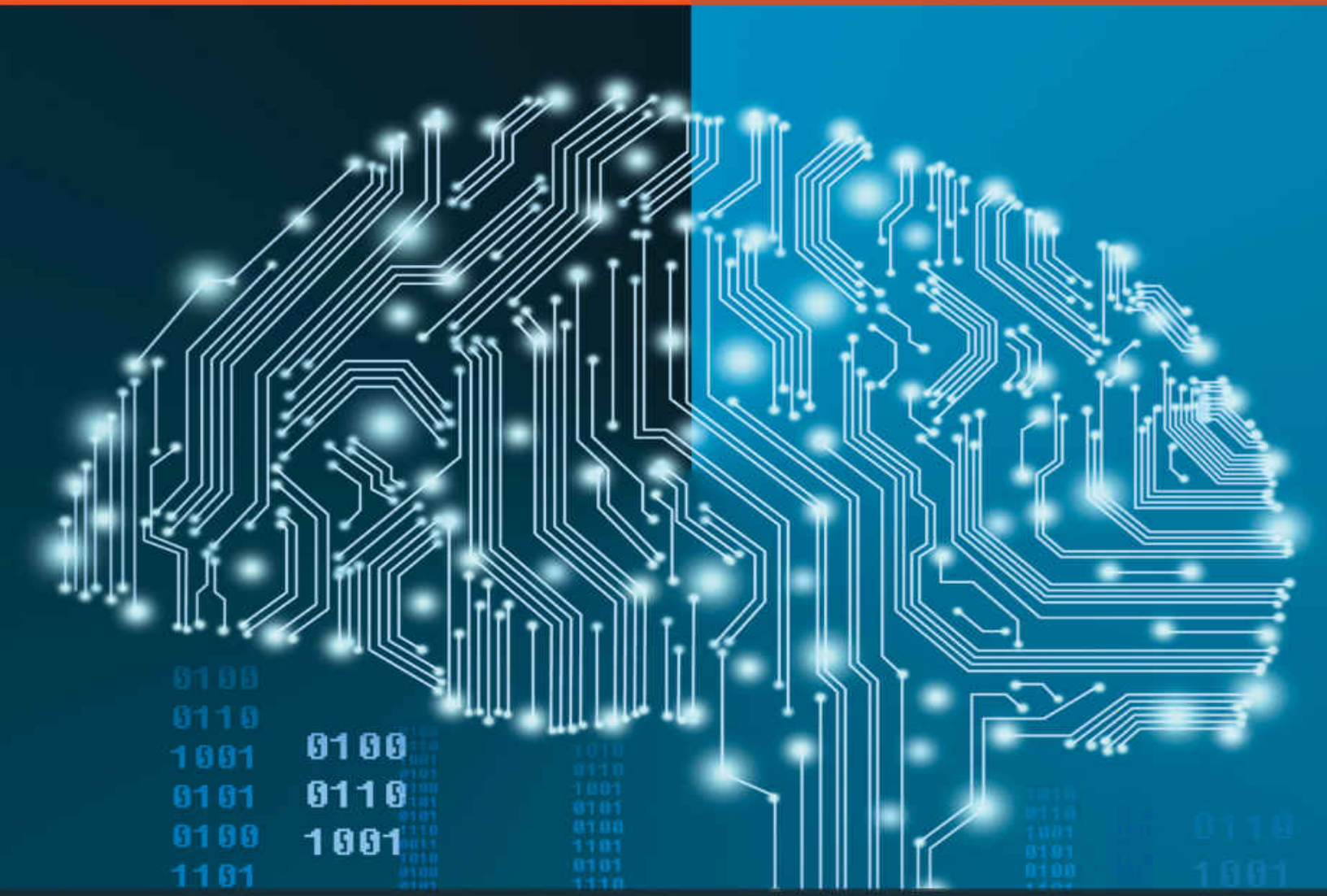
SEVENTH EDITION

CYBERETHICS

Morality and Law in Cyberspace



Richard A. Spinello

SEVENTH EDITION

CYBERETHICS

Morality and Law in Cyberspace

Richard A. Spinello

Professor of Management Practice
Carroll School of Management
Boston College
Chestnut Hill, Massachusetts

JONES & BARTLETT

LEARNING

World Headquarters
Jones & Bartlett Learning
5 Wall Street
Burlington, MA 01803
978-443-5000
info@jblearning.com
www.jblearning.com

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

Substantial discounts on bulk quantities of Jones & Bartlett Learning publications are available to corporations, professional associations, and other qualified organizations. For details and specific discount information, contact the special sales department at Jones & Bartlett Learning via the above contact information or send an email to **specialsales@jblearning.com**.

represent, or participate in the activities represented in the images. Any screenshots in this product are for educational and instructive purposes only. Any individuals and scenarios featured in the case studies throughout this product may be real or fictitious, but are used for instructional purposes only.

19913-0

Production Credits

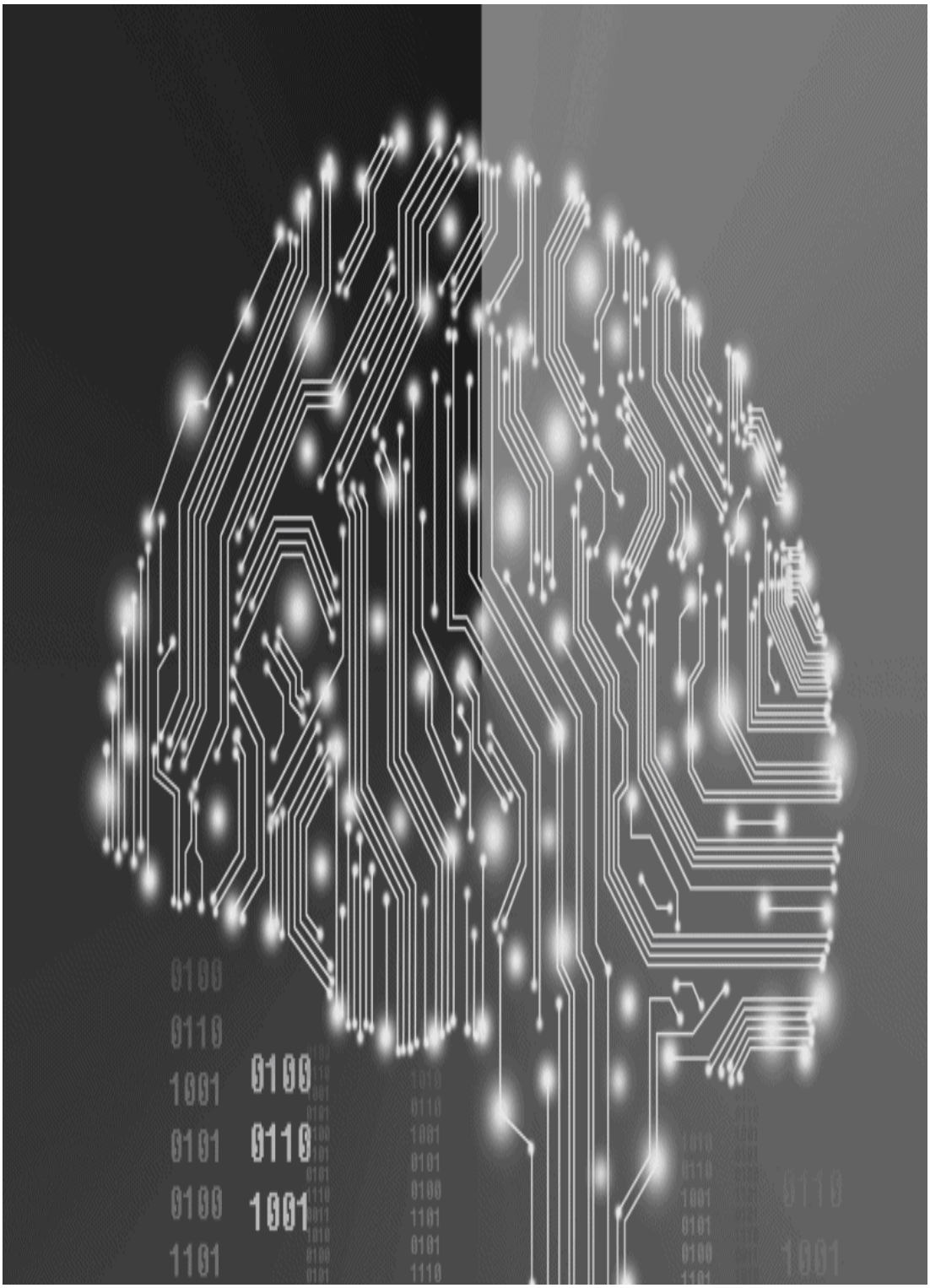
VP, Product Management: Amanda Martin
Director of Product Management: Laura Pagluica
Product Manager: Edward Hinman
Product Assistant: Melissa Duffy
Product Coordinator: Paula-Yuan Gregory Project Specialist: Jamie Reynolds
Digital Project Specialist: Angela Dooley
Marketing Manager: Michael Sullivan
Product Fulfillment Manager: Wendy Kilborn
Composition and Project Management: codeMantra U.S. LLC
Cover Design: Scott Moden
Text Design: Scott Moden
Senior Media Development Editor: Troy Liston
Rights & Media Specialist: Rebecca Damon
Cover Image (Title Page, Chapter Opener): © Dong Wenjie/Getty Images
Printing and Binding: McNaughton & Gunn

Library of Congress Cataloging-in-Publication Data

Names: Spinello, Richard A., author.
Title: Cyberethics : morality and law in cyberspace / Richard A. Spinello.
Description: Seventh edition. | Burlington, MA : Jones & Bartlett Learning, [2021] | Includes bibliographical references and index.
Identifiers: LCCN 2019042895 | ISBN 9781284184068 (paperback)
Subjects: LCSH: Internet--Moral and ethical aspects. | Cyberspace--Moral and ethical aspects. | Computers and civilization. | Law and ethics.
Classification: LCC TK5105.875.I57 S68 2021 | DDC 303.48/34--dc23
LC record available at **https://lccn.loc.gov/2019042895**

6048

Printed in the United States of America
24 23 22 21 20 10 9 8 7 6 5 4 3 2 1



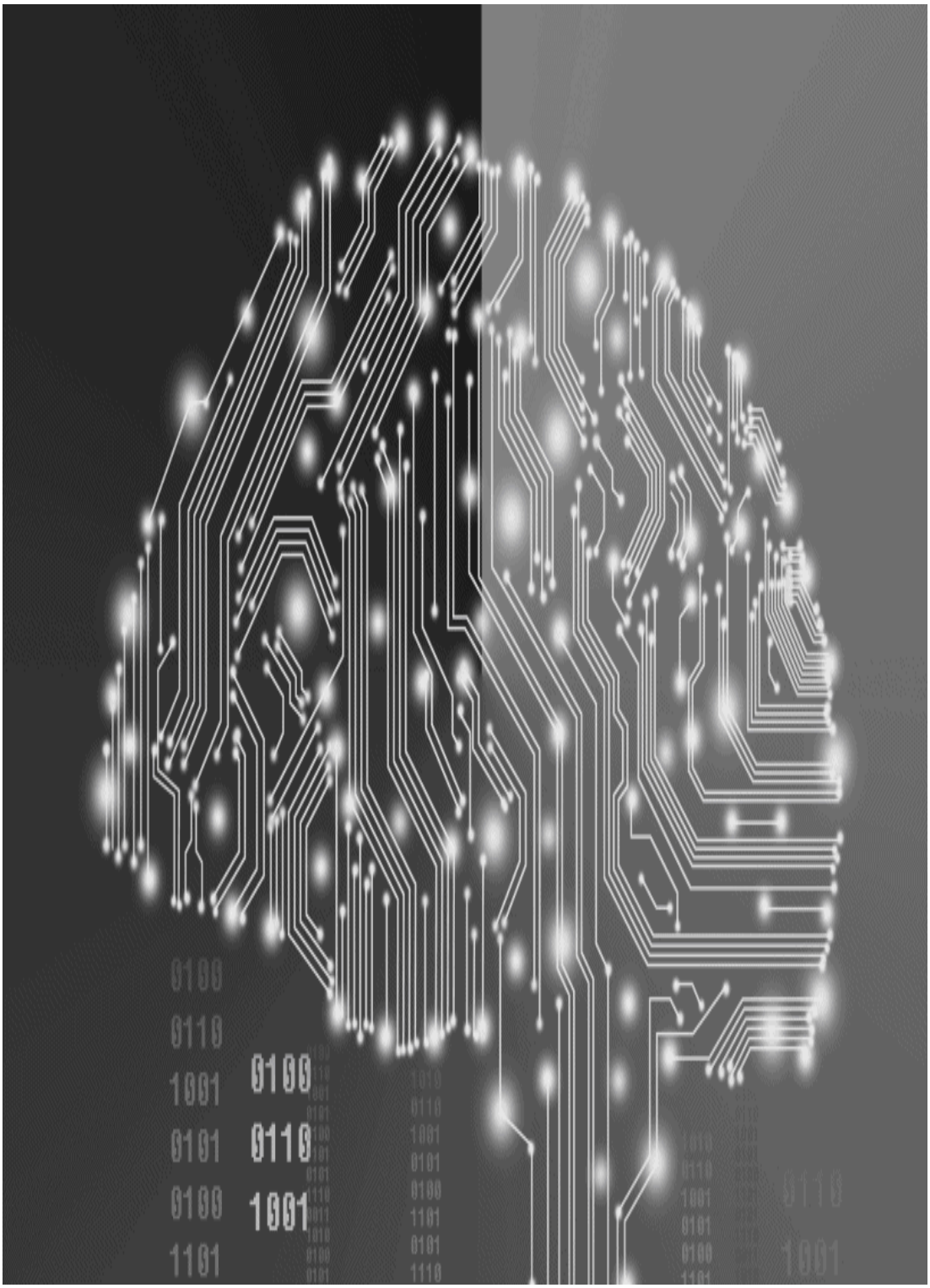
CONTENTS

CHAPTER 3 Free Speech and Censorship in Cyberspace

CHAPTER 4 Intellectual Property in Cyberspace

CHAPTER 5 Privacy Rights in the Age of Surveillance

CHAPTER 6 Securing the Digital Infrastructure



PREFACE

Since the sixth edition of *Cyberethics: Morality and Law in Cyberspace* appeared several years ago, the social and technical landscape of cyberspace has undergone signifi cant changes. In the United States, the intense debate over "net neutrality" continues, while the European Union has passed a new set of strict privacy laws known as the General Data Protection Regulation. Major security breaches at companies like Yahoo and Equifax have focused unprecedented attention on cybersecurity. Fake news, propagated on social media platforms like Facebook, disrupted the 2016 Presidential election in the United States, as social media companies grapple with how to deal with disinformation among its several billion users. The clash between Oracle and Google over software copyright protection reveals that, despite the popularity of open source code, some companies still zealously protect their intellectual property. And the new "crypto wars" have intensifi ed, thanks to the strong encryption now being used for consumer devices like iPhones and software programs such as WhatsApp. We have tried to take these and other developments into account in this new edition.

This technological dynamism, known as the internet, continues to shape our personal and professional lives, but not without social costs. Aside from the growing use of political censorship by tech oligarchs like Google, what is especially worrisome is the more pronounced erosion of privacy with few paths of resistance available for most users. Vast quantities of personal data are extracted and assembled in order to make targeted advertising more precise. Linked to this problem is the matter of information

security and the abject failure of many companies to properly safeguard their data.

This Seventh Edition preserves much of the thematic content of previous editions, but also carefully reviews these emerging social problems and the fresh assaults on basic rights such as privacy. Our related purpose is to stimulate the reader's refl ection on the broad issues of internet regulation and the behavior of platform monopolies such as Facebook and Google. Have those companies become a threat to individual liberty and free choice?

To accomplish our objectives, we first lay out some theoretical groundwork drawn from the writings of contemporary legal scholars and philosophers such as Kant, Locke, and Finnis. We then focus on four broad areas: censorship and free speech, intellectual property, information privacy, and cybersecurity. For each of these critical areas, we consider the common ethical and public policy problems that have arisen and how technology, law, or some combination of the two would resolve some of those problems.

The first of these four topics concerns the fringes of internet communication, such as pornography, hate speech, and online threats. We review the history of public policy decisions about the problem of pornography and consider in some depth the suitability of automated content controls. Are these controls technically feasible, and can they be used in a way that is morally acceptable to the relevant stakeholders? We also consider other prominent free speech issues, such as private censorship by platforms like Facebook and Twitter, violent video games, and the

censorship infrastructures that have been constructed in countries like China.

We then review the full spectrum of intellectual property issues that accompany the digitization of information. These include ownership of domain names, peer-to-peer networks, software patents, the practice of remixing, and eBook pricing schemes that best reward creative authors. There are new critiques of restrictive copyright and patent laws that proclaim the primacy of open source code along with a robust digital commons. Those critiques insist that networked spaces should generally be devoid of digital locks or anti-copying systems. This chapter concludes with a case on the acrimonious dispute between Oracle and Google over the scope of software copyright protection.

