not arrive until 1999. By 2008, there were more devices connected to the Internet than people on Earth. As of April 2017, Apple’s App Store had 2.2 million products, while Google Play boasted 2.8 million applications.

Technological advances are testing moral and legal boundaries on an unprecedented scale. “Computer systems design and related services” is the most rapidly growing industrial category in the U.S. economy. Private companies in this field increased their sales by 18% in 2016, more than twice the 6.8% growth rate of the average corporation.<sup>1</sup> The software industry increased its direct employment “from 778,000 jobs in 1990 and 1,083,000 jobs in 1995, to 2,095,000 in 2010 and 2,501,000 in 2014.”<sup>2</sup> The average American spends nearly two hours a day on social media websites. Nearly one in five Americans report being online “almost constantly.” Reevaluations of morality, human rights and the proper role of government regulation must evolve to address these technological and cultural developments.

## **[B] Computer Ethics and the Law: Past, Present, Future**

In Roman mythology, Janus, the god of beginnings, had two faces, one looking to the past and one to the future. Law and ethics, too, are Janus-faced because they must evaluate the past with an eye toward future developments. While every computer ethics book describes scores of legal rules, we are the first to follow Mahatma Gandhi’s lead in systematically treating law as a form of “codified ethics.” Law incorporates ethical norms that “are propositions about how values ought to be distributed, including those. . . like power, respect, knowledge, safety, health, comfort and convenience.”<sup>3</sup>

Ethical disputes are often fought out in the court system. Gender discrimination in Silicon Valley's top companies, for example, is an endemic problem that requires a strong ethical culture to root out workplace inequities. In August 2017, James Damore was fired for posting a ten-page memo critical of what he labeled "Google's Ideological Echo Chamber."<sup>4</sup> In his internal posting, he charged that Google was "pressing individual managers to increase diversity" by hiring women and minorities even if they were less qualified.<sup>5</sup> Google fired Damore on the grounds that his "memo promoted harmful gender stereotypes and violated its code of conduct."<sup>6</sup>

Google, like many other information technology leaders, strongly values a diverse work force. In an employment-at-will workplace, Google has a legal right to terminate an employee who violates its code of corporate conduct. Damore is reportedly considering suing for wrongful dismissal, perhaps alleging a violation of Section 7 of the National Labor Relations Act that bars employers from interfering with "concerted activities" to improve the workplace. Damore would face an uphill battle because federal labor law requires a showing that this protected form of expression relates to labor union organizing or similar activities.

## **[C] Law Lags Behind Technological Advances**

### ***(1) What Is Legal Lag?***

"Legal lag" occurs when legal institutions fail to keep up with changing societal conditions. A rapid change in one social institution requires readjustments in the other parts of the culture. Justice Benjamin Cardozo argued that law must continually evolve to deal with emergent social realities: "The inn that provides shelter for the night is not the journey's end. The law, like the traveler, must be ready for the morrow. It must have a principle of growth."<sup>7</sup>

New technologies often take many years to reshape other social institutions. The development of reliable electrical power in the 1870s, for example, did not immediately displace steam power. The steam-driven factory was organized around a central drive shaft, while electricity worked best in a less centralized factory setting. Reorganizing the workplace around the assembly line versus the drive shaft required decades of adjustment.<sup>8</sup> Recent advances in artificial intelligence will require similar social, ethical and legal reconfiguration over the next decades.

Today, technology is on an exponential expansion curve that is impacting everything—everywhere. Changes of a scale that once took centuries now happen in a few years. Not long ago, Facebook was a dorm-room dating site, mobile

phones were for the ultra-rich, drones were multimillion-dollar war machines and supercomputers were largely employed for secret government research. Today, hobbyists can build drones and poor villagers in India access Facebook accounts on smartphones that have more computing power than the Cray 2 supercomputer, which in 1985 cost \$17.5 million and weighed 2,500 kilograms.

A full human genome sequencing, which cost \$100 million in 2002, today can be completed for \$1,000 and will likely cost less than a cup of coffee by 2020.<sup>9</sup> Will insurance companies be permitted to modify coverage for those whose genetic profiles predict a potential need for expensive medical treatments? Will limitations be imposed on the rights of parents to abort fetuses with genetic features that they consider undesirable? Ethical and legal codes often remain unsettled for decades after new social problems emerge.

### ***(2) Legal Lag in Response to Technological Changes***

President John F. Kennedy stated: “Change is the law of life. And those who look only to the past or present are certain to miss the future.” The rise of the automobile affected nearly every branch of the law in the first half of the twentieth century. The current penalty for jaywalking in Boston is only a \$1 fine, a holdover from a period when pedestrians resisted giving priority to the “pleasure vehicles” of the wealthy over people on foot or traveling by horse-drawn wagon. Widespread middle-class ownership of cars, combined with an automobile industry-funded public relations campaign against jaywalking, changed public attitudes in most of the U.S. by the 1940s.

By 1930, Henry Ford had sold three million Ford Model A Coupes, fulfilling his goal of making cars so affordable that any “any man with a job could own his own automobile.” By the 1950s, cars had become important symbols of widespread prosperity, rather than being viewed as toys for the arrogant rich. Futurologists predict the demise of the personal automobile over the next quarter century, with robot vehicles being conveniently dispatched from a central location whenever needed. This “distributed public transportation system” will require dramatically different laws than those that currently govern traffic.

Eighty-one years ago, in 1936, a Duke University student published a law review article predicting the future path of automobile liability law.<sup>10</sup> He observed that, in 1905, all American automobile case law could be contained within a four-page law review article. Only three decades later, explaining the complexities of automobile law would require an entire encyclopedia. That law student was Richard M. Nixon, who would later become President of the United States. Nixon’s conclusion was that the courts of his day were mechanically extending

“horse and buggy law” to this new mode of transportation. However, the most creative judges developed entirely new rules that were specifically designed to address the growing use of the automobile.

### (a) Products Liability for the Age of the Internet

Prior to the mid-1960s, the doctrine of privity shielded manufacturers and others in the line of distribution from legal responsibility for deaths and injuries caused by defective products. Under privity, only a direct purchaser of a product from a manufacturer could file suit for injuries caused by defective products. Consumers injured by defective cars had no recourse against car makers because they were not in direct contractual privity with the company but were only in privity with the local automobile dealer.

Pedestrians and other injured bystanders had no privity either and no cause of legal action against the car maker if injured by a dangerously defective vehicle. This contract-based defense may have made some sense in an earlier America in which sellers were largely local and dealt directly with their customers. However, privity left those injured by defective automobiles without recourse as giant companies increasingly distributed their products through dealerships.

Numerous automobile safety improvements were available, but not instituted, until the law mandated them. “While a headrest design was patented in 1923, the National Highway Transportation Association only enacted a regulation that all passenger cars should have headrests in 1969—after hundreds of thousands of spine injuries as the result of whiplash.”<sup>11</sup> Ralph Nader’s 1965 best-selling book, *Unsafe at Any Speed: The Designed-In Dangers of the American Automobile*, charged U.S. car manufacturers with resisting the introduction of safety features such as seat belts, anti-roll bars, safety glass and the elimination of sharp edges and knobs on dashboards.

Without legal responsibility for the epidemic of deaths that resulted from needlessly hazardous vehicles, automobile manufactures had little incentive to improve the safety of their vehicles. Advertisements stressed the fun and social admiration that came with owning the latest model of luxury automobile, not the possibility of flaming death from an insecure fuel system or of being impaled by a rigid steering wheel column after a collision.

Privity finally collapsed in a 1960 in a New Jersey Supreme Court case when a court refused to recognize this doctrine, as it was out of step with the modern marketing of automobiles.<sup>12</sup> The decision in *Henningsen v. Bloomfield Motors, Inc.*,<sup>13</sup> altered legal thinking, leading courts and legislatures around the country to

overturn privity of contract in products liability litigation. In *Henningsen*, Chrysler sold an automobile to a dealer, Bloomfield Motors. The dealer then resold the car to Claus Henningsen. Henningsen's wife was injured when the car's steering gear malfunctioned only ten days after delivery.

Helen Henningsen was driving at 20–22 miles per hour on a smooth two-lane highway. She heard a loud noise, the steering wheel spun in her hands and the vehicle suddenly veered, crashing into a wall. Helen Henningsen filed suit to recover for her injuries and the loss of her new automobile. Helen had no direct contractual relationship (no privity) with the dealer because Claus had bought the car for his wife as a Mother's Day present. Neither Claus nor Helen was in privity with the Chrysler Corporation because the vehicle had been purchased from a New Jersey dealership.

New Jersey's highest court ruled that consumers could recover for damages caused by defective parts despite the lack of privity and the manufacturer's disclaimers. Justice John Francis, writing for the majority of the New Jersey Supreme Court, held the manufacturer liable despite the lack of privity. The court reasoned that privity was a legal anachronism, given the reality that car makers use local dealers to sell their vehicles nationally:

Under modern marketing conditions, when a manufacturer puts a new automobile in the stream of trade and promotes its purchase by the public, an implied warranty that it is reasonably suitable for use as such accompanies it into the hands of the ultimate purchaser. Absence of agency between the manufacturer and the dealer who makes the ultimate sale is immaterial.<sup>14</sup>

Most other state courts soon adopted the New Jersey Supreme Court's reasoning, allowing a consumer to file a products liability action despite the absence of privity. A growing number of courts also refused to enforce the manufacturer's warranty disclaimers. Automobile manufacturers and dealers could no longer limit the customer's remedy to only the replacement of the defective parts by writing this restriction into the car's purchase and sale agreement.