The issue of information privacy is the next topic. The primary axis of discussion is on the new threats posed by companies, like Google and Facebook, that seek to manipulate and monetize our behavioral data. The chapter begins with some theoretical material on the nature of privacy but then proceeds to an assessment of these threats. What, if anything, should be done about the privacy-invasive technologies that are the source of such substantial profits for the digital giants? Is the solution to be found in technology itself or in the comprehensive laws being developed in venues such as the European Union?

Finally, we treat the critical area of cybersecurity and pay special attention to the vulnerabilities of our technical infrastructure. We dwell on the issue of hacking and on the philosophy of hacktivism as a means of civil disobedience. Effective measures companies must take to protect their information systems and data are also considered. In this

context we treat encryption technology and policy. The controversy over unbreakable encryption, which has now spread to the iPhone and other mobile technologies, epitomizes the struggle between government control and individual rights that has shaped many of the public policy debates about the internet.

What can be done about all of these problems? While individuals are becoming increasingly subordinate to the exigencies of modern technology, they still have the capacity to control its use and curtail its injurious side effects. Such control requires prudent assessment and decision making, which will help to ensure that technology is utilized with respect for standards of justice and fairness.

Like most traditional books on ethics, this one emphasizes virtues such as honesty, openness, and solidarity. It is optimistic about the tenacity of the human spirit and the depth of moral conviction, even in cyberspace where certain trends must be resisted. The technology determinists believe that the forces of technology have already won the battle, but the realists, buoyed by the promise of greater freedom and egalitarianism, contend that the struggle continues and that the final outcome is still in doubt.

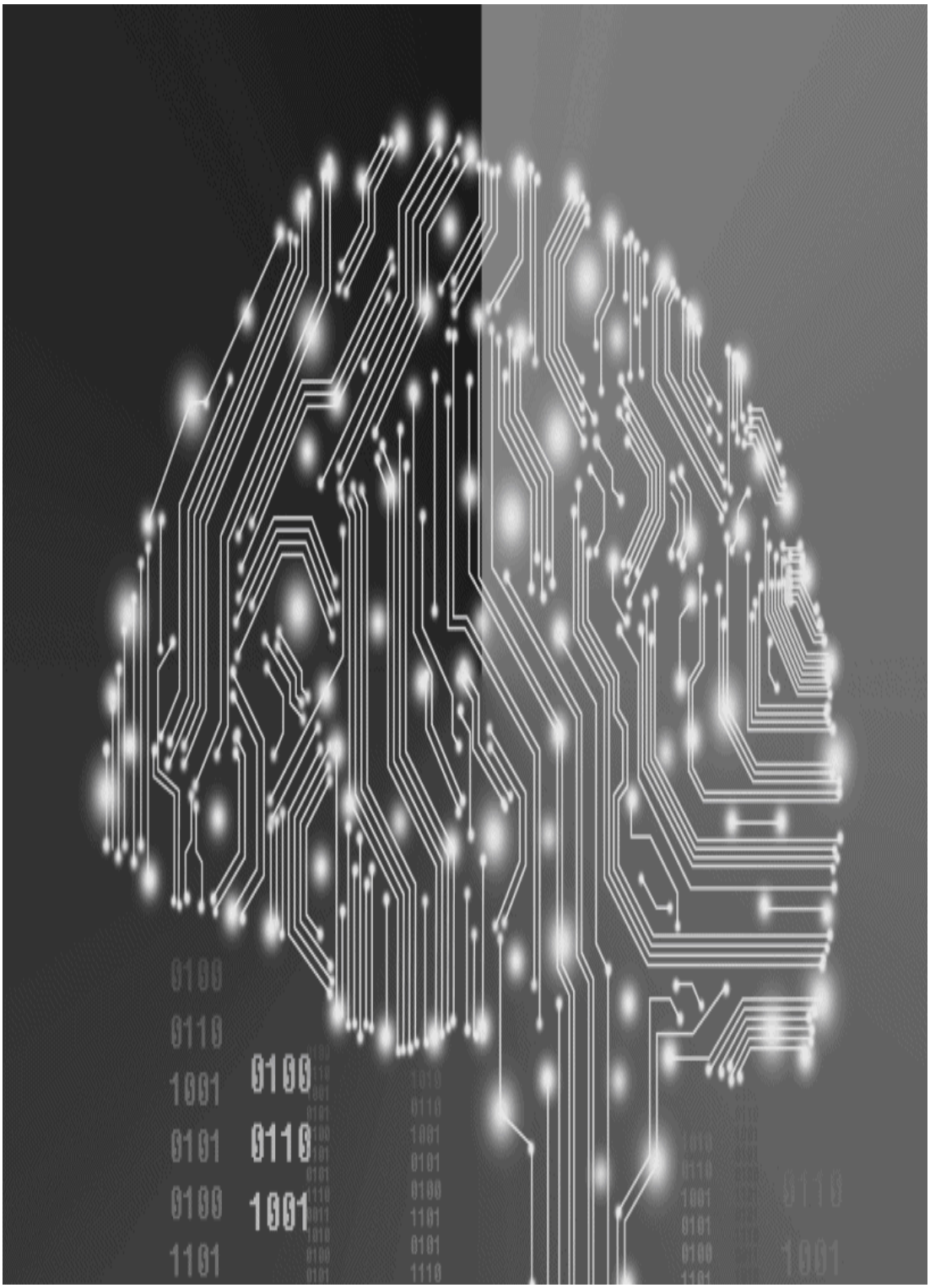
Additional Resources
For the Seventh Edition, a Test Bank, Slides in PowerPoint format, an Instructor's Manual, and a Sample Syllabus are available for instructor download. Visit **go.jblearning.com/Cyberethics7e** to request access.

Acknowledgments

It is an honor to acknowledge many individuals to whom I owe a debt of gratitude. The list begins with many faculty members at a wide range of universities who have adopted the first six editions of this book. They have given me valuable feedback and suggestions that I have attempted to incorporate into this new Seventh Edition. I am indebted to the Carroll School of Management which encourages and fosters work on ethical topics such as the ones discussed in this book. I am especially grateful to the chairperson of the Management and Organization Department, Judy Gordon, and to Dean Andy Boynton for their continued support for my research. Thanks also to Michael Smith for handling some of the logistics of manuscript preparation, and to Ezabel Lynch for her invaluable assistance in helping me acquire some of the research material for this project. And many thanks to several individuals at Jones & Bartlett Learning, especially Laura Pagluica, Ned Hinman, and Melissa Duffy for their invaluable assistance in publishing this Seventh Edition. Finally, I owe a great debt of gratitude to my wife, Susan T. Brinton, for her patience and continued tolerance for the lonely life of an author.

Richard A. Spinello

Dedham, MA



CHAPTER 1

The Internet and Ethical Values

Many decades have passed since the first communications were transmitted over a fledgling global network, which would later be called the internet. At the time, few would have predicted the internet's explosive growth and persistent encroachment on our personal and professional lives. For techno-optimists, the emancipatory promise of this technical infrastructure is still unfolding. As the internet matures it has become a more personal experience, thanks to the fusion of smartphones and social networks. Retrieving the latest news, an online search with Google's help, listening to music, watching a YouTube video, and checking one's Newsfeed on Facebook are just some of the activities done countless times each day with the help of apps and mobile devices.[1]

Some sovereignties, however, have felt threatened by this decentralized power and information egalitarianism. As a result, they have attempted to extend their power over this anarchic network and its information flows. However, the control of networked technologies through law and regulation has often been a futile effort. Technical infrastructures that expedite the flow of information can easily become a means for obstructing or excluding information. The regime of law has had a hard time suppressing the dissemination of pornography on the internet, but software systems that filter out indecent material have been much more successful. This reality reflects technology's paradoxical nature—it not only endows

individuals with the capacity to more fully exercise their rights (such as free speech), but it also makes possible the development of tools that can undermine those rights.

Although the primary axis of discussion in this text is the ethical issues that surface in the ever-expanding infosphere, we must devote attention to these related matters of cyber regulation and public policy. Thus, we explore in some detail the tensions between the radical empowerment network technologies have presumably allowed and the impulse to tame these technologies through laws and other mechanisms.

Because this is a text about ethics, about *acting* in the right way as a human person in both the real and the virtual worlds, we begin by reviewing some basic concepts that will enrich our moral assessment of these issues. Hence, in this introductory chapter our purpose is to provide a concise overview of the traditional ethical frameworks that can guide our analysis of the moral dilemmas and social problems that arise in cyberspace. We should bear in mind, however, the insight of Aristotle, who reminds us that while ethics is an applied science, every science is only as accurate as the subject matter allows. Therefore, we cannot expect mathematical certainty in ethics any more than we can find such certainty in disciplines like psychology or sociology. At the same time, ethics is a rational discipline with intelligible and objective principles that can be taught and defended.[2]

In addition, we also elaborate here on the two underlying assumptions of this work: (1) the directive and architectonic role of moral ideals and principles in determining responsible behavior in cyberspace and (2) our capacity to subject networked technologies to objective moral evaluation. Let us

begin with the initial premise concerning the proper role of cyberethics.

Cyberethics and Code

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

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

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

Social norms, on the other hand, are expressions of the community. Most communities have a well-defined sense of the common good, which is reflected in their norms or standards of behavior. There may be no laws against marijuana smoking in a private setting with young children present, but those who try to do so will most likely be stigmatized and ostracized by others. When we deviate from these norms, we are behaving in a way that is socially "abnormal."

The third regulative force is the market. The market regulates through the price it sets for goods and services or for labor. Unlike norms and laws, market forces are not an expression of a community and they are imposed immediately (not in *ex post* fashion). Unless you hand over $4 at the local Starbucks, you cannot walk away with a cup of their coffee.

The final modality of regulation is known as architecture. The world consists of many physical constraints on our behavior; some of these are natural (such as the Rocky Mountains), whereas others are human constructs (such as buildings and bridges). A room without windows imposes certain constraints because no one can see outside. Once again "enforcement" is not *ex post*, but at the same time the constraint is imposed. Moreover, this architectural constraint is "self-enforcing"—it does not require the intermediation of an agent who makes an arrest or who chastises a member of the community. According to Lessig, "the constraints of architecture are self-executing in a way that the constraints of law, norms, and the market are not."[3]

Lessig explains that in cyberspace we are subject to the same four constraints. Laws, such as those that provide copyright and patent protection, regulate behavior by proscribing certain activities and by imposing *ex post* sanctions for violators. It may be commonplace to download copyrighted digital music and movies from unauthorized websites, but this activity breaks the law.

Markets regulate commercial and personal interactions in cyberspace in various ways. The market reacted quite favorably to Google's targeted ads based on their users' behavioral data and rewarded the company with financial success. But the market has not been so kind to some of Google's competitors who cannot match its tracking

capabilities. Theoretically, consumers can migrate from privacy-invasive sites to those that respect privacy rights. It should be noted that the constraints of the market are often different in cyberspace than they are in real space. For instance, pornography is much easier and less expensive to distribute in cyberspace than in real space, and this increases its available supply.

The counterpart of architectural constraints in the physical world is software “code,” that is, programs and protocols that make up the application layer of the internet. They, too, constrain and control our activities. These programs are often referred to as the “architectures of cyberspace.” Code, for example, limits access to certain websites by demanding a username and password. Cookie technology enables e-commerce but compromises the consumer’s privacy. Sophisticated software has been successfully deployed to filter out unsolicited commercial email (or spam).

Finally, there is a changing set of norms that regulate cyberspace behavior, including internet etiquette and social customs. For example, spamming and hacking were always considered “bad form” on the internet, and those who did it were chastised by other members of the internet community. Just as in real space, cyberspace communities rely on shame and social stigma to enforce cultural norms.

But what role does ethics play in this neat regulatory framework? Lessig apparently includes ethical standards in the broad category he calls “norms,” but in our view cultural norms should be segregated from ethical ideals and principles. Cultural norms are nothing more than variable social action guides, completely relative and dependent on a given social or cultural environment. Their validity depends to some extent on custom, prevalent attitudes, public opinion,

and myriad other factors. Just as customs differ from country to country, the social customs of cyberspace could be quite different from the customs found in real space. Also, these customs will likely undergo some transformation over time as the internet continues to evolve.

The fundamental principles of ethics, however, are metanorms with universal validity. They remain the same whether we are doing business in Venezuela or interacting in cyberspace. Like cultural norms, they are prescriptive; however, unlike these norms, they have lasting and durable value because they transcend space and time. Ethics is primarily about (or should be about) the moral principles and norms of justice that apply to all human choices.

Our assumption that ethical standards are not reducible to customs or social convention defies the popular notions of personal or cultural relativism. A full refutation of these theories is beyond the scope of our discussion. But as David Oderberg has argued, personal relativism ultimately dissolves into moral nihilism, which stipulates that there are no objective moral rules that govern our interpersonal interactions. Similarly, Philippa Foot affirms that while it is wrong to assume the exact identity between people of different cultures, there is certainly a great deal that all human persons share in common with one another. The human person is intrinsically relational. Therefore, we all need love and affection, the cooperation of others, and an opportunity to live in community. Human beings simply cannot flourish without these things. When there is isolation and constant divisiveness or an absence of friendship and loving kindness, human fulfillment is damaged or impeded. According to Foot, we are not referring to arbitrary standards

> if we think of some moral systems as good moral systems and others as bad. Communities as well as individuals can live wisely or unwisely, and this is largely the result of their values and the codes of behavior that they teach. Looking at these societies, and critically also at our own, we surely have some idea of how things [will] work out based on values.[4]

None of this by any means invalidates Lessig's framework. His chief insight is that "code and market and norms and law together regulate in cyberspace as architecture and market and norms and law regulate in real space."[5] Also, according to Lessig, "Laws affect the pace of technological change, but the structures of software can do even more to curtail freedom. In the long run the shackles built by programmers could well constrain us more."[6] This notion that private code can be a more potent regulatory force than public law has significant implications. The use of code as a surrogate for law may mean that certain public goods or moral values, once protected by law, will be ignored or marginalized by those in both the private and the public sectors who design and implement this code. There is also a danger that governments will leverage the architectures of cyberspace to advance their own political or social agendas.

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

Before we can answer this question we must say something about the nature of those values. The notion that there are transcendent normative values that reflect our common human nature has a deep tradition in the history of

philosophy. It is intuitively obvious that there are basic human goods that contribute to human well-being or human flourishing. Although there are several different versions of what these goods might be, they do not necessarily contradict each other. Some versions of the human good are “thin,” whereas others are “thick.” James Moor’s list of core human goods includes life, happiness, and autonomy. According to Moor, *happiness* is “pleasure and the absence of pain” and *autonomy* includes those goods that we need to complete our projects (ability, security, knowledge, freedom, opportunity, reason). Individuals may rank these values differently, but all human beings attribute value to these goods or “they would not survive very long.”[7]

Oxford philosopher John Finnis offers a thicker version of the human good. He argues persuasively for a set of intrinsic goods that include life and the component aspects of its fullness (health, bodily integrity, and security), knowledge (including aesthetic appreciation), play and skillful work, friendship, and practical reasonableness. According to Finnis, participation in these goods allows us to achieve genuine human flourishing. These irreducible aspects of human well-being are opportunities for realizing our full potential as human beings, for being all that we can be.[8]

For both Moor and Finnis, then, the ultimate source of moral normativity is these intrinsically valuable human goods, which adequately explain the reasons for our choices and actions and overcome the presumption of subjectivism. Morality can begin to claim objectivity because this collection of basic human goods is not subjective or contingent on our cultural differences.

These intrinsic goods, intelligibly worthwhile as ends-in-themselves, constitute the foundation of morality and serve

as a basis for identifying moral rights and duties and for crafting just laws to govern human behavior. Those rights and duties can function as practical guidelines for moral decision making, as they enable us to pursue the basic human goods in a way that respects our fellow humanity. According to Finnis, our fundamental responsibility is to respect each of these human goods "in each person whose well-being we choose to affect."[9]

We contend, therefore, that these basic human goods, which are all aspects of our well-being, along with the rights and duties that flow from these goods, should play an architectonic or *directive role* in the regulation of cyberspace. They should guide and direct the modalities of regulation described by Lessig: code, laws, the market, and social norms. Moral principles, for example, must determine to some extent the laws that govern political communities so that those laws are rationally and morally grounded. And moral principles should inform activities such as writing software code. Accordingly, we have enhanced Lessig's model as depicted in **FIGURE 1-1**.

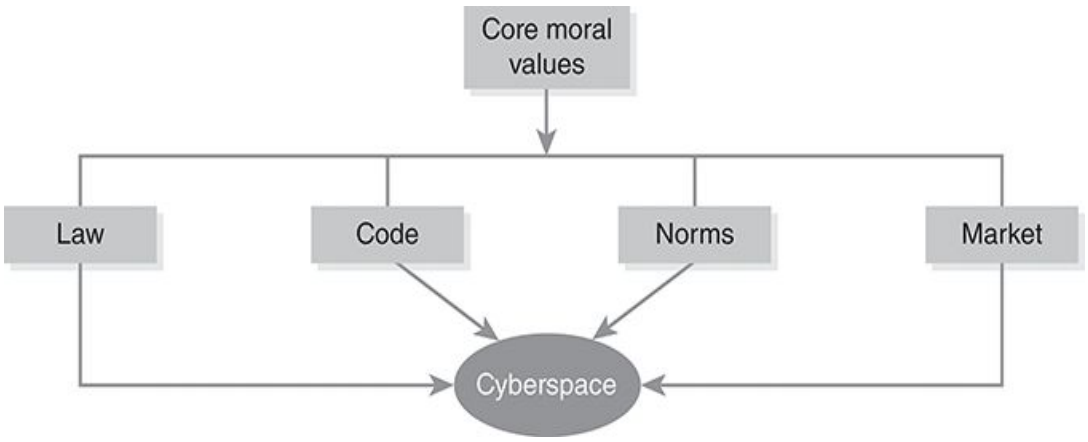


FIGURE 1-1 Constraints on Cyberspace Activities.

Data from Professor Lessig's framework.

To illustrate our point about the role of these directive ethical values, let us consider the regulatory impact and the power of code. From a moral point of view, there are responsible and irresponsible ways to write code. An example of the latter is a failure to properly acknowledge a software program's impact on human welfare by failing to respect basic goods such as personal security and psychological well-being and the right of privacy that protects these goods. In 2007, Facebook introduced a program called Beacon, described as "a new way to socially distribute information." Beacon allowed Facebook advertisers to track users across the internet and disclosed the users' purchases to his or her personal network of friends without their consent. Beacon could easily become a source of harm for Facebook users in certain circumstances. For example, maybe a Facebook user purchases an intimate item online, and when that purchase is revealed to her "friends" she is profoundly embarrassed and even suffers some psychological trauma. Facebook users balked at the functionality of Beacon, and the company had to shut down the program. Beacon was a dangerous piece of code that infringed privacy rights, especially given the asymmetries of knowledge between Facebook and its users. This code was legal and may even have been in conformity with evolving social norms, but it was not developed in a responsible manner, since it was inconsistent with both core human goods (such as personal security) and instrumental goods like autonomy. This code failed to take into account the fundamental human need for sovereignty over one's own life and lived experiences.[10]

Iron Cage or Gateway to Utopia?

Although most of us agree that some limits will need to be imposed on networked information technologies that pervade the home and workplace, there is legitimate skepticism about anyone's ability to control the ultimate evolution and effects of these technologies. Are our attempts to regulate cyberspace merely a chimera? Are we too trammeled by the forces of technology, or are we still capable of exercising sovereignty over the extensive reach of the technical infrastructure?

Some philosophers have long regarded technology as a dark and oppressive force that menaces our individuality and authenticity. These pessimistic determinists typically see technology as a powerful, independent force, largely out of our control. The French philosopher Jacques Ellul presents a disturbing vision of technology in his seminal work *The Technological Society*. His central argument is that *technique* has become a dominant and untranscendable human value. He defines technique as "*the totality of methods rationally arrived at and having absolute efficiency* (for a given stage of development) in *every* field of human activity."[11] According to Ellul, technique has

become an autonomous force that obeys its own laws. Modern technology has irreversibly shaped the way we live, work, and interact in this world, and it cannot be effectively tamed or resisted.

Ellul was not alone in advancing such a pessimistic outlook on technology. Max Weber coined the term “iron cage” to describe how technology locks us in to certain ways of being or patterns of behavior. And Martin Heidegger had little confidence that humanity could transcend the exploitative nature of modern technology. Technology is destiny, and we are trapped in the attitude of technicity (*die Technik*) that induces us to see all reality as a collection of objects to be manipulated. But is it really so that technology forces us into this “iron cage” so that we are more like its servants rather than its masters?

In contrast to the bleak outlook of Ellul and Heidegger, we find technology neutralists who argue that technology is a neutral force, completely dependent on human aims and objectives. According to this viewpoint, technologies are free of bias and do not promote one type of behavior over another. Technology is only a tool, and it does not compromise our human freedom or determine our destiny in any appreciable way; it is up to us whether this

powerful force is used for good or for questionable purposes.

Some go even further and embrace a sort of "technological utopianism" that regards certain technologies as making possible an ideal world with improved lifestyles and workplaces. This optimistic philosophy assumes that humanity can eradicate many of technology's adverse effects or social costs and manipulate this tool effectively to consistently improve the human condition.

The philosophy of technological neutralism (or, for that matter, utopianism) seems problematic for several reasons. We live in a technocratic society where technology affects how we see the world and conditions our choices with certain "givens" that are virtually impossible to fully overcome. Langdon Winner describes this as a process of reverse adaptation or "the adjustment of human ends to match the character of the available means."[12]

However, it is also an exaggeration to claim that computer and network technologies lock us into a virtual but inescapable iron cage. The middle ground between these extreme positions is *technological realism*, which holds that "although technology has a force of its own, it is not independent of political and social forces."[13]

Technological realism acknowledges that technology has reconfigured our political and social reality and reshaped the culture.

However, although technology determines to some degree how we live and work, we still have the capacity to redirect or subdue it when necessary. We have freedom to use technology poorly or to use it well and to subject technology of all stripes to moral assessment. Our human freedom is undoubtedly attenuated by technology's might and its atomizing tendencies, but it is not completely neutralized. We can still choose to implement systems and develop code in ways that protect fundamental human rights, such as autonomy or privacy.

Beyond any doubt, technology and its counterpart —instrumental rationality—are dominant forces in this society that exert enormous pressures on us to make choices and behave in certain ways. But as Charles Taylor points out, one can find throughout history pockets of concerted opposition to oppressive technologies. Further, the chances for such successful resistance are greatly enhanced when there is some common understanding about a particular threat such as the ecological crisis that occupied our attention during the 1970s. Perhaps the same common consciousness will emerge about the expanding

threat to personal privacy and become a catalyst for overcoming this technological dynamism. Although we should not be overly optimistic about our freedom and our capacity for resisting infatuation with new technology, we must recognize that we still have *some* degree of freedom in this world. Therefore, we agree with Taylor's assessment: "We are not, indeed, locked in. But there is a slope, an incline in things that is all too easy to slide down."[14]

We can avoid this slide and its accompanying perils only if we conscientiously adopt the moral point of view as we evaluate technology's capabilities and make decisions about its proper deployment. How can we characterize this moral point of view? According to Kenneth Goodpaster, it can be seen "as a mental and emotional standpoint from which all persons have a special dignity or worth, from which the Golden Rule derives its worth, and from which words like *ought* and *duty* derive their meaning."[15] This is quite consistent with our earlier claim that the fundamental moral imperative is the promotion of human flourishing, both in ourselves and in others.

Several distinct types of ethical reasoning have been associated with the moral point of view, and they provide us with the basic principles that serve as a moral "compass" for making normative judgments. Some of these theories ground moral judgment in human well-being or those goods basic to our fulfillment, while others defend the dignity of the human person through an emphasis on rights and duties. All of the principles reviewed here are worth our careful consideration, since they allow us to transcend the prejudices and

rationalizations of everyday life. They help us to engage in the critical analysis necessitated by the moral vexations of our commercial and personal interactions in cyberspace. Moral reflection at its best is dialectical, since it maneuvers between complex concrete situations and the principles that will inform our judgment about should be done.[16]

Utilitarianism

Classic utilitarianism, sometimes called "consequentialism," was developed by two British philosophers, Jeremy Bentham (1748–1832) and John Stuart Mill (1806–1873). According to this theory, the right course of action is to promote the general good. This general good can also be described in terms of "utility," and this principle of utility is the foundation of morality and the ultimate criterion of right and wrong. Utility refers to the positive benefits (or good) created by an action. According to Frankena, utilitarianism is the view that the ultimate standard of right and wrong is the *principle of utility*, "which says quite strictly that the moral end to be sought in all that we do is *the greatest possible balance of good over evil* (or the least possible balance of evil over good)." Thus, a moral agent should choose the action or policy that overall and in the long run produces the net best proportion of benefit to harm (however those terms are defined).[17]

It should be emphasized that utilitarianism is quite different from ethical egoism. The moral value of an action is not measured by the benefits or results achieved for a particular moral agent but by whether that action maximizes utility for all affected parties. With this in mind we might reformulate the moral principle of utilitarianism as

follows: persons ought to act in a way that promotes the maximum net expectable utility, that is, the greatest net benefits or the lowest net costs, for the broadest community affected by their actions.

On a practical level, utilitarianism requires us to make moral decisions by means of a rational, objective cost/benefit analysis. In most ethical dilemmas there are several possible alternatives or courses of action. Once one has sorted out the most viable and sensible alternatives, each of those alternatives is evaluated in terms of its costs and benefits (both direct and indirect). Based on this calculation, one chooses whatever option produces the greatest net expectable utility, that is, the greatest net benefits (or the lowest net costs) for the affected stakeholder community (e.g., employees and their families, customers, suppliers).

A concrete example illustrates how cost/benefit analysis might work. Let us assume that a corporation has to make a policy decision about random inspection of employees' email without their knowledge or consent. This might be done as a routine part of a performance review as a means of checking to make sure that workers are using email only for work-related purposes and are not involved in any untoward activities. In the United

States, this practice is perfectly legal, but some managers wonder if it is really the right thing to do; it seems to violate the privacy rights of employees. Rightness in the utilitarian ethical model is determined by consequences that become transparent in a cost/benefit analysis. In this case, the managers might face three options: email messages are not inspected on a routine basis and are kept confidential (unless some sort of malfeasance or criminal activity is suspected); email messages are inspected regularly by managers, but employees are informed of this policy and reminded of it every time they log in to the email system, so that there is no expectation of privacy; or email is regularly but surreptitiously perused by managers with employees uninformed of the company policy. Which of these alternatives promotes the general good, that is, produces the greatest net expectable utility?

TABLE 1-1 provides an idea of how this analysis might work out. It becomes clear from this exercise that it is difficult to objectively calculate the diffuse consequences of our actions or policies and to weigh them appropriately. And herein lies a major obstacle in using this approach. Nonetheless, there is value in performing this type of analysis; it induces us to consider the broad consequences of our actions and to take into account the social and

economic costs of implementing various technologies.

TABLE 1-1 Illustrative Cost/Benefit Analysis

	Costs	Benefits
Keep email confidential	Lack of control over employees; difficult to prevent misuses of email; email could be used for various personal reasons without company knowledge.	Maintains morale and an environment of trust and respect for workers; protects personal privacy rights.
Inspect email with employees informed of policy	Violates privacy rights; diminishes trust and impairs morale; workers are less likely to use email if communications are not confidential—instead they will rely on less efficient modes of communication.	Prevents misuse along with inappropriate comments about superiors and fellow workers via email; workers know the risks of misusing email; they are less likely to use email for personal purposes.
Inspect email surreptitiously	Same as option 2, but even more loss of trust and morale if company policy is uncovered.	Better chance to catch employees doing something wrong such as transmitting trade secrets; perfectly legal.

Although this theory does have certain strengths, it also has serious flaws. Depending on the context, utilitarianism could be used to justify the infliction of pain on a small number of individuals for the sake of the happiness or benefits of the majority. There are no intrinsically unjust or immoral acts for the utilitarian, and this poses a problem. What happens when human rights conflict with utility? Can those rights be suppressed on occasion for the general good? There is nothing in utilitarianism to prevent this from happening, as long as a cogent and objective case is made that the benefits of doing so exceed the costs. The primary problem then is that this theory lacks the proper sensitivity to the vital ideals of justice and human rights.

Moral Rights

Another mode of reasoning that exemplifies the moral point of view is rights-based analysis, which is sometimes referred to as contractarianism. It looks at moral issues not from the perspective of consequences but from the viewpoint of the human rights that may be at stake. A *right* is an entitlement or a claim to certain things or actions that impose an obligation or duty on others. For instance, the Fourth Amendment of the U.S. Constitution offers legal protection for the natural right to privacy and safeguards American citizens from unwarranted search and seizure in the privacy of their homes. In contrast to the utilitarian view, the consequences of an action are morally irrelevant for those who support a rights-based morality. Rights are unequivocally enjoyed by all human persons, and the rights of some minority group cannot be suspended or abolished even if that abolition will maximize social welfare.

An important distinction needs to be made between positive and negative rights. Possession of a *negative right* implies that one is free from external interference in one's affairs. Examples of negative rights include the right to free speech, the right to property, and the right to privacy. Because all citizens have a right to privacy in their homes, the state cannot interfere in their affairs by tapping

their phone calls unless it has demonstrated a strong probability that laws are being broken.

A *positive right,* on the other hand, implies a requirement that the holder of this right be provided with whatever one needs to pursue one's legitimate interests. The rights to medical care and education are examples of positive rights. In the United States, the right to health insurance funded by the government may still be a matter of debate, but the right to education is unequivocal. Therefore the state has a duty to educate children through the 12th grade. If everyone had a "right" to internet access, there would be a correlative duty on the part of the government (or others) to provide that access for those who could not afford it.

Rights have been philosophically grounded in several ways. According to social contract philosophers, such as Hobbes and Rousseau, rights have their origin in an implicit social contract between the individual and civil society. Individuals agree to such a contract to escape the state of nature and enter into organized civil society for the sake of their own security. Rights are one side of a *quid pro quo*—we are guaranteed certain rights (e.g., life, liberty, and the pursuit of happiness) in exchange for obeying the laws and regulations of civil society. Contemporary contractualists, such as John Rawls, clarify that this contract is not a

historical fact but a theoretical instrument for discerning the most rational principles to govern society. The question posed by the contractualist is this: what sort of social arrangement would people in the “original position” enter into if they seriously thought about their valid needs and desires? Rawls argues that people in that pre-political position would demand an extensive system of liberties in order to pursue their goals and fulfill their life’s plan, including “freedom of the person along with the right to hold personal property.”[18]

Other philosophers, such as John Locke, have argued that we have natural rights that are prior to the origin of civil society. Those rights, such as life and property, are grounded in our self-possession. According to Locke, “man, by being master of himself and having a right to his own person, and the actions or labor of it, had still in himself the great foundation of rights.” The chief end of entering into civil society is the protection of those rights. The natural law tradition also argues for natural rights, such as life and health, property and security, that are prior to the formation of civil society. The foundations of those rights, which give normative recognition to human equality, are those basic human goods identified by philosophers like Finnis. These rights arise

whenever there are moral principles based on those goods that compel us to act (or refrain from acting) in certain ways out of respect for the welfare and dignity of persons who are affected by our actions. Justice is the willingness to recognize the other's rights, by not depriving a person of his or her rights or, in some cases, by protecting that right from being deprived.[19]

The problem with most rights-based theories is that they do not provide adequate criteria for resolving practical disputes when rights are in conflict. For example, the use of strong encryption code protects privacy rights for smartphone users. In a famous case (see **Chapter 6**), Apple refused to cooperate with the FBI and break the encryption code of a terrorist's iPhone, even though national security and public safety were at stake. Apple claimed that it was protecting the privacy rights of its users. But when do physical security interests justify an infringement of privacy rights? Rights are inviolable but limited, and the challenge is to determine when they can be validly infringed.

Moral Duty

The next framework for consideration is not based on rights, but on duty. The moral philosophy of Immanuel Kant (1724–1804), which can be found in his short but difficult masterpiece on ethics, *Fundamental Principles of the Metaphysics of Morals,* is representative of this approach. It assumes that the moral point of view is best expressed by discerning and carrying out one's moral duty. Moral action, therefore, should be motivated by duty or obligation rather than the achievement of optimal results.

Kant believed that the consequences of an action are morally irrelevant: "An action performed from duty does not have its moral worth in the purpose which is to be achieved through it but in the maxim by which it is determined."[20] According to Kant, actions only have moral worth when they are done for the sake of duty. But what is our duty and how is it derived? In Kant's systematic philosophy our moral duty is simple: to follow the moral law which, like the laws of science or physics, must be rational. Also, as is the case for all rational laws, the moral law must be universal, because universality represents the common character of rationality and law. And this universal moral law is expressed as the categorical imperative: "I should never act except in such a way that I can also will

that my maxim should become a universal law."[21] The imperative is "categorical" because it does not allow for any exceptions.