These new legal principles shifted the cost of accidents created by defective design from consumers onto manufacturers, who were in the best position to redesign the cars and fortify warnings of known defects. Today, a product seller is "subject to liability to the user or consumer even though he has exercised all possible care in the preparation and sale of the product."<sup>15</sup> Today, courts are beginning to extend this principle to software companies, who have a history of routinely disclaiming any liability to users.

### (b) Legal Lag & Information Technologies

Internet technologies are evolving far faster than industry groups, legislatures and international standards organizations can formulate new laws and regulations. The legal system law limps behind technological developments, inevitably failing to catch up to advances in the digital world. Neither criminal nor tort law, for example, has yet developed appropriate remedies to punish and deter gender-linked injuries such as online stalking, harassment and humiliation.

Google's Larry Page expressed the frustration felt by many computer professionals about the need for a living law that adapts more fluidly to cyberspace developments: "The law can't be right if it's 50 years old. Like, it's before the Internet." The U.S. Court of Appeals for the Second Circuit compared revising laws to keep up with rapidly changing technologies as being "somewhat like trying to board a moving bus."<sup>16</sup>

U.S. jurisdictions often have different community standards for what content is considered obscene, defamatory or is otherwise illegal content. In *United States v. Thomas*,<sup>17</sup> a married couple was charged and convicted of violating federal obscenity statutes. The couple's California-based online bulletin board uploaded erotic pictorial images. A postal inspector obtained a password from the couple and transmitted allegedly obscene material to his computer in Tennessee. The couple also sent allegedly obscene videotapes to the Tennessee-based inspector.

The U.S. Court of Appeals for the Sixth Circuit affirmed the Thomas's conviction in a Tennessee district court. The court reasoned that the defendants had knowingly sent their material into Tennessee by accepting a subscription from a resident of that state and it was therefore appropriate to apply the community obscenity standard of Tennessee.

The erotic images would be protectable under the First Amendment in California, where they had been uploaded, but the same images were deemed obscene in Tennessee, where the images were downloaded because of that state's more conservative community standards. This was the first case to apply the community standard definition of obscenity to an Internet transmission. The U.S. Supreme Court in *Miller v. California* acknowledged that: "It is neither realistic nor constitutionally sound to read the First Amendment as requiring the people of Maine or Mississippi to accept public depiction of conduct found tolerable in Las Vegas or New York City."<sup>18</sup>

Chart One (below) provides examples of the potential legal consequences of actual moral dilemmas faced by our students over the past two years. Without

knowledge of the applicable laws, it is easy to become entrapped in a costly and potentially career-destroying legal quagmire.

**CHART ONE: LEGAL ISSUES RAISED BY  
COMMON ETHICAL DILEMMAS**

<i>Ethical Issues Facing Computer Professionals</i>	<i>Legal Issues Raised</i>
You have been asked to install software that monitors the keystrokes of a client's employees.	What privacy rights do the employees have? If the employees are working in a European subsidiary, do you owe them a duty of notice that they are being monitored?
You are working as a computer consultant for an educational institution and asked to install software that secretly monitors peer-to-peer sharing of music and software.	Will the software take into account the students' fair use rights under copyright law? Are the students entitled to receive notice that their downloaded content is being monitored? What duty does the computer professional have to notify law enforcement if students download illegal content?
You have been asked to develop software for a hospital that is a "covered entity" under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If the cost of implementing security is great, how much security is enough to protect patients' privacy?	The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and it applies to health plans, health care clearinghouses and those health care providers that conduct certain health care transactions electronically.
What privacy information must be protected and at what cost if your client is subject to the HIPAA's Security Rule? What steps must a programmer take to protect medical records?	The HIPAA Privacy Rule protects most "individually identifiable health information" held or transmitted by a covered entity or its business associates, in any form or medium, whether electronic, on paper or oral. The Privacy Rule calls this information protected health information.

<p>What security safeguards must be implemented at what cost to protect medical records? Does it matter whether the health care provider is a “covered entity” under HIPAA? Are all patients entitled to reasonable computer security or only those covered by HIPAA?</p>	<p>HIPAA’s Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical and physical safeguards for protecting patient information.</p>
<p>You are a computer professional served with a legal summons requiring you to turn over the personally identifiable records of your service provider client.</p>	<p>There is a definite legal requirement to respond to and comply with a court order, even though this may conflict with the privacy rights of the client’s customers.</p>

## § 1.1: ETHICAL ROOTS OF COMPUTER LAW

### [A] Rapidly Evolving Technologies Raise Moral Issues

Critics warn that the increasing economic and cultural power of the Internet’s largest corporations may alter the political system in unpredictable ways.<sup>19</sup> Skillful tweeting, banner fundraising advertisements, manipulative emails, online opinion polling, strategic leaking and other newly enhanced online political techniques will play increasingly central roles in election campaigns. President Trump continues to use Twitter to communicate directly with his constituents, redefining the relationship between government and the electorate. Trump’s leading critics, such as Senator Elizabeth Warren and entrepreneur Mark Cuban, are increasingly employing social media postings to counter the President’s tweets.

The ISIS terrorist organization rose from obscurity by broadcasting violent recruitment propaganda on social media. As a presidential candidate, Donald Trump proposed restricting the Internet access of such groups, stating; “We have to talk to [cyberspace experts] about, maybe in certain areas, closing that Internet up in some way . . . Somebody will say, ‘Oh, freedom of speech, freedom of speech.’ These are foolish people.” Critics fear that such proposals will lead to censorship of all oppositional groups, noting that the Internet plays a key role in organizing grassroots social movements such as the Native American opposition to the Keystone oil pipeline. The activist group, *Grab Your Wallet*, is employing the Internet to organize consumer boycotts against retailers that carry Ivanka Trump branded clothing.

Calls for greater computer security have increased since intelligence services confirmed that Russian hackers undermined Senator Hillary Clinton's candidacy and the integrity of the American political system in the 2016 U.S. Presidential election. Facebook has disclosed that more than "\$100,000 worth of divisive ads were purchased by a Russian company linked to Prime Minister Putin's government."<sup>20</sup> In September 2017, Facebook admitted that it hosted a Russian influence operation that micro-targeted millions of users with hate speech messages.<sup>21</sup>

Texas separatists and other U.S. activist groups were manipulated to create an "AstroTurf" social movement that encouraged demonstrations against Senator Clinton. The AstroTurf designation refers to political efforts that have the appearance of being spontaneous expressions of popular outrage, but in fact are composed of hoaxes and half-truths that are orchestrated by public relations experts. In August 2017, Facebook moved to discourage disinformation campaigns by banning websites that repeatedly shared stories marked as false from advertising on its platform.<sup>22</sup>

The vastness of the Internet makes it difficult to enforce rules against illegal postings. The peer-to-peer file sharing movement on the Internet, for example, pits the movie, record and film industries against copyright infringing Internet users. Visitors upload 300 hours of content per minute. YouTube has one billion users who account for four billion views each day. It would take 600 persons watching YouTube 24/7 just to classify the content as infringing or not. In May 2017, Facebook announced that would increase the number of employees charged with reviewing bad behavior such as crimes and suicides shown in its postings from 4,500 to 7,000 individuals.

## **[B] Resolving Ethical Disputes Through Law**

### ***(1) The Ethics & Law of Ticket Bots***

Michael Rustad remembers standing in line for six hours in 1974 so he could attend a nationally televised basketball game between two ACC powerhouses, the Maryland Terrapins and the North Carolina Tar Heels. The only way to get a student ticket was to personally buy one at the Cole Field House ticket office in College Park, Maryland. Today, a student can make a last-minute decision to purchase a ticket from a resale website without the buyer needing to interact with potentially dishonest street scalpers. Nevertheless, the virtue of the older method of ticket distribution is that those who stood in line when the office opened could buy a face value ticket.

Today's college students, in contrast, often have no recourse but to pay inflated prices for a popular concert or sporting event on a resale website, which often has acquired a huge block of tickets electronically. The New York Attorney General (New York AG) reports receiving numerous complaints from consumers citing "price gouging," "scalping," "outrageous fees" and "immediate sell-outs." As one citizen wrote in a typical complaint: "The average fan has no chance to buy tickets at face value . . . this is a disgrace."<sup>23</sup> The New York AG describes online ticketing as a "fixed" game:

Consider, for example, that on December 8, 2014, when tickets first went on sale for a tour by the rock band U2, a single broker purchased 1,012 tickets to one show at Madison Square Garden in a single minute, despite the ticket vendor's claim of a "4 ticket limit." By the end of that day, the same broker and one other had together amassed more than 15,000 tickets to U2's shows across North America. Consider that brokers sometimes resell tickets at margins that are over 1,000% of face value.<sup>24</sup>

Companies producing ticket bot software boast that they can easily circumvent the security of event websites by masquerading as human buyers. Is it ethical to use bots to gain an unfair advantage by preventing the public from purchasing tickets at a fair market value? Until recently, there was no state or federal regulation prohibiting ticket-buying bots.

The ticket bot problem is an example of how emergent moral predicaments are often resolved through legislation, regulations or legal decisions. In late 2016, Congress enacted a statute declaring that the use of ticket bots is an unfair or deceptive trade practice in violation of the Federal Trade Commission Act. The use of anti-circumvention ticket bots arguably violates several states' unfair and deceptive trade practices statutes. As new forms of wrongdoing emerge, judges must determine how far existing laws can stretch to cover cyberspace disputes.

## ***(2) Updating the Law for Price Bots***

In the fall of 2017, several U.S. airlines raised prices dramatically for flights leaving cities in the path of Hurricane Irma. This price gouging was not a human management decision. Bots automatically increased prices in response to Internet searches for and purchases of these airline tickets. Observers fear that as Internet giants come to dominate commercial transactions, price-monitoring bots will be able to conspire against consumers through algorithmic pricing that allow suppliers to coordinate cost increases. "A cabal of AI-enhanced price-bots might

plausibly hatch a method of colluding that even their handlers could not understand, let alone be held full responsible for.”<sup>25</sup>

It is unclear under what circumstances AI programmers or their employers can be held legally responsible for the unanticipated misdeeds of a defectively programmed rogue bot. Legislation against this new form of price fixing will be difficult to design because:

the more consumers are pushed to deal directly with price-bots (to thwart the transparency that allows rival sellers to collude), the more the algorithms learn about the characteristics of individual customers. That opens the door to prices tailored to each customer’s willingness to pay, a profitable strategy for sellers.<sup>26</sup>

Overregulation of technology’s cutting-edge products and services is a danger if lawmakers move too quickly to remedy perceived digital wrongs.

### ***(3) Classifying Workers as Independent Contractors***

Ethical questions regarding the just distribution of societal burdens and benefits arise from the widespread introduction of digital products. For example, Intuit.com, a software corporation, estimates that 40% of all American workers will be classified as independent contractors by the year 2020. Uber drivers are challenging their classification as independent contractors in the U.S. courts.

They argue for the right to enjoy employee benefits such as unemployment insurance, workers’ compensation and to organize labor unions. In 2016, Uber settled two class action lawsuits filed by its drivers, agreeing to pay \$84 million and allow their drivers to organize to remedy grievances, receive tips from passengers and appeal deactivations by Uber.

### ***(4) Algorithmic Bias***

Algorithms may make sexist or racist decisions that reflect the non-conscious assumptions of their programmers. The software used by property owners to screen out potentially troublesome tenants has the appearance of objectivity, but the underlying algorithms discriminate against immigrants. The algorithm will unjustly reject people who cannot document a stable work history in the United States. The website Algorithmic Justice’s mission is to “identify and discuss ethical challenges of algorithms, big data and artificial intelligence, but also to suggest solutions how algorithms can be harnessed for ethical purposes.”

Uber's subjective passenger and driver-rating system is said to discriminate against socially disfavored groups because minority drivers tend to receive unfairly lower scores from white passengers. Cornell University researchers argue that:

We know that people tend to have implicit biases that affect how they evaluate people from different groups. It would be illegal for an employer to discriminate directly, but this creates the possibility for backdoor bias creeping in from customers. These new technologies challenge the traditional way law prevents discrimination in the workplace.<sup>27</sup>

AI programs stand accused of depicting women disproportionately in ads for lower paying jobs and tracking African-Americans into cheaper neighborhoods.<sup>28</sup> Algorithmic beauty contest judges overwhelmingly find white contestants to be the most attractive, which is a systematic bias against other races.

A crime prediction algorithm might focus surveillance on minority neighborhoods in response to official statistics showing that these areas have the highest recorded crime rates. These statistics, however, may be the result of an unwritten law enforcement policy of aggressively arresting minority youth from "bad neighborhoods" while releasing teens from "better" families into the custody of their parents. When the AI's efforts result in the arrest of a disproportionate number of residents of these areas, the program might interpret the apparent increase in criminal activity as a need to further increase its targeting of minority youth.

Racist software in the criminal justice system is not a mere hypothetical. A 2016 study of the accuracy of software that predicts the likelihood that a criminal defendant will reoffend concluded that "[w]hite defendants who re-offended within the next two years were mistakenly labeled low risk almost twice as often as black re-offenders (48 percent vs. 28 percent)."<sup>29</sup>

### ***(5) Balancing Security Versus Privacy Concerns***

The most perplexing dilemmas arise when policymakers must choose between conflicting ethical principles. In early 2016, the FBI sought a court order to compel Apple to write software that would decrypt the messages contained on an iPhone used in a San Bernardino, California terrorist attack. Apple opposed this order, contending that if the company developed software to unlock the iPhone, the technology inevitably would lead to mass surveillance, especially of their customers living under despotic regimes. Apple argued that unconditional user trust is essential for the continuing vitality of information technology companies.

The dispute became moot when the FBI announced that an unidentified third party had developed a method to defeat the iPhone's encryption. In a parallel 2016 case, Amazon refused to provide Arkansas murder investigators with audio recordings gathered by its Echo smart speaker system.<sup>30</sup> Such fundamental ethical conflicts between technology corporations and law enforcement agencies appear destined to be decided by the U.S. Supreme Court.

## § 1.2: TECHNOLOGY, ETHICS, AND LAW

### [A] How New Technologies Disrupt the Law

Throughout American history, new information technologies have remade social institutions. The fabled Pony Express of the American West was displaced by the telegraph after less than two years of operation when Western Union completed its transcontinental telegraph system in October 1861.<sup>31</sup> The telegraph, in turn, was replaced by the telephone as the leading mechanism for long-distance communication. Operator-assisted telephone calls gave way to direct dialing. Today, smart phones are rapidly replacing the classic landline, which had required the installation and maintenance of an extensive string of telephone poles and wires.

Netflix's streaming service has driven Blockbuster almost out of business. Of the 9,000 Blockbuster stores in the 1990s, less than ten are still in operation. Netflix's future, in turn, is now being threatened by the proposal of the head of the Federal Communications Commission (FCC), Ajit Pai, to weaken net neutrality. Under the principle of net neutrality, the Obama administration treated Internet Service Providers as similar to public utility providers, which prevented ISPs from favoring one content provider over another. Pai, in contrast, takes a libertarian position, that government intervention to protect online equality should give way to market-driven decisions by private entities. Netflix fears that its entertainment services could be slowed to give priority to rivals that are owned or collaborate with the major ISPs.

Those who resist new information technologies often lose out to those who first learn to exploit new methods of communication. In the sixteenth century Protestant Reformation, Martin Luther played a key role in transforming Europe's ethical and legal order. Luther was the equivalent of a blogger in his day, authoring frequent essays about the need to radically reform Christianity.

Luther's sacrilegious broadsides could be printed relatively quickly and inexpensively thanks to advances in the development of the movable type printing press.<sup>32</sup> The Roman Catholic Church was slow to marshal the power of these

improvements in information technology and therefore was unable to crush Martin Luther's Protestant movement before it gained a rock-solid foothold in Northern Europe.

As Martin Luther's reputation grew, he began to make money from the sales of his writings. However, his profits were limited because Luther was unable to prevent unauthorized copying. Unscrupulous printers reproduced Luther's texts with impunity, sometimes stealing his original manuscripts to make their illicit editions. Copyright law had not evolved to the point where Luther's rights could be vindicated. The British Statute of Anne, 1710, "An Act for the Encouragement of Learning, by vesting the Copies of Printed Books in the Authors or purchasers of such Copies, during the Times therein mentioned," was the first copyright statute.

In the preface of one edition of his German translation of the New Testament, a frustrated Martin Luther wrote: "I beg all my friends and foes, my masters, printers and readers, let this New Testament be mine. If you lack one, then make one for yourselves. . . . But this Testament is Luther's German Testament."<sup>33</sup>

"Technological determinism" overstates the role of technical innovations as the driver of social change. It is far too simplistic to attribute the Protestant Reformation solely to the technological advances in movable type printing. Without the support of local Saxon princes, Luther's writings would have been easily suppressed. His polemics would not have been influential without a critical mass of literate Christians, who were already receptive to his message. Germany already had a long tradition of opposition against the Catholic Church's oppressive hierarchy, which predisposed the populace to support Luther's attacks.<sup>34</sup>

## **[B] Unauthorized Copying in the Information Age**

The ethics of downloading copyrighted material without paying royalties to the author remains a hotly contested issue. Is unlawful downloading of content equivalent to stealing physical objects? While the original work is expensive to produce, additional copies can be created at almost no cost, making the theft of intellectual property feel morally different from traditional types of misappropriation that deprive the original possessor of physical property.

Martin Luther's attempt to shame printers who copied his religious writings without permission parallels contemporary attempts to shame unauthorized downloaders from pirating music, films and software. Paul Stanley, the rhythm

guitarist and singer of the rock band *Kiss*, argues, “Illegal music downloading is ‘morally’ and ‘ethically wrong,’ and laments the fact that new artists “don’t have a chance in hell” of “ever getting that pot of gold.”<sup>35</sup> Bono, the lead singer of *U2* rebuts the idea that illegal downloading only harms greedy capitalists:

A decade’s worth of music file-sharing and swiping has made clear that the people it hurts are the creators—in this case, the young, fledgling songwriters who can’t live off ticket and T-shirt sales like the least sympathetic among us.<sup>36</sup>

The Australian film industry uses shame in its advertising campaign to deter illegally copying of the country’s movies: “You wouldn’t steal a car, you wouldn’t steal a handbag, you wouldn’t steal a television and you wouldn’t steal a movie. Downloading pirated films is stealing.” The public relations campaign to label unauthorized downloading as immoral “piracy” has failed to gain widespread credibility because:

Copyright infringement is illegal, and like many things that are illegal (jaywalking, driving a car with an expired license), it doesn’t have anything in common with stealing except for the (not unimportant!) fact that it’s illegal. Piracy, by contrast, is a special form of stealing committed on the high seas. It involves rolling up to a boat, and taking stuff away from the occupants of the boat. Normally one accomplishes this by threatening to kill the occupants of the boat, and from time to time people actually get killed. By contrast, nobody has ever been killed downloading an authorized copy of a Katy Perry song or sharing the license key of a copy of PowerPoint with a colleague. Sensible people understand this, which is one reason that the content industry’s efforts to get copyright infringers treated like dangerous violent criminals have fallen into increasing discredit.<sup>37</sup>

### **[C] The Policy Debate over Unauthorized Copying**

Copyright has always been contested ethical and legal terrain in American society. In the 1780s, the famous textbook and dictionary creator, Noah Webster, campaigned for strong U.S. copyright laws to stop wholesale distribution of unauthorized reproductions of his dictionary. His efforts, along with those of other stakeholders, were rewarded with a clause in the U. S. Constitution that recognized copyright protection.