A *maxim,* as referred to in Kant's categorical imperative, is an implied general principle or rule underlying a particular action. If, for example, I usually break my promises, then I act according to the private maxim that promise breaking is morally acceptable when it is in my best interests to do so. But can one take this maxim and transform it into a universal moral law? As a universal law this particular maxim would be expressed as follows: "It is permissible for everyone to break promises when it is in their best interests to do so." Such a law, however, is invalid because it entails both a pragmatic and a logical contradiction. There is a pragmatic (or practical) contradiction because the maxim is self-defeating if it is universalized. According to Korsgaard, "your action would become ineffectual for the achievement of your purpose if everyone (tried to) use it for that purpose."[22] Consider this example: An individual borrows some money from a friend and he promises to pay her back. However, he has no intention of keeping that promise. But this objective, that is, getting some money from her without repaying it, cannot be achieved by making a false promise in a world where this maxim has

been universalized. As Korsgaard puts it, “The efficacy of the false promise as a means of securing money depends on the fact that not everyone uses promises that way.”[23]

Universal promise breaking also implies a logical contradiction (such as a square circle); if everyone were to break their promises, the entire institution of promising would collapse; there would be no such thing as a “promise” because in such a climate anyone making a promise would lack credibility. A world of universalized promise breaking is inconceivable. Thus, in view of the contradictions involved in universalizing promise breaking, we have a perfect duty to keep all of our promises.

Kant strongly implies that *perfect duties,* that is, duties that we are always obliged to follow, such as telling the truth or keeping a promise, entail both a logical and pragmatic contradiction. Violations of imperfect duties, however, are only pragmatic contradictions. Korsgaard explains that “perfect duties of virtue arise because we must refrain from particular actions *against* humanity in our own person or that of another.”[24] *Imperfect duties,* on the other hand, are duties to develop one’s talents where the individual has the latitude to fulfill this duty using many different means.

Kant's categorical imperative is his ultimate ethical principle. It is the acid test of whether an action is right or wrong. According to Kant, then, any self-contradictory universalized maxims are morally forbidden. The categorical imperative functions as a guide, a "moral compass" that gives us a reliable way of determining a correct and consistent course of action. According to Norman Bowie, "the test of the categorical imperative becomes a principle of fair play—one of the essential features of fair play is that one should not make an exception of oneself."[25]

Also, from the categorical imperative we can derive other duties, such as the duty to keep contracts, to tell the truth, to avoid injury to others, and so forth. Kant would maintain that each of these duties is also categorical, admitting of no exceptions, because the maxim underlying such an exception cannot be universalized.

How might we apply Kant's theory to the mundane ethical problems that arise in cyberspace? Consider the issue of intellectual property. As Korsgaard observes, "property is a practice,"[26] and this practice arguably makes sense for both physical property and intellectual property. But a maxim that permitted stealing of such property would be self-defeating. That maxim would say, "It's acceptable for me to steal the intellectual

property validly owned by the creators or producers of that property." Such a universalized maxim, permitting everyone to take this intellectual property, is self-defeating precisely because it leads to the destruction of the entire "practice" of intellectual property protection. Because the maxim allowing an individual to freely appropriate another's intellectual property does not pass the universalization test, a moral agent is acting immorally when he or she engages in acts such as the unauthorized copying of a digital movie or music file.[27]

At the heart of Kant's ethical system is the notion that there are rational constraints on what we can do. We may want to engage in some action (such as downloading copyrighted files), but we are inconsistent and hence unethical unless we accept the implications of everyone doing the same thing. According to Kant, it is unethical to make arbitrary exceptions for ourselves. In the simplest terms, the categorical imperative suggests the following question: What if everybody did what you are doing?

Before concluding this discussion on Kant, it is worth taking note of his second formulation of the categorical imperative: "Act in such a way that you treat humanity, whether in your own person or in the person of another, always at the same time as

an end and never simply as a means."[28] For Kant as well as for other moralists (such as Finnis), the principle of humanity as an end in itself serves as a limiting condition of every person's freedom of action. We cannot exploit other human beings and treat them exclusively as a means to our ends or purposes. This could happen, for example, through actions that deceive one's fellow human beings or actions that force them to do things against their will. According to Korsgaard:

> According to [Kant's] Formula of Humanity, coercion and deception are the most fundamental forms of wrongdoing to others—the roots of all evil. Coercion and deception violate the conditions of possible assent, and all actions which depend for their nature and efficacy on their coercive or deceptive character are ones that others cannot assent to . . . Physical coercion treats someone's person as a tool; lying treats someone's reason as a tool.[29]

If we follow this categorical imperative, we will make sure that our projects and objectives do not supersede the worth of other human beings. This principle can also be summed up in the notion of *respect*. One way to express universal morality is in terms of the general principle of respect for other human beings who deserve that respect because of their dignity as free and rational persons.

One of the problems with Kant's moral philosophy is its rigidity. There are no exceptions to the moral laws derived from the absolute categorical imperative. Hence, lying is *always* wrong even though we can envision situations where telling a lie (e.g., to save a human life) is a reasonable and proper course of action. In cases such as this, there is a conflict of moral laws: the law to tell the truth and the law to save a life in jeopardy, and we have no alternative but to admit an exception to one of them. As A. C. Ewing points out:

> In cases where two laws conflict it is hard to see how we can rationally decide between them except by considering the goodness or badness of the consequences. However important it is to tell the truth and however evil to lie, there are surely cases where much greater evils can still be averted by a lie, and is lying wrong then?[30]

Ewing's argument that it is difficult to avoid an appeal to consequences when two moral laws collide has some plausibility, and it is not adequately resolved in Kant's ethical synthesis.

An alternative duty-based philosophy proposed by William D. Ross (1877–1940), a contemporary English philosopher, attempts to obviate the difficulties posed by Kant's inflexibility. Ross argues in his book *The Right and the Good* that we are obliged to follow several basic *prima facie*

duties that each of us can intuit through simple reflection. These duties are *prima facie* in the sense that they are conditional and not absolute. This means that under normal circumstances we must follow a particular duty, but in those unusual situations where duties conflict with one another, one duty may be overridden by another duty that is judged to be superior, at least under these specific circumstances. According to Ross, moral rules or principles are not categorical as they are for Kant, so they can have exceptions. Thus, a moral principle can be sacrificed or overridden, but only for another moral principle, not just for arbitrary, selfish, or even utilitarian reasons.[31]

According to Ross, the seven *prima facie* moral duties that are binding on all moral agents are the following:

1. One ought to keep promises and tell the truth (*fidelity*).
2. One ought to right the wrongs that one has inflicted on others (*reparation*).
3. One ought to distribute goods justly (*justice*).
4. One ought to improve the lot of others with respect to virtue, intelligence, and happiness (*beneficence*).

5. One ought to improve oneself with respect to virtue and intelligence (*self-improvement*).
6. One ought to exhibit gratitude when appropriate (*gratitude*).
7. One ought to avoid injury to others (*noninjury*).

Ross makes little effort to provide any substantial rationalization or theoretical grounding of these duties. We might just say that they are common rules of morality, obvious to all rational humans because they have the general effect of reducing harm or evil to others.

The Achilles' heel of Ross's theory can be isolated by examining two specific problems: (1) his list of duties seems arbitrary because it is not metaphysically or even philosophically grounded, and (2) the list seems incomplete—where, for example, is the duty not to steal property from another? It may be included under the duty to avoid injury to others, but that is not altogether clear. Moreover, is it really true that all human beings (even those in different cultures) simply "intuit" these same principles? Finally, *The Right and the Good* provides little help for resolving situations where two *prima facie* duties are in conflict. Ross offers few concrete criteria for

determining when one moral obligation is more urgent and therefore should override another obligation.

Despite these shortcomings, however, Ross's framework, as with the others we have considered, is not without some merit. A focus on one's moral duty (or even conflicting duties) in a particular situation is a worthy starting point for moral reasoning about some dilemma or quandary. Further, for many moral conundrums, a sincere and rational person can develop sound, objective reasons for determining which duty should take priority.

New Natural Law

The natural law tradition has been neglected in most books on business and computer ethics. Detractors claim that it is too “impractical” and too closely associated with the theistic philosophy of St. Thomas Aquinas. Natural law theory is valuable, however, because of its focus on human well-being and fulfillment along with specific principles that direct us toward basic human goods and away from their privation or impediment.[32]

The new natural law, developed by John Finnis and Germain Grisez, remains faithful to the broad lines of natural law theory found in the philosophy of Aquinas. But it also elaborates on that philosophy and makes some useful refinements. For Aquinas and the new natural law theorists the starting point of moral reflection is the first practical principle: “Good should be done and pursued, and evil avoided,” where good means what is intelligibly worthwhile. Free, rational agents pursue what is good for them, what perfects their nature and makes them better off. But what is the good? Recall Finnis’ set of basic human goods that contribute to human flourishing: life, health, and security; knowledge (including aesthetic appreciation); skillful performance at work and play (for its own sake); friendship; marriage and good family relationships; harmony with God; and

practical reasonableness. All of our rational choices ultimately point to one of these intrinsically valuable goods. For example, if someone asks Paul why he plays golf so much, he could answer that he enjoys the game or that he needs the exercise. The first answer points to the intelligible good of play for its own sake and the second to the good of health.

It is difficult to refute the thesis that these goods contribute to the good life, whatever one's culture or social order. Each one of us participates in these fundamental goods, though we may participate in some goods more than others. Practical reasonableness, which includes the value of authenticity, shapes a person's participation in these basic goods. And one requirement of practical reasonableness is that it is unreasonable to choose directly against any of these goods, either in ourselves or in other human persons. Right action, on the other hand, aims at achieving this set of goods that make the life of a human person worthwhile.[33]

But how do we get from these basic human goods to specific moral norms and human rights? Our practical reason grasps that each of these basic human goods is an aspect of human flourishing and that a good in which any person shares also fulfills other persons. Life and health are

fundamental goods not just for me but for anyone like me. Whenever one intentionally destroys, impedes, or damages one of these goods in a way that interferes with human flourishing, there is moral evil. Thus, we can stipulate the First Principle of Morality: *keep one's choices open to integral human fulfillment,* the fulfillment of all persons and communities.[34]

This principle, however, is too general and so we also need intermediate principles or "modes of responsibility." These modes include the "Golden Rule" ("Do to others as you would wish them to do to you") along with the imperative to avoid acting out of hostility or vengeance and never to choose evil as the means to a good end. The good or the end of my actions does not justify the use of unjust means that damage a basic good. According to this principle, for example, one could not justify telling a lie that damages the truth to preserve a friendship. In this case, one is exercising favoritism with regard to these goods, which are incommensurable and all deserving of the same respect.[35]

Specific moral norms can be deduced from those basic human goods with the help of these intermediate principles, such as the Golden Rule. For example, because human life is a basic human good, certain acts such as the taking of

innocent life are forbidden as a matter of natural law. Since no rational person would want to be deprived of his life, he should not deprive another innocent person of her life. Finnis states this natural law (or absolute moral norm) as follows: “Every act which is intended, whether as end or means, to kill an innocent human being and every act done by a private person which is intended to kill any human being” is prohibited.[36] And from the basic good of knowledge defined as justified belief, we can deduce norms that prohibit lying or deception.

These basic goods constitutive of human well-being and flourishing also serve as the foundation for our judgments about justice and human rights. Human rights flow from the principles of practical reason (such as the norm forbidding the taking of innocent life) that direct us to act or refrain from acting out of respect for the well-being and the dignity of other persons. These rights cannot be overridden by utilitarian considerations. Thus, given the direct or indirect harm caused to our well-being by the loss of privacy, it is intelligible to speak about a right against infringements of privacy, a right required by the demands of justice.[37]

Although the new natural law has tried to disengage itself from any metaphysical

underpinnings, some critics claim that it does not succeed. Can this set of human goods stand without an underlying metaphysical account of human nature? Finnis argues for only a thin connection between human nature and the basic human goods. Those goods merely “reflect” human nature to the extent they indicate “what is good for human beings with the nature they have.”[38] But opponents fault the new natural law philosophy because this theory is not sufficiently grounded in the natural order. Nonetheless, this theory’s main advantage is its comprehensiveness: it focuses on human goods intrinsic to our fulfillment as well as the defense of a person’s dignity through moral rights that protect those goods from being deprived.[39]

Postscript on Moral Theory

As we have seen, none of these moral theories are without flaws or contradictions, but they do represent viable avenues for reasoning about moral issues, especially when those issues go beyond the level of moral common sense. They also have certain elements in common: a willingness to give weight to others' interests as well as one's own, along with a repudiation of egoistic moral reasoning. Most give some salience to moral and legal rights, and recognize that persons are to be respected for their own sake.

Before concluding this material on ethical theories, we can summarize how they can be applied to some of the moral quandaries that arise in the electronic frontier of cyberspace. **TABLE 1-2** provides a concise framework for putting these four basic theories into action.

TABLE 1-2 Summary of Ethical Frameworks

Theory Type	Operative Questions
Consequentialism/utilitarianism	Which action or policy generates the best overall consequences or the greatest net expectable utility for all affected parties?
Duty-based morality	Can the maxim underlying the course of action being considered be universalized? Is the principle of fair play being violated? If there appear to be conflicting duties, which is the stronger duty?
Rights-based morality	Which action or policy best protects the human and legal rights of the individuals involved?
New natural law	Does the proposed action or policy promote the well-being of persons and the communities they form? Does it impede, damage, or destroy any of the basic human goods?

Floridi’s Macroethics

Before concluding this discussion, it is worth considering a new high-level theory specifically designed to accommodate our contemporary Information Age, which is so irreversibly centered on digital information. Despite the breadth and depth of traditional ethical theories, some contemporary philosophers believe that they are inadequate to address the complex moral problems of our networked information society. One such thinker is Luciano Floridi, who finds fault with these traditional approaches because they are too anthropocentric or too preoccupied with how personal actions affect other persons. Those theories pay little attention to how actions impact the broader biological, social, and informational environment. As a complement to those theories, Floridi proposes his more ecological macroethics, or information ethics (IE).

Floridi’s ethical theory has three major characteristics: it is ontocentric, ecological, and patient-oriented. First, what does he mean by “ontocentric”? At the core of Floridi’s theory is the thesis that all entities in the universe, both animate and inanimate, are informational objects or “clusters of data,” and this common feature

endows them with some moral value. This category of beings deserving moral consideration includes even digital objects that exist only in cyberspace or in a database because they, too, are obviously informational objects. As a result, ethical discourse and reasoning must take into account the moral status of all entities in the infosphere. Floridi explains that according to IE, "even ideal, intangible, or intellectual objects can have a minimal degree of moral value."[40]

Although biocentrists maintain that we should not needlessly destroy or harm any living being, the ontocentrist espouses the belief that no being or informational object should be damaged or destroyed by the alteration of that being's data structure without sufficient reason. Being, therefore, is more fundamental than life. According to Floridi, all beings have the Spinozian right to persist in being and a "constructionist right to flourish."[41] Of course, the moral worth of certain informational objects is minimal and "overrideable," but even these objects still warrant some degree of moral consideration. Ontocentrism, Florid maintains, is the only authentic ecology because of its sensitivity to the entire infosphere.

IE is a "patient-oriented" theory because it is concerned with what qualifies as a moral patient,

that is, an object worthy of moral consideration. Because all information objects *qua* information objects have intrinsic value, they qualify as moral patients, worthy of some degree of moral worth. In this moral framework, evil is equated with entropy, which refers to any kind of "disruption, corruption, pollution, and depletion of informational objects."[42] Floridi's chief concern is the welfare of the whole infosphere. IE is a macroethics precisely because of its interest in the entire infosphere and the entropy or impoverishment of being that could happen to any entity that occupies this environment.

Floridi's theory is also concerned with the theme of moral agency, and once again he departs from the anthropocentric assumptions of traditional ethical theory. Floridi broadens the class of moral agents to include robots, software bots, and other information technology (IT) systems. He defines the moral agent as an interactive, autonomous, and adaptable transition system capable of performing "morally qualifiable" actions, that is, actions that can cause good or evil. A transition system is one that changes its states, and this system is interactive when it acts upon and is affected by the environment. That system is autonomous when it can change its state without direct response to interaction, and it is adaptable

when those interactions change the transition rules. Given these criteria, we can reasonably conclude that artificial agents, such as robots, have some degree of moral agency. Floridi concedes that although artificial moral agents occupying the infosphere, such as robots and corporations, can be held morally accountable, they lack moral responsibility for their actions. In the infosphere, however, we must transition from a responsibility-oriented ethics based on punishment and reward to an ethics based on "accountability and censure."[43]

In this text we only tangentially explore the role of artifacts in cyberspace such as surveillance tools and software bots that collect information for search engines and other data aggregators. The reader might ponder whether these entities have any sort of artificial moral agency, if considered from Floridi's nonanthropocentric perspective. Also, as these artifacts become more sophisticated and "intelligent," the debate about their moral status will surely intensify.

As with the other theories we have considered, thoughtful critics point to certain shortcomings. They question the premises of ontocentrism, which assumes that every being, including a rock or a piece of spam email, has some degree of moral worth. Others argue that this abstract theory is not

as useful or broadly applicable as utilitarianism or rights-based approaches to ethics. Floridi insists that IE is not meant as a substitute for traditional ethics but as a supplement. He admits, however, that we need “an ethical framework that can treat the infosphere as a new environment worth the moral attention and care of the human inforgs inhabiting it.”[44]

Normative Principles

Those who find ethical theory too abstract can turn to an approach known as *principlism.* It is commonly used in biomedical ethics and has become popularized through the work of Beauchamp and Childress.[45] These moral principles are derived from and are compatible with all of the moral theories articulated here. They constitute *prima facie* duties that are always in force but may conflict on occasion. The four principles proposed by Beauchamp and Childress are autonomy, nonmaleficence, beneficence, and justice. Those who advocate this approach also prescribe certain "prudential requirements" that determine when one *prima facie* principle should be given more weight than another. These include "being sure that there is a realistic prospect of achieving the moral objective one has chosen to honor; no alternative course of action is possible that would honor both conflicting obligations; and we minimize the effects of infringing on the prima facie duty."[46] A brief sketch of these four principles follows.