Two important American ethical principles appear to conflict in copyright law. The First Amendment’s right to free expression in the form of reprinting,

modifying and parodying existing works, clashes with the right of the original artists to be fully compensated for their creative efforts. Opponents of overly expansive copyright laws argue that corporate owners of intellectual property are attempting to extort excessive profits by privatizing everyone's common heritage. Music industry spokespeople counter that strong copyright protection and free expression have been mutually supportive throughout U.S. history:

In a two-year span, this nation adopted two major, interlacing principles: Americans were free to write whatever they wanted and had every right to be compensated for their work. The First Amendment encouraged creativity, and the copyright clause guaranteed compensation. So often, the debate over illegal downloading focuses on technology. Those who defend the unauthorized sharing of music say that critics are living in the past and had better get used to the new reality. But that new reality is taking a toll. Over the past decade, America has lost a staggering number of professional songwriters and composers; primarily due to the impact of illegal music downloading. . . Those that remain in the profession are struggling to earn even a minimal income.”<sup>38</sup>

Congress has responded to extensive lobbying by pro-copyright interests by ramping up criminal penalties for intellectual property infringement. President Bill Clinton signed the *No Electronic Theft Act of 1997* (NET), which fortified criminal penalties for Internet-related theft. NET amended the U.S. Copyright Act to include online piracy that caused commercial harm, even where there was no proof that the defendant was attempting to make a profit. The media industry continues to press for harsher penalties to deter illegal downloaders.

When the authors of this book ask our students if they illegally download copyrighted music, the great majority admit that they have done so. When asked if they feel guilty for engaging in this infringing activity, only a few indicated that they perceive their downloading as unethical. Moral codes often evolve over time. In the future, this act may be widely viewed as immoral “piracy,” or perhaps efforts to punish downloaders will be castigated as an example of illegitimate and futile government overreach.

Changes in online music distribution technology and corporate practices raise new ethical and legal concerns for musicians who are attempting to gain increased recognition. Spotify, with thirty million subscribers, and Apple Music, which has signed up fifteen million subscribers since launching in 2015, are said to be using their immense economic leverage to pressure lesser-known artists through the threat of giving a lower profile to their musical creations:

Spotify has been retaliating against musicians who introduce new material exclusively on rival Apple Music by making their songs harder to find, according to people familiar with the strategy. Artists who have given Apple exclusive access to new music have been told they will not be able to get their tracks on featured playlists once the songs become available on Spotify, said the people, who declined to be identified discussing the steps. Those artists have also found their songs buried in the search rankings of Spotify, the world's largest music-streaming service, the people said. Spotify said it doesn't alter search rankings.<sup>39</sup>

Such practices are likely to be challenged by attorneys as an updated version of the monopoly power used by anti-competitive business "trusts" during the period of America's robber barons.

### § 1.3: PERSONAL VS. FORMAL ETHICS

#### [A] Personal and Informal Ethical Codes

The social disruption created by rapid advances in computer technology requires software decision-makers to consider the societal impact of their inventions. Programmers are being challenged to take "responsibility for the outcomes, externalities and downright damaging impacts of our hyper-consumer, ever-changing landscape of new gadgets and virtual arenas that are coming on board at a lighting-speed pace."<sup>40</sup> To quote Spider-Man's Uncle Ben: "With great power, comes great responsibility."

Ethical computing guidelines draw from three sources: "(1) the individual's own personal code, (2) any informal code of ethical behavior that exists in the workplace and (3) exposure to formal codes of ethics."<sup>41</sup> For example, individuals may have very different beliefs about the moral justification involved in an online purchase of recreational marijuana. A drug user who is illegally diverting his legally purchased Colorado supply to make a fast profit in jurisdictions where the possession of marijuana is still criminalized, may be viewed as unethical or alternatively, as advancing liberty. The willingness to limit Internet freedoms in order to enforce laws against this illegal reselling will vary sharply in America's pluralistic society.

Similarly, informal rules of online behavior in the workplace or within other small groups will differ significantly according to local conditions. One office will encourage forwarding jokes as a method of keeping morale high, while, in another work setting, this behavior may result in termination, especially if the jokes are risqué. The macho "bro" culture of some Silicon Valley firms such as Uber has

been widely criticized as unethically sexist but praised by a few as encouraging the aggressively competitive ethos necessary in an economic environment where, in the famous aphorism of Intel CEO Andy Grove, “only the paranoid survive.”

Formal rules about the use of computers in the classroom vary between outright bans on the use of the Internet to incorporating cyberspace into in-class learning. Some professors encourage students to consult the Internet to look up applicable statutes or a relevant news story, while others view online surfing during class as undermining the educational experience. A lecture on the importance of having a nuanced Internet-deployed advertising campaign can be enhanced as students find examples for themselves and share their discoveries with the class. On the other hand, holding the attention of students is more challenging in classrooms because of the mesmerizing appeal of instant messaging, social networks and other Internet-related distractions.

## [B] Formal Codes of Computer Ethics

### Preamble to Association of Computer Machinery Code of Ethics

- (1) *Public*—Software engineers shall act consistently with the public interest.
- (2) *Client and Employer*—Software engineers shall act in a manner that is in the best interests of their clients and employers consistent with the public interest.
- (3) *Product*—Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
- (4) *Judgment*—Software engineers shall maintain integrity and independence in their professional judgment.
- (5) *Management*—Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
- (6) *Profession*—Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
- (7) *Colleagues*—Software engineers shall be fair to and supportive of their colleagues.
- (8) *Self*—Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.

### *(1) The ACM's Code of Ethics*

Formal codes of ethics play an important role in the socialization of professionals. The world's largest educational and scientific society devoted to computing, the Association for Computing Machinery (ACM), has developed a code of ethics to guide computer professionals away from immoral practices. The ACM notes that these principles also can serve as a basis for judging the merits of any formal complaint about violations of professional ethical standards.

The organization's Code of Ethics (ACM Code) consists of twenty-four broad rules that define the personal responsibilities of computer professionals. This code is not legally enforceable since membership in the association is voluntary and the ACM cannot prohibit violators from continuing their work in the information technology field. As this book goes to press, the ACM Committee on Professional Ethics (COPE) is revising the ACM Code of Ethics and Professional Conduct to reflect the shifts in technology and society since the Code's creation in 1992. The ACM ethics committee requests that computer professionals respond to four guiding questions:

What parts of The Code no longer make sense due to changes in technology or society? What could be done to make them better fit the current context? Are there any blind spots in The Code? Are there principles that ought to be contained in The Code that are currently missing? In the area of technology where you are most expert, what have been the greatest changes since 1992, and how might The Code be updated to reflect these changes? What parts of The Code are confusing, ambiguous or likely to be misinterpreted?<sup>42</sup>

Rule 2.3 of the Association of Computer Machinery Code of Ethics calls for ACM members to "know and respect existing laws pertaining to professional work." However, ACM members, the Code explains, should not blindly obey unjust laws because "compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged." For example, Edward Snowden argues that his exposure of the National Security Agency's (NSA) mass monitoring of online communications and its subsequent misleading of Congressional committees about its systematic privacy invasions, created a situation where his personal ethical code and his moral obligations to the American people were more important than obeying U.S. law.

Libertarians, who believe in battling government overreach, have supported Snowden. However, backing from the libertarians will not save Snowden from severe punishment if he returns to any nation that recognizes U.S. legal

jurisdiction. The ACM has no power to protect computer professionals from suffering the consequences of breaking the law, even if its membership were to agree that Snowden did the right thing. Chapter Two will address the intersection between ethical perspectives and legal responsibilities.

Section 1.2 of the ACM Ethics Code requires computer professionals to avoid doing harm to others, which is an ethical admonition that applies to diverse legal duties. Chapter Three on Cybertorts, Chapter Four on Cybercrime and Chapter Five on Information Privacy all discuss the legal standards that enforce this ethical dictate. ACM's Code notes that:

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others.

Chapter Five examines information privacy issues from a globalized perspective. Section 1.7 of the Code requires respect for the privacy of others. Failure to protect data privacy may lead to legal liability:

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus, there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals.

ACM ethical rules implicitly require computer professionals to understand and comply with not only the letter of the law, but also with its spirit. Section 2.6 of the ACM Ethics Code requires computer experts to "honor contracts, agreements and assigned responsibilities." Examining the law and ethics of electronic contracts allows one the exploration of such issues as when online contracts are so deceptively presented that courts may refuse to enforce them. If software publishers use licensing to disclaim all responsibility for remedies in the event that their software fails, is it ethical, even if it is legal? Chapter Six discusses the difficult ethical issues raised by contract law in inequitable information technology contracts.

Chapters Seven and Eight of this book will apply ethical and principles to copyrights, patents, trademarks and trade secrets. As Section 1.5 of the ACM notes:

Violation of copyrights, patents, trade secrets and the terms of license agreements are prohibited by law in most circumstances. Even when

software is not so protected, such violations are contrary to professional behavior. Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

ACM Ethics Code Section 1.8 requires computer professionals to “honor confidentiality.” Reviewing how different countries have adopted varying approaches to the trade-offs between protecting personal privacy and other social values such as security and intellectual property rights will reveal the complexity of this issue. Once again, there has been significant litigation over when confidentiality legally applies and when it can be broken.

## ***(2) Computer Professionals for Social Responsibility***

Computer Professionals for Social Responsibility (CPSR), an organization founded to further ethical behavior in computing, existed from 1983 until it was disbanded in 2013. Like the ACM, the CPSR realized that computers are instrumentalities for accomplishing good, but they can also enable morally questionable behavior. The CPSR developed a similar, though less detailed, list of ethical principles as the ACM. CPSR’s Ten Commandments proscribe wrongs that may arise in a computer professional’s work life. This code of personal conduct parallels the Biblical Ten Commandments in being overwhelmingly composed of “don’ts” rather than positive actions.

Both the ACM’s and CPSR’s ethical codes are merely aspirational, like the Scout Oath or The American’s Creed, rather than a set of legally enforceable duties. The coercive power of law makes it difficult to craft. Criminal law must be carefully fashioned so that people know in advance what activities are illegal and have a clear idea of what punishment is proper. Hastily drafted statutes encourage unethical people to exploit legal ambiguities by sidestepping the exact wording of the law or they may unnecessarily frighten ethical individuals from doing the right thing for fear of legal jeopardy. The overwhelming message implicit in CPSR’s Ten Commandments is that moral principles frequently overlap with explicit legal duties and rights.

Unethical conduct can trigger legal liability as computer ethics is concretized in judicial opinions, regulations and statutes. Chart Two (below) describes U.S. laws that prescribe punishments for violating the CPSR’s ethical principles. The history and effectiveness of these and other laws, including the laws of the European Union, will be discussed in depth in subsequent chapters.

**CHART TWO: CPSR'S TEN COMMANDMENTS  
OF COMPUTER ETHICS**

Ten Commandments	Legal Issues Addressed	Illustrations
(1) Thou shalt not use a computer to harm other people.	Applies to cybercrimes as addressed by the Computer Fraud & Abuse Act and the Electronic Communications Privacy Act.	Intercepting an electronic communication or trespassing on a government computer.
(2) Thou shalt not interfere with other people's computer work.	Applies to cybercrimes and personal property cybertorts.	Ransomware, computer viruses and worms. Malicious software also constitutes the tort of trespass to chattels or conversion.
(3) Thou shalt not snoop around in other people's computer files.	Applies to the tort of the "intrusion upon seclusion," a privacy-based tort and a crime under the Computer Fraud and Abuse Act, which forbids downloading data without authorization.	Obtaining data from a computer system's private files. Snooping around in another person's files or reading someone else's personal messages.
(4) Thou shalt not use a computer to steal.	Applies to cybercrimes and to personal property, privacy torts and business torts.	Hacking constitutes a violation of the Economic Espionage Act as well as the misappropriation of trade secrets.
(5) Thou shalt not use a computer to bear false witness.	Covers many cybercrimes, cybertorts and regulatory actions by the Federal Trade Commission.	False information about individuals constitutes defamation.
(6) Thou shalt not copy or use proprietary	Prohibits using software without a license, which is both a violation of contract	Using proprietary software without a license can result in

software for which you have not paid.	law and intellectual property.	copyright or patent infringement lawsuits, which can result in millions of dollars in judgments and fines.
(7) Thou shalt not use other people's computer resources without authorization or proper compensation.	Unauthorized access to a password protected computer system is a crime under the Computer Fraud and Abuse Act and could also be a personal property tort.	Unauthorized access may also constitute a tort if the computer system is impaired. If the computer system is destroyed, the tort of conversion applies.
(8) Thou shalt not appropriate other people's intellectual output.	IP infringement can violate criminal law.	If a programmer uses software developed for his employer for other applications, it is likely a breach of a nondisclosure agreement and may constitute copyright infringement.
(9) Thou shalt think about the social consequences of the program you are writing or the system you are designing.	Failure to consider social consequences could result in tort liability.	Software engineers who do not consider social consequences may find themselves liable for negligent computer security, illegal discrimination and other torts.
(10) Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.	N/A (Only Commandment that does not address legal liability issues.)	The law does not reward good behavior. Instead, it penalizes bad acts.

## § 1.4: ETHICS & THE INTERNET OF THINGS

The Internet of Things (IoT) refers to all everyday consumer products and services that receive and transmit data on the Internet. A 2015 Federal Trade Commission report provides examples of this rapidly expanding phenomenon and the dangers presented by lax security:

The Internet of Things adds new security dimensions to consider. For example, an insecure connection could give a hacker access not just to the confidential information transmitted by the device, but also to everything else on a user's network. . . If that home automation system isn't secure, a criminal could override the settings to unlock the doors. And just think of the consequences if a hacker were able to remotely recalibrate a medical device—say, an insulin pump or a heart monitor.<sup>43</sup>

The IoT is evolving in a policy vacuum, with minimal regulation or legal precedent. Industry remains ill-prepared to deal with the security issues raised by smart products, despite the government's warning. In September 2016, cybercriminals took advantage of substandard IoT security to build a massive botnet using smart devices such as Internet-enabled televisions, baby monitors, security systems, cameras and printers.

Companies like Amazon, Twitter and Netflix were crippled for hours, while Internet access was interrupted on the East Coast. Whether the burden of such losses should be principally borne by the websites or by those who did not adequately protect their devices is a legal and ethical judgment that will shape the future of information engineering.

Internet-enabled vehicle safety devices, for example, can dramatically lessen the carnage on America's highways, but they also raise vexing ethical and legal issues. This technology permits the tracking of any automobile. Under what circumstances should law enforcement personnel be permitted to access a car's travel record? When should insurance companies or traffic police be allowed to evaluate the safety of a driver's conduct? When should an employer be permitted to check an auto's electronic records to see if the employee took an unauthorized break? Should the records be available to determine whether a restraining order has been violated or should the records be automatically destroyed to preserve individual privacy?

If these questions in applied ethics appear complex, examine the "futurecraft" city envisioned by the Massachusetts Institute of Technology's Senseable City Project, where nanosensors, cell phones and other information-gathering devices would provide optimal services by tracking every movement of

individuals.<sup>44</sup> People could be warned away from crime scenes or traffic jams and toward opportunities to engage in their favor hobbies. Developing new laws to regulate this predicted “smart city” will require ethical visionaries. How should information engineers make certain that this highly useful technology does not create a dystopian future in which constant surveillance renders privacy nonexistent?

### **Policy Issues for the Internet of Things (IoT)**

What are the privacy concerns raised specifically by IoT? How are they different from other privacy concerns?

Do these concerns change based on the categorization of IoT applications? What role or actions should the Department of Commerce and, more generally, the federal government takes regarding policies, rules and standards about privacy and the IoT?

Are there other consumer protection issues that are raised specifically by IoT? If so, what are they and how should the government respond to the concerns? In what ways could IoT affect and be affected by questions of economic equity? In what ways could IoT potentially help disadvantaged communities or groups? Rural communities? In what ways might IoT create obstacles for these communities or groups?

What effects, if any, will Internet access have on IoT, and what effects, if any, will IoT have on Internet access? What role, if any, should the government play in ensuring that the positive impacts of IoT reach all Americans and keeping the negatives from disproportionately affecting disadvantaged communities or groups?

Source: United States Department of Commerce, *Internet of Things* (2017).

## **§ 1.5: GLOBALIZED LAW AND ETHICS**

### **[A] The Internet as a Cross-Border Legal Environment**

Advances in information technology are bringing cultures that were once geographically separate into constant interaction. The Internet crosses national borders at the speed of light, making it very difficult to avoid violating different national laws and moral standards. No virtual tollgates warn users that they are entering into the jurisdiction of a country with very different legal, ethical and political realities.

## **[B] Global Business Dilemmas**

A U.S. e-commerce business must not only comply with consumer law, competition law and regulations in every country where it does business, but its corporate leadership must understand that law enforcement effectiveness varies significantly around the world. Highly paid industrial and professional jobs may also be readily transferred to much less expensive Third World countries or assigned to robots, destroying what were once the secure careers of millions. Some futurologists foresee a huge growth of unemployment among those replaced by artificially intelligent machinery, which might require a vastly expanded, globalized system of unemployment compensation or mass retraining of displaced workers.

## **[C] Cross-Border Cultural Clashes**

European law differs sharply from U.S. legal practices in evaluating what is protected as free expression. For example, the Union of Jewish French Students filed suit against Twitter because it refused to disclose the “names of anti-Semitic tweet authors, despite a French court ruling commanding their identification.” In the United States, these tweets, though objectionable to many, are protected expression under the First Amendment of the U.S. Constitution.

Some European countries still retain anti-blasphemy criminal law but Europe’s recognition of free expression as a fundamental right is now supplanting the older law. In May 2017, the Irish government investigated Stephen Fry for blasphemy after the prominent actor was quoted as asking why he should “respect a capricious, mean-minded, stupid God who creates a world that is so full of injustice and pain?” and for denouncing God as “utterly monstrous.” Irish prosecutors did not file charges against Fry. It is highly unlikely that the European Court of Justice would permit prosecution for these anti-religious statements, as free expression is also a fundamental right throughout the European Union.