Autonomy

Kant and other philosophers have consistently argued that a defining element of personhood is one's capacity to be autonomous or self-determining. According to Gary Doppelt, "the Kantian conception of personhood ties the moral identity of persons to the supreme value of their rational capacities for normative self-determination."[47] All rational persons have two key moral powers or capacities: they possess the ability to develop and revise a rational plan to pursue their conception of the good life, and they possess the capacity to respect this same capacity of self-determination in others. Thus, autonomy is not only a necessary condition of moral responsibility, it is also through the exercise of autonomy that individuals shape their destiny according to their notion of the best sort of life worth living. When someone is deprived of their autonomy, their plans are interfered with and they are not treated with the respect they deserve. Of course, respect for autonomy must be balanced against other moral considerations and claims.

Nonmaleficence

The principle of nonmaleficence can best be summarized in the moral injunction: “Above all, do no harm.” According to this core principle, one ought to avoid unnecessary harm or injury to others whenever possible. This negative injunction against doing injury to others is sometimes called the “moral minimum.” However one may choose to develop a moral code of conduct, this injunction must be given a preeminent status. Most moral systems go well beyond this minimum requirement, as we have seen in the theories already discussed, but that does not detract from the central importance of this principle. According to Jon Gunneman and his coauthors,

> We know of no societies, from the literature of anthropology or comparative ethics, whose moral codes do not contain some injunction against harming others. The specific notion of *harm* or *social injury* may vary, as well as the mode of correction and restitution but the injunctions are present.[48]

Beneficence

This is a positive duty and has been formulated in many ways. In the simplest terms it means that we should act in such a way that we advance the welfare of other people when we are able to do so. In other words, we have a duty to help others. But what does this really mean? When am I duty bound to help another person or even an institution? It is obvious that we cannot help everyone or intervene in every situation when someone is in need. Hence, some criteria are necessary for determining when such a moral obligation arises. In general, it can be argued that we have a duty to help others under the following conditions:

1. The need is serious or urgent.
2. We have knowledge or awareness of the situation.
3. We have the capability to provide assistance (“ought assumes can” is the operative principle).

If, for instance, one is an Olympic swimmer and sees someone drowning at the beach, one has an obligation to attempt a rescue of that person, especially if this is the only recourse and there is little risk to one’s own life. This principle has some relevance when we evaluate society’s

questionable duty of beneficence to provide universal internet service.

Justice

Although theories of justice have their differences, most have a common adherence to this basic formal principle: “Similar cases ought to be treated in similar ways.” Above all else, justice requires fair treatment and impartiality. This is a formal procedural principle of justice and needs to be supplemented by the criteria for determining “similar” cases. This leads into theories of distributive justice, which attempt to formulate an underlying principle for how we should distribute the benefits and burdens of social life. Some theories emphasize equality, that is, all goods should be distributed equally. John Rawls, for example, adopts an egalitarian approach, though he does argue that an unequal distribution of goods is acceptable when it works for the advantage of everyone, especially the least advantaged (the difference principle).[49] Other theories emphasize contribution and effort as formulated in this maxim: “Benefits or resources should be distributed according to the contribution each individual makes to the furtherance of society’s goals.” And still another theory of justice that has typically been associated with socialism argues for justice based on need: “From each according to his ability, to each according to his needs.”[50]

Our purpose here is not to defend one of these theories against the other, but to illustrate that moral judgments should be based in part on the formal principle of justice and take into account some standard regarding how the benefits and burdens should be fairly distributed within a group or society at large.

There is no reason that these formal moral principles cannot be applied to some of the controversial problems that we consider in this text. They are certainly general enough to have applicability in the field of computer and internet ethics as well as bioethics. A person who makes choices and develops policies attentive to the core human goods and to these more practical principles that generally promote those goods would surely be acting with the care and prudence that is consistent with the moral point of view.

DISCUSSION QUESTIONS

1. Do you agree with the philosophy of technological realism?
2. Explain the basic elements of Lessig's framework. What does he mean when he says that in cyberspace "the code is the law"?
3. Explain and critically analyze the essentials of Kant's moral theory.
4. In your estimation, which of the moral frameworks presented in this chapter has the most promise for dealing with the moral dilemmas associated with networked information technologies?

REFERENCES

1. Brian McCullough, *How the Internet Happened: From Netscape to the iPhone* (New York: W.W. Norton, 2018), 319–20.
2. Aristotle, *Nicomachean Ethics*, trans. Martin Ostwald (Indianapolis: Bobbs-Merrill, 1962) I, 3: 1094b. See also David Oderberg, *Moral Theory* (Oxford: Blackwell, 2000), 3–5.
3. Larry Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), 236. See also 85-108.
4. Philippa Foot, "Moral Relativism" (1979 Lindley Lecture, Department of Philosophy, University of Kansas). See also Oderberg, 20.
5. Larry Lessig, "The Laws of Cyberspace," **http://cyberlaw.stanford.edu/lessig**.
6. Larry Lessig, "Tyranny in the Infrastructure," *Wired* 5.07 (1997): 96.
7. Jim Moor, "Just Consequentialism and Computing," in *Readings in Cyberethics*, eds. Richard Spinello and Herman Tavani (Sudbury, MA: Jones and Bartlett Publishers, 2001), 100.

8. John Finnis, “Liberalism and Natural Law Theory,” *Mercer Law Review* 45 (1994): 687–91. See also John Finnis, *Reason in Action* (Oxford: Oxford University Press, 2011), 210.
9. John Finnis, *Fundamentals of Ethics* (Washington, DC: Georgetown University Press, 1983), 125. See also Robert George, “Natural Law,” *American Journal of Jurisprudence* 52 (2007): 55.
10. Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: Public Affairs, 2019), 47–48, 521.
11. Jacques Ellul, *The Technological Society*, trans. John Wilkinson (New York: Vintage Books, 1964), xxv.
12. Langdon Winner, *Autonomous Technology: Technics-out-of-Control as a Theme of Political Thought* (Cambridge, MA: MIT Press, 1977), 229.
13. Priscilla Regan, *Legislating Privacy* (Chapel Hill: University of North Carolina Press, 1995), 12.
14. Charles Taylor, *The Ethics of Authenticity* (Cambridge, MA: Harvard University Press, 1991), 101.
15. Kenneth Goodpaster, “Some Avenues for Ethical Analysis in Management,” in *Policies*

and Persons, eds. John Matthews et al. (New York: McGraw-Hill, 1985), 495.

16. Michael Sandel, *Justice* (New York: Farrar, Straus & Giroux, 2009), 29. See also Germain Grisez, "A Contemporary Natural Law Ethic," in *Normative Ethics and Objective Reason,* ed. George F. McLean (2001). **http://www.mccc.edu/~howarthk/Grisez_Ethical_Theory.docx**.

17. William Frankena, *Ethics* (Englewood Cliffs, NJ: Prentice-Hall, 1963), 29. See also Robert George, *Conscience and Its Enemies* (Wilmington, DW: ISI Books, 2013), 88.

18. John Rawls, *A Theory of Justice* (Cambridge, MA: Harvard University Press, 1971), 61. See also Oderberg, 63–65.

19. John Locke, *Two Treatises of Government*, ed. Peter Lasslett (Cambridge, UK: Cambridge University Press, 1988), II, v. 44. See also S. Adam Seagrave, *The Foundations of Natural Morality* (Chicago, IL: University of Chicago Press, 2014), 34–35, John Finnis, *Philosophy of Law* (Oxford: Oxford University Press, 2011), 116–17, and George, *Conscience and Its Enemies* 77.

20. Immanuel Kant, *Foundations of the Metaphysics of Morals* (Indianapolis, IN:

Bobbs-Merrill, 1959), 16.

21. Ibid., 18.

22. Christine Korsgaard, *Creating the Kingdom of Ends* (Cambridge, UK: Cambridge University Press, 1996), 78.

23. Ibid., 92.

24. Ibid., 21.

25. Norman Bowie, *Business Ethics: A Kantian Perspective* (Oxford: Blackwell Publishers, 1999), 17.

26. See Korsgaard, *Creating the Kingdom of Ends*, 97.

27. Richard A. Spinello, "Beyond Copyright: A Moral Investigation of Intellectual Property Protection in Cyberspace," in *The Impact of the Internet on Our Moral Lives*, ed. Robert J. Cavalier (Albany, NY: SUNY Press, 2005), 27–48.

28. Kant, *Foundations of the Metaphysics of Morals*, 36.

29. Korsgaard, 194.

30. Alfred Cyril Ewing, *Ethics* (New York: Free Press, 1965), 58.

31. William D. Ross, *The Right and the Good* (Oxford: Oxford University Press, 1930).

32. Robert George, "Natural Law, God, and Human Dignity," in *Natural Law*

Jurisprudence, eds. George Duke and Robert George (Cambridge, UK: Cambridge University Press, 2017), 71.

33. John Finnis, *Natural Law and Natural Rights* (New York: Oxford University Press, 1980), 225. See also Alasdair Macintyre, *Ethics in the Conflicts of Modernity* (Cambridge, UK: Cambridge University Press, 2016), 222, 291.
34. Grisez, "A Contemporary Natural Law Ethic."
35. Ibid.
36. John Finnis, *Aquinas* (Oxford: Oxford University Press, 1998), 141.
37. George, "Natural Law, God, and Human Dignity," 60–61 and "Natural Law," 61.
38. Finnis, *Natural Law and Natural Rights*, 34.
39. Jonathan Crowe, "Metaphysical Foundations of Natural Law Theories," in *Natural Law Jurisprudence*, 104.
40. Luciano Floridi, "Information Ethics," in *The Cambridge Handbook of Information and Computer Ethics,* ed. Luciano Floridi (Cambridge, UK: Cambridge University Press, 2010), 85.
41. Ibid., 84.
42. Ibid.
43. Ibid., 88.

44. Luciano Floridi, “Ethics after the Revolution,” in *The Cambridge Handbook of Information and Computer Ethics*, ed. Luciano Floridi (Cambridge, UK: Cambridge University Press, 2010), 19.

45. Thomas Beauchamp and J. F. Childress, *Principles of Biomedical Ethics*, 4th ed. (New York: Oxford University Press, 1994).

46. Mark Kaczeski, “Casuistry and the Four Principles Approach,” in *Encyclopedia of Applied Ethics,* vol. 1, ed. Ruth Chadwick (San Diego, CA: Academic Press, 1998), 430.

47. Gary Doppelt, “Beyond Liberalism and Communitarianism: A Critical Theory of Social Justice,” *Philosophy and Social Criticism* 14 (1988): 278.

48. Jon Gunneman, *The Ethical Investor* (New Haven, CT: Yale University Press, 1972), 20.

49. Rawls, *A Theory of Justice*, 85–90.

50. Karl Marx, *Critique of the Gotha Program* (London: Lawrence and Werhart, Ltd., 1938), 14.

ADDITIONAL RESOURCES

Baase, Sara. *A Gift of Fire*: *Social, Legal and Ethical Issues in Computing.* 3rd ed. Upper Saddle River, NJ: Prentice-Hall, 2013.

Bynum, Terrell Ward. *Information Ethics: An Introduction*. Cambridge, MA: Blackwell, 1998.

Bynum, Terrell Ward, and Simon Rogerson. *Computer Ethics and Professional Responsibility*. London: Blackwell, 2002.

Cavalier, Robert, ed. *The Impact of the Internet on Our Moral Lives*. Albany, NY: SUNY Press, 2005.

Collste, Goran, ed. *Ethics in the Age of Information Technology*. Linkoping, Sweden: Linkopings Universitet Centre for Applied Ethics, 2000.

Edgar, Stacey. *Morality and Machines.* 2nd ed. Sudbury, MA: Jones and Bartlett Publishers, 2003.

Finnis, John. *Natural Law and Natural Rights*. New York: Oxford University Press, 1980.

Floridi, Luciano, ed. *The Cambridge Handbook of Information and Computer Ethics*. Cambridge, UK: Cambridge University Press, 2010.

Floridi, Luciano. *Philosophy and Computing: An Introduction*. London: Routledge, 1999.

Hester, D. Micah, and Paul Ford, eds. *Computers and Ethics in the Cyberage*. Upper Saddle River, NJ: Prentice-Hall, 2001.

Himma, Kenneth, and Herman Tavani, eds. *The Handbook of Information and Computer Ethics*. Hoboken, NJ: Wiley, 2008.

Johnson, Deborah. *Computer Ethics.* 4th ed. Upper Saddle River, NJ: Prentice-Hall, 2009.

Lessig, Larry. *Code and Other Laws of Cyberspace.* New York: Basic Books, 1999.

Macintyre, Alasdair. *Ethics in the Conflicts of Modernity.* Cambridge, UK: Cambridge University Press, 2016.

Moore, Adam, ed. *Information Ethics*. Seattle, WA: University of Washington Press, 2005.

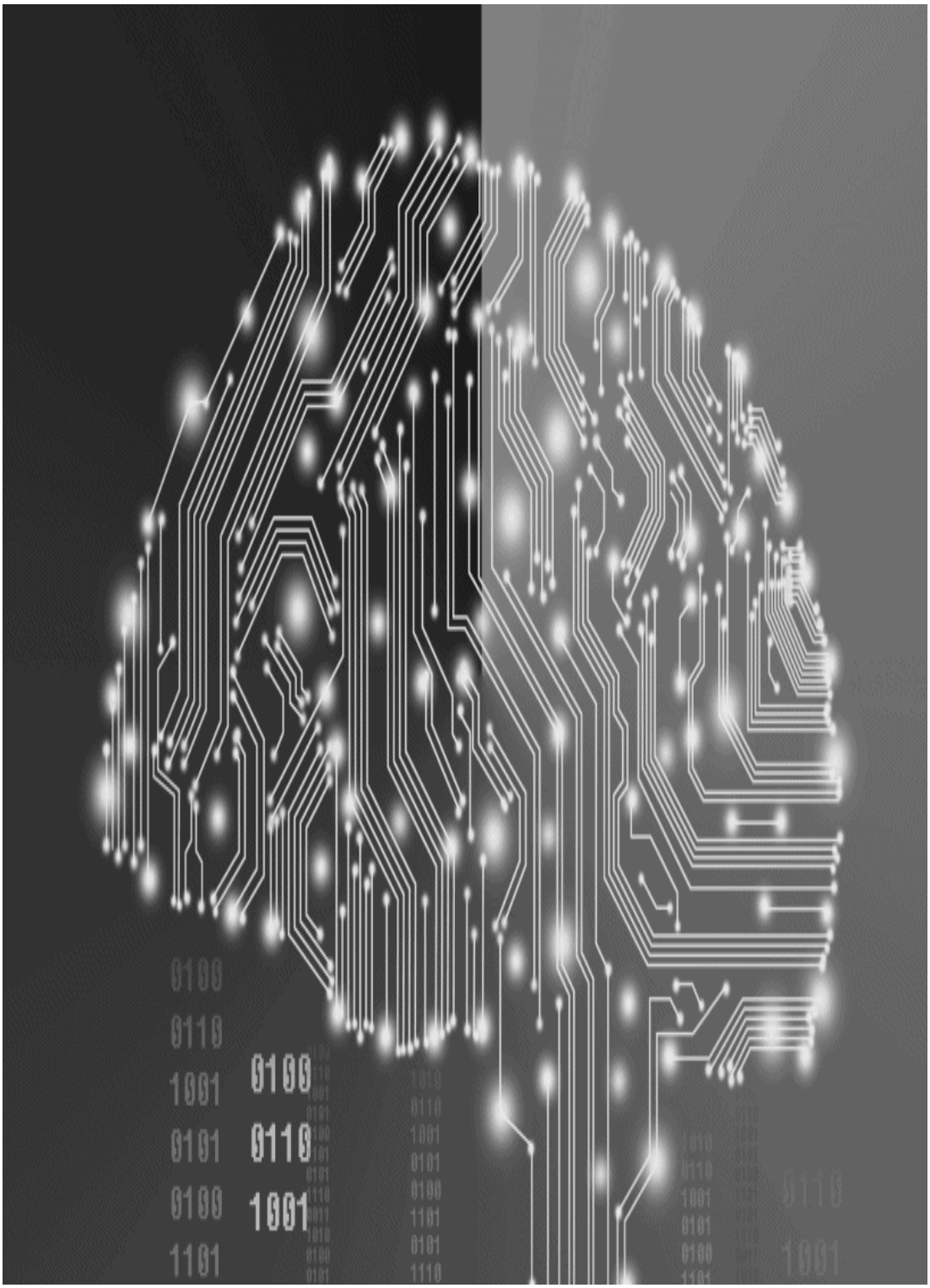
Oderberg, David. *Moral Theory*. Oxford, UK: Blackwell, 2000.

Sandel, Michael. *Justice.* New York: Farrar, Straus & Giroux, 2009.

Spinello, Richard, and Herman Tavani, eds. *Readings in Cyberethics.* 2nd ed. Sudbury, MA: Jones and Bartlett Publishers, 2004.

Tavani, Herman. *Ethics and Technology: Controversies, Questions and Strategies for Ethical Computing.* New York: Wiley, 2012.

Tavani, Herman. “The State of Computer Ethics as a Philosophical Field of Inquiry.” *Ethics and Information Technology* 3, no. 2 (2001): 97–108.



CHAPTER 2

Information and Power: Regulating and Governing Networked Technologies

During the 2016 U.S. presidential election internet users were exposed to an unprecedented level of disinformation, sensational news stories that had no basis in fact. There were bogus claims that presidential candidate Jeb Bush, brother of former President George W. Bush, had close Nazi ties. One news story claimed that President Obama had signed a law allowing immigrants with leprosy and other contagious diseases into the United States. During the election, the *Christian Times* treated its readers to this incredible headline: “Tens of Thousands of Fraudulent Clinton Votes Found in Ohio Warehouse.” But, as the *New York Times* reported, from its headline to the accompanying photograph, this was simply a “fake news masterpiece.” There seemed to be a profound epistemic crisis in cyberspace, with social media users asserting as true and credible what was in fact false or misleading.[1]

In addition to this flow of disinformation, sometimes aided by the cloak of anonymity, terrorists still use social media to encourage new recruits to their cause or to propagate their venomous messages. Citizens of New Zealand were justly outraged when they found out that a gunman who committed a massacre at two mosques in the city of Christchurch had distributed his hateful manifesto online. He

also streamed part of the mass shootings on his Facebook page.[2]

Perhaps these developments do not augur well for the future of ubiquitous networked technologies. But from its earliest origins a free-wheeling spirit has dominated the rules of discourse in cyberspace where user-generated content has been subject to few restrictions. Hence one of the most formidable issues faced by public policy makers and internet companies is how to impose some limits on this free and unencumbered flow of information. How can they restrict fake news or misinformation, and stop the exploitation of these technologies by infamous terrorist groups like ISIS?

The debates over “fake news” or the glamorization of terrorism on the internet reflect deeper questions about jurisdiction and the effectiveness of internet controls. Responsible governments can only do so much when it comes to terrorist recruiting through social media websites. It is also impossible for host sites to promptly shut down all extremist speech, but whether social media companies make adequate efforts is debatable. Although the internet’s anarchy and lack of structure have led to these and other excesses, many people continue to favor a libertarian spirit and loose controls. Some political activists still idealize the internet as an authentic social and intellectual commons independent of government authority, while others are far more skeptical.

Before plunging into a discussion of these complex matters, it is instructive to review the history and technology of the internet, and so we devote a portion of this chapter to that purpose. It is important to understand the architectures of the internet to appreciate the various possibilities for self-

regulation and government intervention. This overview includes a cursory treatment of the World Wide Web, the proliferation of social networking websites, and the expanding role for internet gatekeepers. It is also instructive at this point to consider the separate but related issue of governance, that is, the managing of mundane tasks such as assignment of domain names. This process, too, has triggered ethical controversies that are worthy of consideration.

This discussion sets the stage for a more in-depth treatment of speech, property, privacy, and security in the remaining chapters. For each of these broad issues, it is necessary to evaluate how underlying technologies change our ability to establish and enforce policy.

The Early History of the Internet

This summary of the internet's creation is not a mere indulgence in nostalgia. We investigate the past to understand the present. By looking at the internet's technological evolution, we can better appreciate the contours of its present architecture and the contingency of that architecture. We might also be able to uncover some clues about its future.

The origin of the internet's basic architecture can be traced back to the search for a "survivable communications" system. During the late 1950s, the U.S. Department of Defense (DOD) was concerned about the need for a failure-resistant communications method. In 1961, Paul Baran developed such a method, which has become known as *packet switching*. Baran admits that "the origin of packet switching itself is very much Cold War."[3] Package switching (originally called "message switching") works by breaking up a message into fixed-sized units or "packages"; each package is "labeled with its origin and destination and is then passed from node to node through the network."[4] This technology was also being separately developed by Donald Davies, a British expert on computer security, who was the first to

use the term “packet” in reference to data communications. Davies also built an experimental packet-switching network in the mid-1960s.

The first large-scale packet-switching network that was developed based on the insights of Baran and Davies was the work of the Advanced Research Projects Agency (ARPA), a research agency of the DOD, which financed high-tech research. In the late 1960s, the DOD provided generous grants to universities and corporations to establish a communications network between major research centers in the United States, including universities such as MIT and Stanford. It recruited Lawrence Roberts of MIT’s Lincoln Laboratory to oversee the construction of the ARPANET, the first incarnation of what is now known as the internet.

The basic infrastructure of the ARPANET consisted of several time-sharing host computers, packet-switching interface message processors (IMPs), and leased telephone lines. The host computers were already in place at the universities and research centers that would be part of the network; AT&T provided the telephone lines. The IMPs were needed to perform key network functions, such as sending and receiving data, error checking, and message routing. The responsibility for building these systems was delegated to Bolt, Beranek and Newman (BBN), a

research and consulting firm in Cambridge, Massachusetts.

By the end of 1971, the primitive ARPANET was up and running. Its primary goal was supposed to be resource sharing, that is, enabling connected sites to share hardware processing power, software, and data. But the network's users soon discovered another function: electronic mail. Instead of using the network primarily to leverage remote hardware resources, users began sending huge volumes of email. As a result, this popular application soon began to dominate traffic on this fledgling network. According to Abbate, "Network users challenged the initial assumptions, voting with their packets by sending a huge volume of electronic mail but making relatively little use of remote hardware and software. Through grassroots innovations and thousands of individual choices, the old idea of resource sharing that had propelled the ARPANET project forward was gradually replaced by the idea of the network as a means of bringing people together."[5]

In the early 1980s, this system was subdivided into two networks, the ARPANET and Milnet. Furthermore, connections were developed so that users could communicate between the two networks. The interaction between these networks came to be known as the internet. The term

“internet” was actually first used in a research paper written by Cerf and Kahn in 1974; that paper described a “network of networks” that would eventually link together computers all over the world. In the late 1980s, the National Science Foundation Network (NSFNET), which relied on five supercomputers to link university and government researchers from across the world, replaced the ARPANET. The NSFNET began to encompass many other lower level networks such as those developed by academic institutions, and gradually the internet as we know it today, a maze of interconnected networks, was born.

In these early days the federal government generously subsidized the internet, and as a consequence there were restrictions on any commercial use. The internet was the exclusive domain of government researchers, scientists, university professors, and others who used it primarily to share their research findings or communicate other academic information.

However, the NSF no longer subsidizes the internet, which has assumed a strong commercial character during the last three decades. During the early 1990s the internet quickly became available to corporate users, and the first email providers such as MCI and Compuserve opened up email gateways. By 1993, 29% of the host computers

connected to the internet belonged to corporations. Commercial and private sector use now accounts for the vast majority of all internet traffic. Management of the network has been transferred to private telecommunications carriers that manage the backbone, that is, the large physical networks that interconnect. Thus, the network's vitality depends on the cooperation and goodwill of these telecom providers.

The global diffusion of internet usage during this period has been an extraordinary phenomenon. In 1983 there were a mere 500 host computers (computers with unique internet protocol addresses) connected to the internet. In 2000 there were 360 million internet users. By 2019, the number of active internet users worldwide had grown to 4.4 billion, approximately 56% of the population.[6] Although the rapid development of the global internet has been extraordinary, there is still a disparity between developed and emerging economies. Africa still lags far behind the rest of the world in internet usage. However, in some developing countries, internet use is expanding rapidly. In Latin America, there were fewer than 20 million internet users in 2000, but that number increased to 438 million by 2018, about 55% of the total population.[7] Of course, those who use the internet have multiple connected devices, and

some estimate that there will be 50 billion connected devices by 2020.[8]

This global connectivity provided by the internet is perhaps its most attractive feature. It brings together millions of people and thousands of organizations all over the world and has helped to achieve what the *Economist* calls “the death of distance,” that is, the overcoming of geographic proximity as a barrier for conducting business.

The Internet's Architecture

How does this all work? There is actually little physical substance to the internet. There are a few dedicated computers or servers at key connection junctures, but "like a parasite, the internet uses the multi-billion dollar telephone network as its hosts and lets them carry most of the cost."[9] Data are fluidly transferred over this network by means of a network protocol called TCP/IP. The TCP/IP protocol allows for complete interoperability on the internet so that computers can communicate with one another even if they have different operating systems or applications software. TCP/IP therefore makes the network virtually transparent to end users no matter what system they are using, and it allows the internet to function as a single, unified network.

TCP/IP consist of two elements: the IP or Internet Protocol, which establishes a unique numeric address (four numbers in the form **nnn.nnn.nnn.nnn** ranging from 0 to 255) for each system connected to the internet. IP is a means of labeling data so that they can be sent to the proper destination in the most efficient way possible. If a user connects to the internet through an internet service provider (ISP), that user is normally

assigned a temporary IP address, but users who connect from a local area network (LAN) in their organizations are more likely to have a permanent IP address. In 2011, the internet ran out of numbers so the transition began to a revised system based on six numbers (IPv6) instead of four (IPv4).

While IP is responsible for the routing and fragmentation of data, TCP, or Transmission Control Protocol, enables reliable network communication over the internet by regulating the flow of information. Thanks to the IP protocol, data are broken up into pieces called “packets,” with the first part of each packet containing the address where it should go. The packets are then sent to their destination by a system of routers, that is, servers on the internet that keep track of internet addresses. These packets can take completely different routes to reach their goal. Once all the packets arrive, the message or data will be reconstructed, based on the sequence numbers in the headers to each packet, and redirected to the appropriate application. The TCP protocol works with IP to ensure that the data arrives correctly and in one piece at its proper destination.

The internet’s physical infrastructure is composed of many large, interconnected networks that are known as network service providers (NSPs). NSPs

include IBM, Sprint Net, and PSINet, as well as several others. According to Hafner, these backbone providers “adhere to what are known as peering arrangements, which are essentially agreements to exchange traffic at no charge.”[10] Each NSP connects to three network access points, and at those points packet traffic may be transferred from one NSP backbone to another. NSPs also sell bandwidth to smaller network providers and to ISPs.

Routers, also known as “packet switches,” perform much of the work in getting data transmitted over the Net to its ultimate destination. When a packet arrives at a router, the router looks at the IP address and checks the routing table, and if the table contains the network included in the IP address, the message is sent to that network. If not, the message is sent along on a default route (usually to the next router in the backbone hierarchy). If the address is in another NSP, the router connected to the NSP backbone sends the message to the correct backbone, where it is sent along by other routers until it reaches the correct address.[11]

As we survey the internet’s technical and social evolution, the distinctive features of its network architecture should be apparent. Perhaps the internet’s most notable characteristic is its

openness; thanks to an open-ended network architecture, the internet has supported an extraordinary level of innovation: email, blogs, instant messaging, digital music and movie files, social media apps—these are just some of the many applications technology platforms have enabled. According to Castells, “the openness of the internet’s architecture was the source of its main strength: its self-evolving development, as users became producers of the technology and shapers of the whole network.”[12]

Second, the internet is *asynchronous.* Unlike telephone communication, there is no need for coordination between the sender and recipient of a message. An email message, for example, can be sent to a mailbox that can be accessed at any time by its owner. Third, the internet permits a *many-to-many format of communications*:[13] many users can interact with many other users through electronic mail, texting, blogs, websites, and other vehicles. Unlike traditional media such as newspapers, the Net is interactive; users can speak back. Fourth, the internet is a *distributed* network instead of a centralized one, whereby data can take any number of routes to their final destination. There is no center to the internet, that is, there is no central server or single controlling authority, because information can travel from one

location to another without being transmitted through a central hub. This gives users more control over the flow of information. Because it is a decentralized, packet-based network, it is more difficult to censor that information. Also, this resilient design makes the internet's structure more durable. As Hafner points out, "that deceptively simple [packet switching] principle has, time and again, saved the network from failure."[14] When a train fire in Baltimore once damaged a critical fiber optic loop, internet data found another route and easily circumvented the problem. Finally, the internet is highly *scalable*, that is, it is not directly affected when new computer links are added or deleted. Thus, it allows for much more flexible expansion or contraction than many other proprietary network technologies. Its basic architecture encourages universal access and participation.

The internet was conceived as a simple, neutral, and open infrastructure. It was designed to maximize interoperability, that is, to be completely independent of software programs, hardware platforms, and other protocols. As a result, it is well suited to new applications and can easily accommodate revolutionary developments in both software and hardware. Because of its malleability, however, it is naïve to assume that the internet of

today will be the internet of the future. The nature of the internet is not fixed but contingent. The architectures of cyberspace could undergo major transformations in the years ahead. As we have seen, what was once a borderless global infrastructure is rapidly becoming a place filled with borders, particularly as countries like China firewall and isolate the Chinese internet through an elaborate system of filtering and blocking mechanisms.

Net Neutrality

At the heart of the internet's original design is a network architectural standard that was first called the "end-to-end" principle. If a network is constructed in accordance with this idea, intelligence in the network (such as software applications) is located at the ends but not in the network itself. The core of the network is simply a data movement capability that transfers data from one destination or "end" to another without inspecting that data or discriminating against certain forms of data in any way. Thus, competitive neutrality and openness were inscribed into the original design of the internet through its basic protocols.[15]

Some insist, however, that in order to preserve the original end-to-end nature of the internet for the future, there needs to be more regulatory oversight. For some time U.S. government regulators have supported the principle of "net neutrality," claiming that this neutrality is threatened by an unregulated internet dominated by powerful gatekeepers like Google and Yahoo. But what precisely is net neutrality? The idea is quite simple. All ISPs and telecom companies are required to treat every form of data equally, in a

way that is consistent with the end-to-end design principle. They cannot discriminate between different packets of data. This means that they cannot enhance the performance of some streams of data to create a “fast lane” for that data, nor can they employ “tolls” or any means that slow down the transmission of internet packets. In addition, they cannot create tiers of service in which some sites (such as a video site that a telecom may operate) perform better than others. They cannot block websites (unless those sites violate the law), and they cannot discriminate against specific hardware or software applications.[16]

Consider what a lack of “neutrality” might imply for a company like Microsoft. The implementation of net neutrality would prevent Microsoft from favoring its own search engine, called Bing, if it were to purchase a telecom company that provides internet access. Regulators argue that without net neutrality rules in place, Microsoft could impede access to Google in order to encourage customers to switch to Bing. Also, according to this hypothetical scenario, Microsoft might degrade its users’ experience of Netflix in order to boost its own video-on-demand service.[17]

By regulating the internet to ensure net neutrality, the end-to-end design principle would essentially become codified into law. Those who oppose

codifying the end-to-end principle in this way maintain that such laws are unnecessary. Let the internet companies, content providers, and consumers sort all this out. Why should a Netflix video be treated in the same way as other data that do not consume nearly as much capacity? Net neutrality is also unrealistic—Netflix and YouTube hog capacity and require some type of “fast lanes” on the internet. They invest in massive networks of computer systems to ensure efficient delivery of their high-bandwidth content.[18]

Yet governments are rapidly moving in the direction of new laws and internet regulations. Chile, the Netherlands, and Slovenia have already passed stringent network-neutrality laws. While some countries, like Chile, do not allow for any sort of internet traffic prioritization, others make room for certain exceptions. The chance of such laws soon coming on the books in Europe is unclear because EU governments must agree on a common set of regulations.[19]

The United States, however, was a different story. On March 12, 2015, the Federal Communications Commission (FCC) released an order called *In re Protecting and Promoting the Open Internet* (also known as the “Open Internet Order”). This mandate, which has been described as “one of the most important in the history of the internet in the

United States," reclassified broadband internet access services from an "information service" to a utility or telecommunication service, making it subject to the common carrier provisions of Title II of the Telecommunication Act of 1996. Broadband providers would be overseen by the FCC and regulated as "public utilities" with the "strongest possible rules." Broadband providers would even be subject to price controls under Title II, which has the authority to set "rates, terms, and conditions" for the provisions of any services. Skeptical analysts pointed out that these rules could effectively wipe out decades of a soft or "light-touch" regulation of the internet and the web. Nonetheless the rules were designed to ensure equal handling of all internet data. They gave the FCC the authority to prevent broadband providers from any sort of blocking or discrimination of lawful content. Nor could they employ "paid prioritization" strategies. Those providers can neither deliberately slow down website traffic nor speed up such traffic in exchange for payments made by a specific site.[20]

However, in December 2017, the Obama-era net neutrality rules were repealed by the FCC. That repeal took effect in June 2018. In explaining this policy reversal, the FCC Chairman claimed that these regulations were an impediment to

innovation. Many consumer advocates disagreed. They worried that without these rules broadband providers would start to sell internet access in bundles. Thus, access to Facebook and Twitter might require paying for a social media bundle. But others have maintained that the suppression of net neutrality rules will not alter the direction of the internet or lead to practices such as paid prioritization.[21]

The World Wide Web

Like the computer itself, the internet needed its own Graphical User Interface (GUI) revolution that would make this global network more user-friendly. This revolution occurred in 1990 just as the GUI called Windows was replacing MS-DOS as the standard operating system for the PC. Thanks to this new interface, users could now navigate every region of the internet with a mouse, moving effortlessly from one location to another by simply clicking on a hyperlink.[22]

The web was developed by Tim Berners Lee at the European Particle Physics Lab as a means of exchanging data about high-energy physics among physicists scattered throughout the world. This group developed a standard known as Hypertext Markup Language (HTML) that supports a procedure whereby “tags” or triggers are attached to a word or phrase that links it to another document located anywhere on the internet. The documents created by HTML are stored on computers known as servers and can include straight text, visual images, streaming video, and audio clips. Documents belong to a website that has a specific address such as “**www.bostoncollege.edu**.” The last three letters

represent a “top-level” identification (e.g., “edu” stands for education and “com” stands for a commercial enterprise), and the middle part of the name designates the actual site (Boston College).