In the United States, the First Amendment protects comedians like Bill Maher, who calls religion a mass delusion.<sup>45</sup> Maher, in his HBO show *Real Time* denounced what he considers liberals’ mistaken argument that both Christians and Muslims are equally likely to engage in violent religious intolerance: “Are there Christian terrorist armies like ISIS, Al Qaeda, Boko Haram, al-Shabaab? Are there armies like that in the world that aren’t Muslim?”<sup>46</sup> In contrast, in July 2017, a Pakistani was sentenced to death for insulting Mohammed in a Facebook post.<sup>47</sup>

Website designers and operators must tailor their content to conform to radically different legal cultures. A news story critical of Islam or the Prophet Mohammed is blasphemous in Saudi Arabia and lead to severe punishment of the

author. This same story would be protected expression under the First Amendment of the U.S. Constitution and as a fundamental right under European law. Article 11 of the European Union's Charter of Fundamental Rights guarantees the "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers."<sup>48</sup>

Where exactly is the line between free expression and enabling terrorism? A Christian Coptic living in California produced *The Innocence of Muslims*, an anti-Islamic film trailer that portrayed Mohammed as a hypocrite, looter and sexual deviant. The amateurish trailer, dubbed in Arabic, was uploaded to YouTube in September 2012, inciting riots that led to fifty deaths and hundreds of injuries throughout the Middle East. Afghanistan, Bangladesh, Sudan and Pakistan blocked YouTube because it would not remove the incendiary video. Should such postings be forbidden as dangerous hate speech or protected under the right to religious freedom?

### **[D] Terrorism and Hate on the Internet**

The Boston Marathon bombers learned to make pressure cooker bombs from an online magazine called *Inspire*, which, in 2010, published detailed instructions for creating lethal devices out of easily acquired materials. How aggressive do websites need to be in locating and removing such potentially dangerous postings? Well after the terrorist attack, a *Guardian* newspaper reporter viewed "a 30-slide guide about how to build a bomb posted on Facebook. Although it was removed by moderators, it had been on the site for some time—and reappeared again weeks later."<sup>49</sup>

Determining whether to block hate speech on the Internet always involves balancing ethical values such as safety, security and property rights against free expression. YouTube, as a privately owned business, is developing its own standards of decency. The website's software reviews hundreds of millions of clips to purge the site of videos showing brutal crimes or glamorizing terrorism. In August 2017, YouTube adopted a new policy calculated:

to catch and flag what it calls "controversial religious and supremacist" videos hosted on the platform. The platform plans to hide these videos from wider audiences and demonetize them to prevent their creators from earning revenue from YouTube.<sup>50</sup>

The Internet forces a rethinking of human rights, legal jurisdiction and other basic moral and legal concepts. Regions with no tradition of free speech feel themselves assaulted by disruptive, obscene and blasphemous online postings. In

contrast, nations that highly value free expression complain of suffocating foreign censorship. The international harmonization of cyberspace law is proving to be extremely complex because different regions vary in their cultural beliefs, legal systems and economic interests.

## § 1.6: ETHICAL NORMS & LAW

Basic agreements on ethical values are the glue that hold voluntary communities together. Internet users collectively determine what violations of these unwritten rules should be penalized. Sociologists divide these collective norms into “mores” (ethical norms reflecting fundamental values) and “folkways” (customary ways of doing things). Spamming, pop-up ads and excessively commercial conduct on websites are relatively minor violations that are classified as folkways. Distribution of child pornography violates mores in the great majority of social circles. In the absence of legal enforcement, group members may develop informal ethical codes that can be enforced through ostracism, harassment or banishing.

In the early years of the Internet, there were few laws regulating online activity. Lacking an effective legal code, citizens of the Internet, or netizens, developed their own normative rules and enforced them through the cyberspace version of vigilante justice. Without a physical presence, a lynch mob can hang no one. However, informal social control mechanisms emerged in the 1990s, when the online community was far smaller and more cohesive than today’s Internet community.

Social ostracism augments acceptable use policies, which tend to be normatively, not legally, based. In a well-known incident, customers in a San Francisco Apple retail store “noticed a vaguely androgynous person spending a lot of time there with a computer,” using the store’s free wireless, which negatively affected the system’s availability to others. “Some people became annoyed at the person and they blogged and posted pictures online” to embarrass the norm breaker. Employing YouTube to shame the annoying Apple user illustrates the emergence of informal social controls to both establish and enforce norms.<sup>51</sup>

Informal social controls also played an important role in punishing bad behavior in the early chat rooms where snarky comments tended to quickly spiral into insulting postings. Angry users “flamed” racists, spammers and deceitful advertisers to enforce ethical norms of civility in the early Internet. “Bozo filters” blocked messages from excessively loquacious participants in discussion groups. User communities still employ online shaming tactics to enforce norms against certain types of behavior when formal legal remedies are either unavailable or

impractical. Public humiliation has now been crowd sourced to outraged Internet denizens who may fire off a stream of hostile postings that attack the violator of informal norms. For example, when L.A. Fitness refused to cancel the memberships of a couple who had lost their jobs, Internet hostility led the company to reverse its policy. Cyberbullies or aggressive proponents of unpopular viewpoints would find their email systems subject to denial of service attacks or other forms of cyber harassment.

The contemporary Internet is too immense and multifaceted to be self-governed by the informal norms and vigilante sanctions that punished wrongdoers during the Internet's infancy. Moderators are often empowered by website owners to enforce norms against purposeful harassment or distasteful Internet postings. Networking site administrators regularly suspend subscribers for spamming, profanity, harassment or other breaches of "netiquette." At some point, moderators employ the equivalent of capital punishment for those who violate norms by permanently banning persistent rule-breakers.

Many computer game servers have automated the process of ejecting rule-breakers. When a user is banned from an online game, the reason for the exclusion is posted to shame the ex-user for his failure to follow the norms of e-sportsmanship. Banned posters often complain that their Constitutional right to free expression has been violated, only to find out that the First Amendment of the U.S. Constitution only applies to governmental actions, not the actions of private actors, such as website owners, private employers or social networks. Posters, of course, are free to leave a website if they disagree with its policies.

## § 1.7: PROFESSIONAL ETHICS

The term "professional" has expanded in the popular lexicon to apply to dedicated practitioners of almost any specialized activity. The Professional Bike Mechanics Association promotes the interests of technicians who repair bicycles. The Professional Beauty Association is the largest and most inclusive trade organization of the beauty industry. Elite athletes, such as NFL or NBA players, label themselves as professionals because they have a strong personal drive to excel. When athletes are asked whether the team will be negatively impacted by unfavorable playing conditions, they often respond that they are professionals who will do their best no matter what unusual difficulties they encounter.

Both law and sociology consider this common use of the term "professional" to be incorrect. A profession for these scholars is an occupational group that mandates specialized educational training, credentialing and adherence to a code of ethics, such as the fields of law and medicine. Professionals owe a fiduciary

duty to their client, which means that consumers have both a legal and ethical right to receive a higher duty of care. Professional ethics is a subfield of applied ethics that attempts to develop the rules of right and wrong in established professions where practitioners must make decisions beyond the expertise of ordinary persons.

### **[A] What Are Professional Ethics?**

Laws governing the traditional professions are comprised of specific duties, established by the state as necessary for maintaining social order, resolving disputes and properly distributing societal resources. Professional ethics may differ from ordinary norms of morality. A criminal defense attorney, for example, has an ethical duty to zealously represent his or her client, even if there is clear evidence of guilt. Some canons of professional responsibility are imported into formal legal duties, such as rules against disclosing the confidential information of clients or misusing client's funds. The norms of ethical communication between a doctor and patient are increasingly shaped by the legal rules that mandate confidentiality and informed consent.

Some cynics charge that the professions are hypocritical conspiracies against the public interest designed primarily to enrich its members. Critics of the legal profession, medical profession and actuaries note that professional organizations make it difficult for "competitors to set up shop. Very long qualification periods and professional bodies that give approval only to a certain number of candidates per year can be viewed as a way of keeping fee payments exorbitantly high."<sup>52</sup>

To become a patent attorney or patent agent, for example, it is necessary to pass the Patent Bar Examination, which is only open to individuals possessing a scientific or technical educational background. This requirement can be viewed as a valid method of ensuring the competence of patent agents, though it inevitably increases the cost of obtaining a patent.

New hardware and software developments are undermining the traditional professions and challenging their ethical codes. Smart devices using expert systems that incorporate artificial intelligence to learn and adapt over time are displacing some of the straightforward professional services. Routine legal work such as discovery is increasingly being automated through software. Bots have been designed to mount legal challenges to invalidate parking tickets. A bot has been developed enabling the victims of Equifax data breach to sue the company in small claims court without the need to retain an attorney.

Fewer lawyers are needed for reviewing legal papers and background information because software applications enable faster and more efficient data searches and document management. E-discovery enables a single lawyer to search through massive numbers of documents in seconds and to gain valuable information about whether to negotiate settlements. YouTube and other content-heavy websites use software to automatically take down infringing or illegal content.