Net browsers such as Firefox, Google’s Chrome, or Microsoft’s Internet Explorer enable users to “explore” the web rather effortlessly. They are highly versatile navigational tools that enable users to access, display, and print documents; they also give users the ability to link to other documents at any location on the web. Hyperlinks can create a maze of interconnected documents and websites that can sometimes confuse users but also greatly expand opportunities for research and investigation.

Despite its brief history, the World Wide Web itself has already become a vast, tangled network. Websites were first deployed at major universities and research centers, but soon proliferated throughout cyberspace at schools, hospitals, corporations, and many other organizations. According to the Internet Systems Consortium, there were approximately 1.7 billion active web domains operating in cyberspace in 2019.[23] Many individuals and small businesses have established their own webpages. These websites have become an indispensable vehicle for electronic commerce and the promotion of many other

network-based activities like education or fund raising. Web-based marketing has shown remarkable results, and, as a consequence, ad banners and commercial messages can be found in almost every region of cyberspace.

This plethora of websites has created a density of information that can make it difficult for users to locate a particular site. Search engines such as those provided by Microsoft or Google can help in this process, but even they are sometimes ineffectual in the face of such voluminous data. Part of the problem, of course, is that the web is just too large and too volatile to index properly, but these search engines have made great strides in this regard.

Regardless of the difficulties that users encounter trying to navigate through cyberspace, the web has become its own unique institution, taking the place of libraries, print catalogs, and even traditional news media for many users. It can be a rich source of research, news and information, and entertainment. And as more and more users develop their own sites, it has helped bring about the democratization of information predicted by many internet visionaries.

Gatekeepers and Search Engines

Some of the fastest growing industries in cyberspace are information intermediaries. The rapid proliferation of networks has created the need for versatile technologies that mediate and shape our experience in cyberspace. These technologies include browsers, ISPs, and portals, such as Yahoo and MSN. Horizontal portals have functioned as gateways to the web by providing an initial point of access from which users could connect to various sites. They also provide many services, such as email and blog hosting, for their users. Vertical portals such as **Quicken.com** in the area of financial services are distinguished by their “deep content” and hyperlinks exclusive to one subject area.

A web browser enables personal computer users to navigate the web and to display or scan various webpages. Those who pioneered this technology believed that the browser had the potential to become a universal interface, a partial substitute for the PC operating system. This hasn’t happened, but the browser is a vital tool for every internet user. The browser industry has gone through intense waves of competition beginning with the lethal “browser wars” of the 1990s

between Microsoft's Internet Explorer and Netscape Navigator. The new browser war pits Microsoft and Firefox against Google's Chrome browser, which has been gaining ground for some time.

But, to a great extent, attention has shifted away from browsers and portals to search engines. Users have become increasingly reliant on search engine technology to find information or point them in the right direction when they are seeking to make a purchase. This technology has been defined as "an information retrieval system that allows for keyword searches of distributed digital text."[24] The search engine functionality is simple enough: a user enters a search term in a search "box," and the search engine retrieves a list of relevant webpages and their hyperlinks.

The leading search engine is Google, founded in 1998 with a mission "to organize the world's information and make it universally accessible." Google was not the first mover in search engine technology but overcame the liability of being a latecomer through its PageRank technology, which provided better search results, free of the spam that bedeviled other search engines. Google has consistently sought to improve its performance by refining its search algorithms. It has developed techniques such as personalized search, which

prioritizes results according to a user's search history. Through its auction format, Google's abundant corporate clients pay for ads that appear alongside or above search results. Google has it both ways: users get unbiased organic (or unpaid) search results while paid content generates ad revenues.[25]

Google's dominance has concerned regulators who worry that this company will monopolize search and perhaps use that monopoly as a lever to gain control over other online industries. Google has also been thrust into the center of many controversies about privacy and free expression. Privacy advocates are troubled over Google's expansive "surveillance" capabilities. The company retains the search history of its users and relies on accumulated behavioral data to deliver those precisely targeted, personalized ads.

But search engine technology raises a host of more subtle ethical concerns that typically are neither well publicized nor properly understood by web surfers. The fundamental question is whether or not users are getting unbiased organic results when they initiate a search. Ethicists have claimed for many years that search engines like Google "systematically exclude certain sites and certain types of sites, in favor of others, systematically giving prominence to some at the expense of

others."[26] They might do this quite deliberately to favor their own online businesses or the websites sponsored by their major advertisers. On the other hand, this favoring of certain sites to the exclusion of others may be a way of giving users what they want based on the popularity of certain sites and based on their own past search history. The search algorithm has been specifically designed to take into account what the users wants (at least what Google thinks a user wants) and generate search results that are compatible with the user's profile. PageRank is also designed to deliver relevance, which usually means that popular sites are given priority over others that may be more informative or instructive. For example, if I search for "breast cancer treatment," I will receive sites that are consistent with my search history and have attracted the attention of other people who have done a similar search. But this list of websites and links might not contain those sites that really have the most accurate, useful, and current information.

This dispute about search engine results is confounded by the fact that the search algorithms are proprietary technology. Thus, the fundamental moral problem is that the opacity of the search process threatens the ideal of equal and fair access to objective information. Google's

algorithms mediate the flow of information so that users see what Google thinks they want to see, which may deprive them of more impartial, neutral results that could open up new perspectives or opportunities for those users. Added to that is the pressure on Google to reward its trusted advertisers and partners.[27]

Perhaps Google's failure to always provide the most objective search results is not so problematic. It may be too much to expect neutral and comprehensive information from search engine queries, given the benefits of personalized search and the fact that search engine technology was not necessarily designed with this sort of objectivity in mind. Nonetheless, the opacity of this technology will continue to stimulate debate, especially as Google expands its commercial presence on the web. For this reason, some legal scholars like Frank Pasquale have argued that a search engine must exhibit at least a "qualified transparency" such that its policies and practices for filtering and displaying search results would be public information.[28] Some level of operational transparency might allay the concerns of regulators and businesses that rely so heavily on Google's search results for the quality of their interactions in cyberspace.

Social Networking

During the last two decades the web has taken on a new facade, thanks to the proliferation of social networking websites, such as Facebook, LinkedIn, Twitter, and Yik Yak. Most of these sites give people an opportunity to create their own personal space on the web, to share their personal data, or to communicate with a network of friends and followers. Many people, for example, find Twitter (**Twitter.com**) to be a useful tool for following the comings and goings of their friends and family or for receiving personalized news feeds from trusted sources.

One of the true pioneers in this social networking technology was Myspace, founded in 2004 and acquired by the media conglomerate News Corp several years later. Myspace copied the basic features of a predecessor site known as Friendster, but gave users considerable latitude in customizing their personal web pages. Each user had a profile page where he or she could post pictures, discuss their interests and hobbies, and provide links to the profiles of family members and friends. On Myspace a user could choose to preserve anonymity and create a whole new identity for herself. According to Angwin, Myspace

was founded partly as a reaction against the "constraints of unitary identity" at websites like Friendster.[29]

But Myspace soon took a backseat to Facebook, which still has the biggest footprint in the social media infosphere. Facebook was launched in 2004 by Mark Zuckerberg as a social network exclusively for Harvard students. The network gradually expanded to include high school and college students, and now it is available to anyone on the internet with an email address. Facebook allowed its members to create a profile and to share personal information and updates with their "friends." By the summer of 2005, the website had grown to 5 million members. It launched Facebook Photos in October 2005 with an innovation that informed friends whenever a photo of one of them was posted online. A year later it added News Feed that collected all of the updates, photos, and status changes of one's friends. Users could log into their Facebook page and look at this stream of data to keep abreast of what was going on with their Facebook friends. News Feed is now regarded as one of the core features of Facebook. Facebook continues to attract new users and its fastest growing demographic is users over the age of 30. It requires that people use their real identities, making it more difficult for sexual

predators or other rogue individuals to operate at this site. Facebook is by far the most popular social network worldwide, with over 2.2 billion monthly active visitors. In 2019, the total number of worldwide social media users was approximately 4 billion.[30]

Another social networking site that has quickly become a social phenomenon is Twitter. Twitter allows users to post very short text messages (not to exceed 140 characters), which are known as “tweets.” These postings can be read by anyone who follows or “subscribes” to this person’s twittering service. A user can see whom other people follow and then choose to follow those same individuals. Users can also comment on a tweet by means of an “at reply” (a short message beginning with the “@” sign). The company sees the potential for Twitter to evolve into a powerful marketing and communications tool. NASA, for example, relies on this service to update subscribers about the status of a space shuttle flight.[31] According to Malone, Twitter sees itself becoming the “epicenter of the web.”[32]

A social media mini-phenomenon that has also gained some attention is Yik Yak. Unlike Facebook and Twitter, Yik Yak is anonymous and does not include user profiles. It sorts messages not by

friends or followers but by geographic location. It posts messages only within a 1.5-mile radius, making it ideally suited for college campuses, where it quickly became a popular communications medium. However, this virtual community of “yakkers” has become known for posts containing mean-spirited remarks about fellow students and even about college administrators and professors. Yik Yak has even been used to make threats of mass violence on more than a dozen campuses. At one college, a yakker suggested that people gather for a gang rape at the local women’s center. Anonymity emboldens some students to launch yaks laced with personal insults and derogatory comments. The widespread abuse of Yik Yak is unsettling for many college and university administrators, but they are hesitant to censor content on social apps, no matter how offensive it may be.[33]

One of the challenges facing all social media sites is monetizing their extensive web traffic. These sites typically do not charge their users for basic services. The primary revenue model is advertising. In addition to generic ads, the sites often rely on certain types of users’ personal information to send them targeted ads. Facebook allows marketers to purchase these targeted ads based on certain forms of behavioral data shared

by their users such as a person's favorite books or music.

The same factors that make social networking sites so popular also make them particularly difficult to control. There is a constant challenge to guard against illegal activities, such as "sexting" and the dissemination of child pornography, and to protect users from online predators. There have also been serious problems with cyberbullying and with users assuming someone else's identity. In one notorious case of cyberbullying involving Myspace, a mother assumed the identity of her teenage daughter in order to taunt one of her daughter's friends. The taunting was so severe that the young woman committed suicide.

Unfortunately, social media has given cyberbullies a versatile platform to prey on their victims. After a wave of online bullying, many states passed laws that make it a crime to bully others online, especially children. The New York law makes it illegal to communicate "private, personal or sexual information" about someone that is intended to "harass, threaten, abuse, taunt, intimidate . . . or otherwise inflict significant emotional harm on another person." In New York, a high school student was arrested for cyberbullying after he created a "Flame page" on Facebook that included graphic and sexual comments about some of his

fellow students. Many of these laws are being challenged, however, as violations of the First Amendment.[34]

How much accountability these intermediary services should have for the illegal or ethically questionable activities of their users is a disputed policy issue with many ethical implications. Thanks to the Communications Decency Act (section 230c), online service providers and social media platforms have fairly broad immunity from defamation, hate speech, and other offenses perpetrated by their users, but this is not the case with most foreign countries.

However, some efforts to control social networks are a source of contention. Facebook's real name principle, for example, has been criticized by some because it denies anonymous free speech (at least on the pages of Facebook). Facebook was a popular platform in Egypt for organizing protests against the repressive Mubarak government, but Facebook removed a popular page called "Silent Stand Against Torture" because its creators had not used their real identities. Is this a prudent policy or should Facebook permit anonymous social networking?[35]

In addition, privacy issues in relation to these sites remain largely unresolved and promise to become

more vexing in the future. Social network sites, such as Facebook, collect vast amounts of personal data, which is central to the success of their business models. Through cookies and pixel tags, Facebook tracks its users across the internet and collects valuable data of the websites they visit when they aren't on the social network. It can even track users through their apps and mobile devices. This browsing history allows Facebook to build rich user profiles, thereby enabling advertisers to send targeted ads or more personalized marketing messages. Virtually every website collects data about visitors, but Facebook is different because it has actual names, giving the social media company the flexibility to do more with the data that it collects.[36]

Finally, the primary users of Facebook and other social media sites are teenagers and young adults. To what extent can Facebook possibly protect them from predators, inappropriate ads, and other perils lurking in cyberspace? Facebook faces an overwhelming challenge in policing a network, with over a billion users and a million advertisers. It's no surprise, therefore, that teenagers end up being exposed to lurid ads they are not supposed to see. Ads for webcam modeling and dating sites, for example, were seen by many young girls even though they were meant to be seen only by adult

women. One problem is that some teenagers exaggerate their age. Also, Facebook's targeting system is quite complex, which can allow ads unsuitable for young adults to slip through the cracks.[37]

These questions about anonymity, privacy, and the self-censorship of advertisements suggest some of the key ethical problems social media sites like Facebook will need to resolve as they become a more formidable presence in the terrain of cyberspace.

Regulating the Digital Infrastructure

Our review of social networking reveals some of the more acute social problems and frictions in cyberspace. The erosion of privacy through constant surveillance by cookies and other digital tools, the upsurge of disinformation, and the scourge of online hate speech that now plagues cyberspace are not easily resolved. In Lessig's terms, is the optimal solution to be found in laws and regulations, the market, code, or the propagation of social norms? It is probably naïve to think that any one of these four modalities of regulation, such as law, can fix a problem such as privacy erosion in cyberspace. The proper solution will undoubtedly be found in the interplay of law, code, and the market, with ethical principles as a compass. But which of these three forces should have primacy? Some have suggested that marketplace forces represent the best forum for addressing the most troublesome social problems. Yet the market is often reactive and unable to solve serious inequities. Asymmetries of knowledge and power work against consumers who feel they have no good substitutes for the prying eyes of Google and Facebook. In response to claims that Google was promoting its own comparison shopping services to the detriment of consumers, Executive Chairman Eric Schmidt said

“if consumers don’t like the answer that Google Search provides, they can switch to another search engine with just one click.” But this is not a realistic option for consumers, since no other search engine has the scope and capabilities of Google.[38]

The alternative to corrective market forces is the greater reliance on the coercive force of law and policy constraints imposed by government. But can cyberspace be effectively regulated—is it really “regulable” in the same way that the physical world can be subjected to the control and laws of local sovereigns? Can the unrestricted freedom of cyberspace be reined in by government forces?

The internet complicates regulation for several key reasons. First, its distributed architecture and resilient design make this online landscape hard to manage. Packet-switching technology, for example, encumbers the control of information flows. As John Gilmore puts it, “Information can take so many alternative routes when one of the nodes of the network is removed that the Net is almost immortally flexible. . . . The Net interprets censorship as damage and routes around it.”[39]

The internet’s lack of a physical center means that it has no moral center that can be held accountable for information flowing over the network.

Second, there is the internet's content, digital information, 1s and 0s, that can be transmitted through cyberspace with ease and stored on the recipient's hard drive. As Negroponte observed, cyberspace "is about the global movement of weightless bits at the speed of light."[40] All forms of information, including images and voice, can be digitized, and a digital file is especially difficult to contain. One consequence of this is that digital file-sharing technologies such as those developed by Grokster and **Torrent-finder.com** (a search engine for file-sharing websites) threaten to undermine the economics of the music and movie industries.

Finally, governments that seek to control or regulate the Net face an array of jurisdictional conundrums. Laws and regulations have force only within a sovereign's territorial boundaries. As one jurist put it: "All law is prima facie territorial."[41] Moreover, because the internet was designed as a borderless global technology, it is difficult for any country to enforce the laws or restrictions it seeks to impose on this sprawling region of cyberspace. If the United States decides to outlaw pornography, it can effectively enforce this restriction only among U.S. purveyors of pornography. It cannot restrict vendors located in Europe or the Caribbean from making

pornography available on the internet for everyone to see. It can, of course, put the burden on internet providers and hold them liable for transmitting the illicit material no matter where its source is located. But this seems to be an unfair and burdensome solution because it is expensive and difficult for ISPs to detect and properly filter out all communications with pornographic elements.