Aggressively competitive technology companies, such as Facebook, whose long-time motto was “move fast and break things,” tend to be skeptical about the relevance of rigid professional codes in their dynamic industry. Big picture thinking encourages the development of disruptive technologies that can revolutionize long established, but inefficient, corporate practices. However, this social network giant recently dropped its original motto in favor of stressing better consumer service, which suggests at least a slight move in favor of the traditional view of the need to build a reputation for high ethical standards:

We used to have this famous mantra . . . and the idea here is that as developers, moving quickly is so important that we were even willing to tolerate a few bugs in order to do it. . . . “What we realized over time is that it wasn’t helping us to move faster because we had to slow down to fix these bugs and it wasn’t improving our speed.”<sup>53</sup>

Silicon Valley has come under criticism for its lack of ethical grounding. High profile startups, such as blood testing company, Theranos, the human relations management systems provider Zenefits, the loan matching company, Lending Club, and others stand accused of misrepresenting the capabilities and success of their products. Critics call for better ethical training because “more money is sloshing around (\$73 billion in venture capital was invested in U.S. startups in 2016, compared with \$45 billion at the peak of the dotcom boom, according to PitchBook), there’s less transparency as companies stay private longer (174 private companies are each worth \$1 billion or more), and there’s an endless supply of legal gray areas to exploit as technology invades every sector, from fin-tech and med-tech to auto-tech and ed-tech.”<sup>54</sup>

Google, and many other leading technological companies, have enacted codes of conduct to provide ethical guidance to their employees and users. Google’s Code of Conduct emphasizes the need for a moral rudder that is strong enough to guide employees in times of uncertainty:

It’s impossible to spell out every possible ethical scenario we might face. Instead, we rely on one another’s good judgment to uphold a high

standard of integrity for ourselves and our company. We expect all Googlers to be guided by both the letter and the spirit of this Code. Sometimes, identifying the right thing to do isn't an easy call. If you aren't sure, don't be afraid to ask questions of your manager, Legal or Ethics & Compliance. And remember. . . don't be evil, and if you see something that you think isn't right—speak up!<sup>55</sup>

Uber's reputation has been badly damaged by what is perceived as an overly aggressive workplace culture, and this is leading it to formulate a more socially acceptable set of ethical conduct guidelines. Uber is "at the center of all this ever-growing list of ethical leadership controversies. The company is accused of violating the most basic standards of business ethics to stifle competition."<sup>56</sup>

The #DeleteUber boycott campaign, which is protesting alleged sexist behavior within the company as well as other moral failings, has led to multiple employee resignations, substantial turnover in the board room and a significant loss of business. Travis Kalanick, Uber's founder was replaced in large part because of his perceived failure to prevent widespread unethical behavior in the company.

## **[B] Medicine as a Profession**

Information technology has yet to become an established profession such as medicine and law. The field of medicine is marked by a mandated curriculum that includes rotations, internships and residencies. Medical schools' admission criteria and their curriculums are similar across the country. After completing four years of medical school, students pursue residencies of three or four years, depending on specialty, and then optional fellowships that last a year or two. Doctors must complete national uniform testing with certification for specialties, such as emergency medicine, pediatric anesthesiology or psychiatry. Physicians who enter into doctor-patient relationships have both an ethical and a legal duty not to abandon their patients. Medical professionals, for example, do not request payment for emergency treatment when they come to the rescue of an airplane passenger who suddenly becomes ill.

The medical field's professional association, the American Medical Association, sharply limits what tasks a nurse or physician's assistant can perform independently. No such formal rule applies in the field of information technology. Computer scientists are not licensed, and there is no state or federal organization that can prohibit them from practicing in their field of expertise. State Medical Boards, in contrast, have the power to conduct a thorough investigation, and have the legal authority to revoke a physician's license.

In New York, for example, the Office of Professional Medical Conduct (OPMC) investigates complaints about physicians, physician assistants and specialist assistants. It also monitors practitioners who are subject to Orders of the State Board for Professional Medical Conduct. The OPMC publishes a list of all physicians, physician assistants, specialist assistants and professional medical corporations who have been disciplined since 1990, who are subject to a non-disciplinary Board Order, or upon whom charges of misconduct have been served.

State Medical Boards will suspend or revoke a doctor's license for serious ethical offenses, such as having a sexual relationship with a patient or performing surgical procedures while under the influence of alcohol. Public Citizen, a consumer rights advocacy group, believes that Medical Board oversight is too weak. The watch dog organization found slightly more than a thousand doctors were reported to the National Practitioner Data Bank due to offenses such as sexual misconduct, and subject to sanctions by medical boards or malpractice settlements over the past decade. State medical boards only acted in only one out of three cases where physicians were disciplined by hospitals or other health care organizations, or made malpractice payments related to an ethical infraction.

Expert testimony, rather than the experience of ordinary laypersons, determines whether a physician is liable for medical negligence. In a medical malpractice case, the crucial element is that the adverse event is of a kind that does not ordinarily occur unless there has been negligence. Courts require experts to testify as to the standard of care and breach, which are elements beyond the common understanding of a typical jury. Informed consent is a negligence concept predicated on the duty of physician to disclose to the patient all pertinent information that will enable him or her to understand the risks attendant to a course of treatment.

The medical profession is regulated by legal standards as well as the ethical codes of their professional association. For example, Congress enacted the Emergency Medical Treatment and Labor Act (EMTALA) in 1986, which requires Medicare-participating hospitals that offer emergency services to provide for an appropriate medical screening examination. If the hospital determines that the individual has an emergency medical condition, the EMTALA imposes a legal duty to stabilize the patient's medical condition, even if he is insolvent. This unfunded mandate is informally referred to as an "anti-dumping law," because it is designed to keep emergency departments from saving money by refusing to provide services for indigents.

## [C] Law as a Profession

Law, like medicine, is an established profession with a prescribed course of formal academic study. Law students nationally take similar courses in the first year of law school. After graduation, they must pass a state bar examination in order to practice law. Lawyers who violate the rules of their profession are subject to sanctions, such as having their law license suspended or being permanently disbarred. The Virginia Bar, for example, imposes graduated punishment for violations of ethical standards:

The lawyer can receive a private reprimand or admonition for less serious rule violations; The lawyer can receive a public reprimand for more serious rule violations; The lawyer's license can be suspended for up to five years, during which time the lawyer cannot practice law; or The lawyer's license can be revoked.

All U.S. attorneys must pass a Multistate Professional Responsibility Examination (MPRE) before they can practice law. The purpose of the MPRE is to assess a law graduate's knowledge and understanding of the specialized code of professional ethics followed by legal professionals. Professional ethics for lawyers are enforced by state bar organizations. In Massachusetts, it is the Board of Bar Overseers, whereas in Virginia, it is the Virginia State Bar (VSB). These state organizations develop lawyer-run disciplinary systems to determine whether a lawyer has violated legal ethics rules and, if so, what the appropriate discipline should be.

Professional associations serve their members by providing a variety of services, such as informing them of important new social, political and technology developments and risks. Bar Associations, for example, are educating their members about "social engineering" hoaxes, which have victimized many lawyers. In these "spear-phishing" attacks, cyber criminals target attorneys who have websites or have posted information about their bar membership. "Often, the e-mails contain accurate information about victims obtained via a previous intrusion, or from data posted on social networking sites, blogs or other websites. This information adds a veneer of legitimacy to the message, increasing the chances that victims will open the e-mail and respond as directed."<sup>57</sup> These phishing schemes will frequently involve fraudulent checks. Scammers frequently access attorneys' email address books to forward:

the e-mail from one attorney to another giving the appearance that it is a referral. It is apparently a scam enlisting attorneys to prepare legal documents upon receiving a cashier's check deposited in trust accounts

with an overpayment of legal fees being returned to the scammer from the attorney's trust account. The initial payment is fraudulent.<sup>58</sup>

### **[D] Computer Science Is Not a Traditional Profession**

Computer science meets all the qualifications of being a scientific discipline, but satisfies almost none of the criteria for being a traditional profession. Software engineering is a relatively new field without a prescribed curriculum or credentialing. Computer scientists have no formal educational requirements or established industry standards as in medicine and law. Lacking licensure requirements, software-coding boot camps are sprouting up across America.

In contrast to the in-depth education required for the four-year computer science degree, coding boot camps promise to make their students ready for employment in a few months at a tenth of the cost. These are the trade schools for the information age. In contrast, paralegals are required to be closely supervised by licensed attorneys just as licensed medical doctors, no matter what their level of skill and practical experience, supervise registered nurses.

Computer scientists cannot be reprimanded, suspended or prohibited from practicing in their field, as they have no professional associations or boards that have the power to police their practices. Whether professionalization is necessary or even desirable is an open question. Most computer practitioners resist traditional professionalization, viewing it as a barrier to innovation, anti-competitive and exclusionary. Computer science may never follow the path of law and medicine.

One exception to this resistance is the Professional Engineers Ontario (PEO). The province of Ontario, which accounts for nearly forty percent of Canada's population, has a strong professional organization that is empowered to investigate engineers who violate the organization's code of professional ethics and to bar violators from practicing their profession within its jurisdiction.<sup>59</sup>

Skilled hackers may be hired as computer security experts with minimal formal training, while alternatively, someone who learns a great deal of law while in prison could not simply become an attorney. Frank William Abagnale, Jr., a master conman and imposter, whose criminal career and imprisonment is chronicled in the book and movie, *Catch Me If You Can*, is advertising his expertise in countering forgery, embezzlement, and the theft of documents.

Abagnale's history of illegal activities is considered by some to be a better qualification for combating crime than having an advanced degree in computer security. Law or medicine, in contrast, does not permit self-taught individuals to

practice in any independent capacity, despite their skill level. In the field of information technology, results are generally valued over formal educational credentials.

Even though computer science requires advanced expertise that is beyond the understanding of typical members of the lay public, courts do not recognize computer malpractice because this field does not have a governing body (such as a state bar association), an enforceable code of professional ethics or licensing laws. Judges have uniformly rejected attempts to apply a professional standard of care to software engineers, designers or consultants.

## CONCLUSION

The rapid evolution of information technologies far outpaces the ability of computer ethics to keep up. Consequently, the study of computer professional ethics must center on general rules of applied ethics. Uses, misuses and abuses of technologies are hotly debated in the information era as practitioners struggle with common ethical issues such as:

Is it wrong for a system operator to disclose the content of employee email messages to employers or other third parties?

Should individuals have the freedom to post discriminatory, degrading and defamatory messages on the Internet?

Is it wrong for companies to use data-mining techniques to generate consumer profiles based on purchasing behavior, and should they be allowed to do so?

Should governments design policies to overcome the digital divide between skilled and unskilled computer users?<sup>60</sup>

Each of these decisions is not merely a matter of personal beliefs about right and wrong. The legal system may punish those who violate the laws that regulate these thorny issues.

When can corporations release software that they know contains design defects in order to win an early market share? Is it sufficient to electronically send patch after patch to fix software vulnerabilities that are discovered by hackers, or after examining the causes of system failures? Different ethical perspectives offer varying conclusions. Chapter Two will describe and apply the five leading ethical perspectives used to analyze and resolve moral dilemmas arising out of rapid advances in information technology.

## REFERENCES FOR CHAPTER ONE

- <sup>1</sup> Mary Ellen Biery, *The Ten Fastest Growing Industries in the U.S.*, FORBES (April 9, 2017).
- <sup>2</sup> Software & Information Industry Association, *The U.S. Software Industry: An Engine for Economic Growth and Employment*, SIIA White Paper (2014) at 2.
- <sup>3</sup> EDWIN PATTERSON, JURISPRUDENCE: MEAN AND IDEAS OF THE LAW (Brooklyn, New York: The Foundation Press, Inc., 1953) at 284.
- <sup>4</sup> Daisuke Wakabayashi, *Google Fires Engineer Who Wrote Memo Questioning Women in Tech*, THE NEW YORK TIMES (August 7, 2017).
- <sup>5</sup> *Fired Google Engineer Damore Says the Company is Hiring and Promoting Workers Based on Race or Gender*, CNBC.com (August 14, 2017).
- <sup>6</sup> *Id.*
- <sup>7</sup> BENJAMIN N. CARDOZO, THE GROWTH OF THE LAW (New Haven, Connecticut: Yale University Press, 1973) at 19–20.
- <sup>8</sup> Tim Harford, *Why Didn't Electricity Immediately Change Manufacturing?* BBC WORLD SERVICE (August 21, 2017).
- <sup>9</sup> Vivek Wahwa, *Law & Ethics Can't Keep Pace with Technology*, MIT TECHNOLOGY REVIEW (April 15, 2014).
- <sup>10</sup> Richard M. Nixon, *Changing Rules of Liability in Automobile Accident Litigation*, 3 LAW & CONTEMPORARY PROBLEMS 476 (1936).
- <sup>11</sup> Michael Frank, *The 13 Most Dangerous Car Interiors in History*, POPULAR MECHANICS (April 18, 2011).
- <sup>12</sup> *Henningsen v. Bloomfield Motors*, 161 A.2d 69, 99–100 (1960) (finding no contractual privity for breach of warranty in accident arising out of a malfunctioning automobile steering system).
- <sup>13</sup> 32 N.J. 358, 161 A.2d 69 (1960).
- <sup>14</sup> *Henningsen*, 32 N.J. at 384, 161 A.2d at 84 (finding liability against both Chrysler and Bloomfield).
- <sup>15</sup> 2 Restatement (Second) § 402A, comment (a).
- <sup>16</sup> *Bensusan Restaurant Corp. v. King*, 126 F.3d 25 25 (2d Cir. 1997).
- <sup>17</sup> 74 F.3d 701 (6th Cir. 1996) cert. denied 117 S. Ct. 74 (1996).
- <sup>18</sup> *Miller v. California*, 413 U.S. 15, 32 (1973).
- <sup>19</sup> Asher Schecter, *Is There a Case to be Made for Political Anti-Trust?*, PRO-MARKET (April 28, 2017).
- <sup>20</sup> Scott Shane & Vindu Goel, *Fake Russian Facebook Accounts Brought for \$100,000 in Political Ads*, THE NEW YORK TIMES (September 6, 2017).
- <sup>21</sup> Christopher Mims, *Facebook Is Still in Denial About Its Biggest Problem*, THE WALL STREET JOURNAL (October 1, 2017).
- <sup>22</sup> Tanya Dua, *Here's Facebook's Latest Move in the War on Fake News*, BUSINESS INSIDER (August 28, 2017).
- <sup>23</sup> ERIC T. SCHEIDERMAN, NEW YORK STATE ATTORNEY GENERAL, OBSTRUCTED VIEW: WHAT'S BLOCKING NEW YORKERS FROM GETTING TICKETS (2017) at 1.
- <sup>24</sup> *Id.* at 3–4 (Executive Findings).
- <sup>25</sup> Free Exchange: Algorithms and Antitrust, *How Price-Bots Can Conspire Against Consumers—and How Trustbusters Might Thwart Them*, THE ECONOMIST (May 6–12) at 71.
- <sup>26</sup> *Id.*
- <sup>27</sup> Leslie Morris, *Rating Systems May Discriminate Against Uber Drivers*, CORNELL CHRONICLE (December 15, 2016).
- <sup>28</sup> Laura Sydell, *Can Computers Be Racist? The Human-Like Bias of Algorithms*, NPR (March 14, 2016).
- <sup>29</sup> Jeff Larson et al., *How We Analyzed the Recidivism Algorithm*, PRO PUBLICA, (May 23, 2016).
- <sup>30</sup> Tom Dotan and Reed Albergotti, *Amazon Echo and the Hot Tub Murder*, THE INFORMATION (December 27, 2016).
- <sup>31</sup> Evan Andrews, *10 Things You May Not Know About the Pony Express*, HISTORY CHANNEL, HISTORY.COM (June 10, 2016).

- <sup>32</sup> Barry Waugh, *The Importance of the Printing Press for the Protestant Revolution*, REFORMATION (October 2013) at 21.
- <sup>33</sup> *Id.*
- <sup>34</sup> CHRIS HARMAN, *A PEOPLE'S HISTORY OF THE WORLD*, (New York, New York: Verso, 2017) at 178.
- <sup>35</sup> Paul Stanley: *'Illegal Music Downloading Is Morally and Ethically Wrong': KISS Frontman Compares File Sharing to Stealing a Car*, ULTIMATEGUITAR.COM (October 21, 2014).
- <sup>36</sup> *Artists Speak Out on Music Piracy*, UPVENUE.COM (December 27, 2016).
- <sup>37</sup> Matthew Yglesias, *Piracy is a Form of Theft, and Copyright Infringement is Neither*, SLATE (December 15, 2011).
- <sup>38</sup> Ken Paulson, *Real Cost of 'Free' Downloads*, USA TODAY (August 20, 2012).
- <sup>39</sup> Lucus Shaw & Adam Satarino, *Spotify is Burying Musicians for the Apple Deals*, BLOOMBERG TECHNOLOGY (August 27, 2016).
- <sup>40</sup> Leyla Acaroglu, *What Would Plato Do? Ethics Isn't Just for Philosophers—Designers Need to Take Responsibility, Too*, QUARTZ (September 28, 2016).
- <sup>41</sup> Margaret Anne Pierce and John W. Henry, *Computer Ethics: The Role of Personal, Informal, and Formal Codes*, 15 JOURNAL OF BUSINESS ETHICS 425 (1996).
- <sup>42</sup> ACM Ethics, Code 2018 Project.
- <sup>43</sup> Federal Trade Commission, *Careful Connections: Building Security in the Internet of Things* (2015) at 1.
- <sup>44</sup> Massachusetts Institute of Technology, *MIT Senseable City Lab* at <http://senseable.mit.edu/>.
- <sup>45</sup> *Bill Maher Calls It as He Sees It*, <https://schwartzdns.wordpress.com/bill-maher-calls-it-like-he-sees-it/>.
- <sup>46</sup> Chris Enloe, *Islamic Terrorism Has Nothing to Do With Islam*, THE BLAZE (March 25, 2017).
- <sup>47</sup> *Pakistan: Death Penalty for Blasphemy on Facebook*, Aljazeera (June 12, 2017).
- <sup>48</sup> Charter of Fundamental Rights of the European Union (2000/C 364/1) at Art. 11.
- <sup>49</sup> Ewen MacAskill & Nick Adams, *Bomb-Making Guides Are Online, But Getting Them to Work Is Not Easy*, The Guardian (May 23, 2017).
- <sup>50</sup> Ian Miles Cheong, *Popular YouTubers React to Censorship of 'Controversial' Content*, THE DAILY CALLER (August 1, 2017).
- <sup>51</sup> DANIEL J. SOLOVE, *THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET* (New Haven, Connecticut: Yale University Press, 2007) at 3.
- <sup>52</sup> TIM HARFORD, *THE UNDERCOVER ECONOMIST*, (Oxford, United Kingdom: Oxford University Press, 2007).
- <sup>53</sup> Samantha Murphy Kelley, *Facebook Changes Its 'Move Fast and Break Things' Motto*, MASHABLE (2014).
- <sup>54</sup> Erin Griffith, *The Ugly Unethical Underside of Silicon Valley*, FORTUNE (December 28, 2016).
- <sup>55</sup> Alphabet Investor Relations, *Google Code of Conduct* (last updated April 11, 2012).
- <sup>56</sup> *Uber is in Dire Need of Ethical Leadership*, INDUSTRY LEADERS (June 14, 2016).
- <sup>57</sup> Internet Crime Complaint Center (2013).
- <sup>58</sup> Joanna Herzlik, *Scams Continue to Target Texas Attorneys*, TEXAS BAR BLOG (September 13, 2017).
- <sup>59</sup> The Code of Ethics of Professional Engineers Ontario, [http://ethics.wikia.com/wiki/The\\_Code\\_of\\_Ethics\\_of\\_Professional\\_Engineers\\_Ontario](http://ethics.wikia.com/wiki/The_Code_of_Ethics_of_Professional_Engineers_Ontario).
- <sup>60</sup> Phillip Brey, *Values in Technology and Disclosive Computer Ethics*, in LUCIANO FLORIDI, *THE CAMBRIDGE HANDBOOK OF INFORMATION AND COMPUTER*, United Kingdom: Cambridge University Press (2009) at 41.