As we observed earlier, despite these obstacles, local sovereignties have not been deterred from regulating the Net. In 2000, a French judge issued an order preventing Yahoo from allowing Nazi memorabilia to be sold on its auction websites, despite the fact that the server hosting these sites is located in the United States. A French group called La Ligue Contre Racise et L'Antisemitisme (LICRA) brought a successful suit against Yahoo, claiming that the company violated local French law. But to what extent should the global internet be subjected to local law? The potential problem, according to Zittrain, is that "anyone posting information on the internet is unduly open to nearly any sovereign's jurisdiction, since that information could have an effect around the world."[42]

Thus, each modality of regulation, including code, has its own peculiar shortcomings. As Cohen observes, we can no longer accept a vision of code as a tool for promoting freedom, access, and

openness. China’s construction of a surveilled and heavily censored domestic Internet is a prime example. Even technologies employed in democratic societies incorporate too many opaque surveillance and control capabilities that make it difficult for users to protect their interests. But with the aid of prudently written code and fair laws, responsible politicians, sensitive to ethical principles, should be able to develop better ways to modulate information flows and hold corporate powers more accountable.[43]

Internet Governance

Although there is some disagreement on how the internet should be regulated through government intervention, no one questions the need for some type of governance and technical coordination. There must be governing bodies that handle ordinary and routine technical matters, such as the determination of technical standards and the management of domain names and IP addresses. For our purposes, *governance* refers to managing these matters rather than regulating the Net through content controls or other mechanisms.

Two major policy groups that provide such governance are the World Wide Web Consortium, an international standards setting body, and the Internet Engineering Task Force (IETF), which develops technical standards, such as communications protocols. According to the *Economist,* a culture of “cautious deliberation” prevails within the IETF, which strives to be democratic in its decision-making processes. Anybody can join the IETF and any member can propose a standard “and so start a process that is formal enough to ensure that all get a hearing, but light enough to avoid bureaucracy.”[44]

The Domain Name System (DNS) also needs coordination. The DNS maps the domain names of organizations, such as eBay or Amazon, to the actual numeric internet protocol address (e.g., 709.14.3.26). The DNS is a hierarchical system divided into separate domains. When a domain name is invoked by a browser, the request is forwarded to the DNS server, which is normally operated by an ISP, and that server locates the databases for each subdomain. If the domain name is **www.bc.edu**, the DNS server first locates the server for ".edu," which is the top-level domain (TLD); it then finds the server for "bc," the second-level domain, and so forth. Using this method, the webpage is found and transmitted back to the recipient.

This system was formerly administered by a small private company called Network Solutions International (NSI), which charged $50 for the registration of a domain name and usually awarded the name on a first-come, first-served basis. As the internet became commercialized, disenchantment with the NSI arrangement escalated. As a result, after some political maneuvering, the domain name system is now in the hands of the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN is an international, nonprofit organization with full

responsibility for the DNS. ICANN itself does not actually distribute domain names. That task is delegated to domain name registrars such as VeriSign. ICANN determines the policies for domain name distribution, and it has the final say for selecting firms that qualify as registrars.

Domain names were introduced to impose some order on the Net, and originally there were six TLDs: .com, .net, .org, .edu, .gov, and .mil. ICANN has recently decided to create several new TLDs, such as .aero (air transport companies), .coop (cooperatives), .biz (business), .museum (museums), .name (individuals), .pro (professionals such as lawyers), and .info (nonrestricted use). The purpose of these new extensions is to handle the over usage of popular TLDs such as .com and .org. It remains to be seen whether these new extensions (like .biz) will be embraced by the public and become as popular as the original TLDs like .com.

To its credit, ICANN acted swiftly and deliberately to deal with the issue of cybersquatting and other domain name disputes. In October 1999, it established the Uniform Dispute Resolution Policy for adjudicating such disputes and protecting legitimate trademarks. That policy is discussed in more detail in **Chapter 4** in the context of the treatment of trademark law and the Lanham Act.

ICANN was under U.S. oversight for many years. As a result, the United States had veto power over all decisions (such as the creation of new web domains). But, in 2016, the United States handed over full administrative control to ICANN, which is currently governed by a board of 18 members; nine of those board members are elected by the at-large membership. ICANN is now fully independent and answers to no government authority. The transfer of power was controversial but widely praised. The hope was that this move would initiate a new era of international cooperation for internet governance. However, ICANN has had to contend with financial problems and internal power struggles, and some have argued that the United States must reclaim its authority over this organization. But as one Trump policy advisor pointed out, “it would be very difficult to put the genie back in the bottle on ICANN.”[45]

Contested Sovereignty in Cyberspace

While almost everyone concurs that the internet must be governed by global bodies like ICANN, there is far less consensus about how much national governments should be involved in internet affairs. The internet has always been regarded as a liberating and transformative technology that gives users a voice. In the past, the Net has facilitated political activism and dissent, especially against repressive governments. Activists like Di Liu and Shi Tao in China have used the internet to criticize the government and advocate for reform. In the aftermath of its 2009 contested election the Iranian government seemed powerless to stop angry citizens from sharing online images and tweets about the escalating protests and violence. Digital empowerment appears to have weakened state sovereignty and given individuals the upper hand. Many remain optimistic about the internet's power to spread and promote freedom.

It would be premature, however, to underestimate the power of the state and to toll the death knell for its sovereignty. As Michel Foucault writes, "wherever there is power, there is resistance."[46] The state has strongly resisted this state of affairs,

seeking to restore its lost dominance by regulate ISPs and pressuring other private surrogates like Google and Yahoo to help carry out its regulatory regime. Public policy makers in these countries also recognize the power of code as a constraint in cyberspace. China has installed powerful filters on the routers that direct internet traffic to maintain a monopoly over information. And in Turkey, the government attempted to block access to social media websites to stifle dissent during its local elections. Turkish authorities also demanded that Google block YouTube videos claiming government corruption.

For their part, activist software developers continue to build tools that will allow users to evade government censorship and surveillance. They have recently introduced a more effective anonymizer tool known as Tor, which allows users to navigate the web and download or upload content without being traced. Tor is a prime example of the power of code in the hands of individuals. Other groups have developed alternatives to social media platforms like Facebook (such as Diaspora) that enable users to enjoy the benefits of social networking without the heavy hand of corporate censorship.[47]

What we are left with, then, is a shifting balance of power between the centralized state and the

dispersed internet community. At the center of that escalating struggle is the code of cyberspace, which undoubtedly has a liberating potential. But even when code is designed to embed important democratic values there can be a high social cost. The software system known as Tor embeds the value of anonymity, whereas Apple's adoption of unbreakable encryption in its operating system for the iPhone embeds the value of absolute privacy. That code gives its users considerable leverage against government intrusion. But the use of this strong encryption could also lead to unintended adverse consequences for national security, since law enforcement authorities cannot examine the iPhone contents of terrorists and criminals. Thus, code can become a means for ensuring privacy but also a vehicle for jeopardizing human well-being.

Internet Monopolies

The inventors of the internet and the World Wide Web could hardly have predicted the undisputed dominance of the online world by a few digital giants including Amazon, Google, and Facebook: Google for online searches, Amazon for electronic commerce, and Facebook for social media. The size and behavior of these firms has sparked severe concern and apprehension across the political spectrum. These companies not only monetize and manipulate their customers' information, they also make critical decisions about who gets a "digital megaphone," and who gets unplugged from the web.[48] Backlash against these monopolies has increased the pressure to curb some of their dubious practices but they still routinely exploit their considerable powers to thwart rivals.

Arguably, these high-tech giants are just as powerful (and dangerous) as their industrial counterparts many decades ago, such as Standard Oil or U.S. Steel. Those monopolies or trusts of the Gilded Age damaged consumer welfare through their predatory pricing policies, and they were eventually dismembered. More recent monopolies such as IBM in the 1970s and

Microsoft in the 1990s were met with resistance by federal enforcers of U.S. antitrust laws. However, the heaviest blow to their dominance was inflicted not by the government but by shifting market forces.

On the other hand, a light regulatory touch has allowed companies like Facebook and Google to grow and prosper. They face few regulatory burdens, an anomaly for corporations with as much influence as these digital giants. They continue to thrive on the lucrative personal information of their users, and they have been able to withstand competitive pressures by swallowing up the competition at an alarming rate and with little resistance from government regulators. Facebook, for example, viewed Instagram, a company that combined a photo app with social media, as a potential future threat. As a result, in 2016 it purchased the company for $1 billion without any interference from regulators. According to *Time*, this purchase showed that Facebook was deadly serious about "dominating the mobile ecosystem while also neutralizing a nascent competitor."[49] Facebook has made 67 acquisitions, while Google has acquired 214 companies and Amazon has purchased 91. As Tim Wu points out, through this stream of

unchallenged acquisitions the tech industry became dominated by these few giant trusts.[50]

However, is this *laissez-faire* attitude likely to change in the future? Is comprehensive regulatory intervention on the horizon for these internet titans as they continue to extend their power throughout cyberspace? There are certainly signs of impatience by regulators, especially in Europe where the EU has imposed a $2.7 billion fine on Google for its anticompetitive practices. Even among U.S. policy makers patience is growing thin, especially in the wake of Facebook's many scandals.

But what is the most effective remedy for this concentration of economic power in the hands of companies such as Google, Facebook, and Amazon? At one extreme, some policy makers argue that these corporations must be dismembered. The only way to dissipate their excessive power and influence is a breakup based on reasonable economic criteria. The debate about the internet giants even found its way into the 2020 U.S. presidential election with some Democratic candidates calling for the dissolution of these monopolies.

Others argue that monopolies like Amazon are fairly benign, and can even be agents of progress.

Monopoly rents provide a consistent stream of resources for innovation and more powerful efficiencies, which are vital for success in a digital world. According to Peter Thiel, the government's obsession with bigness and the lack of competition is a "relic of history." Competition is the result of failure to capture a market in its totality, and success comes from providing a unique solution, and thus "tends to be naturally monopolistic."[51]

A key question in the debate about digital monopoly is determining whether the harm caused by these companies warrants drastic action such as a breakup or more moderate regulations. Antitrust laws in the United States, such as the 1890 Sherman Act, prohibit corporations from monopolizing or attempting to monopolize a particular market. Courts no longer strictly interpret the Sherman Act but instead rely on the more flexible rule of reason. But what criteria guide the courts in determining when giant companies have stepped over the line and transgressed the boundaries laid out by that law and subsequent jurisprudence?

Economists have offered different theories to answer that question. The Chicago School has argued for some time that courts should be guided by the standard of consumer welfare and the economic criterion of higher prices. Antitrust law is

violated only when the alleged anticompetitive behavior leads to a monopolistic price structure or excessive price increases. According to this view, the government must prove beyond a doubt that the questionable monopolistic behavior actually elevated consumer prices and thereby made consumers worse off. Although this interpretation amounts to a narrow reading of the Sherman Act, this standard has clearly influenced antitrust jurisprudence.[52]

For the tech giants like Google or Facebook, which offer their services for free, the consumer welfare standard would not apply since consumers are not hurt by monopoly pricing. On the other hand, these companies are arguably culpable of hindering competition, which can diminish consumer welfare in different ways. Consider the case of Google. If someone searched for an “electric heater” online 15 years ago that person would have found comparison shopping sites like Nextag high in the search results. But when Google launched its own comparison shopping business those sites dropped down in those results, while Google Shopping was given preference. Other comparison sites might have better deals than Google Shopping, but will consumers even notice them? This outcome is a reminder of the power of

Google's opaque search algorithms that determine what and who gets found on the internet.[53]

But if this qualifies as anticompetitive behavior that must be stopped, what is the appropriate remedy. Breaking up big companies is not a simple task. It's expensive, time-consuming, and subject to many unintended consequences. Nonetheless, critics of these monopoly trusts and some policy makers continue to call for a breakup of these firms before it is too late. How might such a policy be implemented? Facebook, for example, could be divested of two key acquisitions that have augmented its power: Instagram and WhatsApp. Social costs would be minimal and the end result would be more competition within the social media industry. At the very least, U.S. policy makers should more diligently review mergers and acquisitions. Broader standards that consider the effects on innovation and economic concentration should be adopted. The goal of antitrust policy and jurisprudence should not be predicated solely on the consumer welfare standard, but also on the protection of competition. Such protection would most likely require more limitations on the concentration of economic power.[54]

DISCUSSION QUESTIONS

1. Discuss the pros and cons of extensive government regulation of the internet, either by a local sovereign government or by an international body specifically constituted for this purpose.
2. Do you agree with Facebook's policy forbidding the use of pseudonyms or fake identities?
3. What is ICANN, and what does it do?
4. Should internet companies like Google or Facebook be dismembered in some way in order to promote a more competitive environment?

Case Studies

American or Australian Libel Law?

Mr. Joseph Gutnick, a prominent Australian businessman, was quite shocked when he came across some unflattering remarks about himself in an online article in *Barron's*:

> Some of Gutnick's business dealings with religious charities raise uncomfortable questions. A *Barron's* investigation found that several charities traded heavily in stocks promoted by Gutnick. Although the charities profited, other investors were left with heavy losses. . . . In addition, Gutnick has had dealings with Nachum Goldberg, who is currently serving five years in an Australian prison for tax evasion that involved charities.[55]

In addition to tax evasion, Gutnick was accused of money laundering in that same article. Gutnick decided to file suit for libel. *Barron's* is owned by Dow Jones & Company, publisher of the *Wall Street Journal*, which has its corporate headquarters in the United States. But Mr. Gutnick and his lawyers wanted to file the libel suit in his home country of Australia where the libel laws are quite strict. U.S. libel

law puts the burden of proof on the alleged victim, but Australian law puts the burden of proof on the publisher.

Thus, Dow Jones sought to have the case heard in the United States, where *Barron's Online* is written and disseminated. The company feared the precedent that would be set if the case were heard in Australia. In the future, posting material online could leave them open to multiple lawsuits in many different jurisdictions. Accordingly, Dow Jones' lawyers argued that the U.S. jurisdiction was the fairest place to hear this dispute. They also argued that Australian courts had no jurisdiction in this case.

But the High Court of Australia ruled that Gutnick could sue in his home state of Victoria, reasoning that this "is where the damage to his reputation of which he complains in his action is alleged to have occurred, for it is there that the publications of which he complains were comprehensible by readers."[56] According to Zittrain, the Australian High Court dismissed Dow Jones' "pile on" argument "that Gutnick could next sue the company in Zimbabwe, or Great Britain, or China," or wherever he read the

allegedly libelous remarks.[57] The court observed that Gutnick lived in Victoria and this was where the alleged harm occurred. It also noted that Dow Jones profited from the sale of *Barron's Online* to Australians. Dow Jones eventually agreed to a settlement and issued a retraction.

Nonetheless, the Australian court's ruling was unsettling for many in the publishing world. According to one lawyer for the publishing industry, "The problem is that rogue governments like Zimbabwe will pass laws that will effectively shut down the Internet."[58] On the other hand, doesn't Gutnick have the right to be judged by the law of his own country where many of his fellow citizens read about his alleged transgressions?

Question

1. Do you agree with the ruling in this case? Why or why not? Are Dow Jones' fears unfounded or do they have some merit?

Case Studies

Google: The New Monopolist?

In 1998 the U.S. Department of Justice (DOJ) filed a major antitrust lawsuit against Microsoft for abusing its monopoly power against Netscape in the browser wars. The protracted case ended with a partial government victory, though it scarcely hurt Microsoft's uncontested monopoly power in the operating system business. At the time, it seemed clear that, in the information age, monopoly was becoming the norm rather than the exception. This normalization of monopoly power began with the emergence of companies like Intel, Cisco, and Microsoft, which controlled critical ubiquitous software and hardware platforms. Concentration of power often depends on network effects, whereby a product's value increases with the number of people who use it. While the power of Intel and Microsoft has waned over the years, there are some new potential monopolists, including Google, Facebook, and Twitter.

Hence it is not surprising that the U.S. and European antitrust officials have shifted their attention away from Microsoft to Facebook

and Google. Google dominates the search engine business with a 78% global market share, despite Microsoft's late entry into the market several years ago with its Bing search engine. Antitrust laws such as the Sherman Act do not necessarily make it illegal to be a monopoly. However, it is illegal for a company to abuse its monopoly power, to leverage that power in order to tilt the playing field against new competitors or competitors in related businesses to which the monopolist wants to extend its scope. Accordingly, Microsoft was accused of "tying" in violation of the Sherman Act, that is, combining its Internet Explorer browser with Windows so that it could gain control of the browser market.

Google's founders realized that the information delivered to users by a pattern of searches was the information needed to determine relevant ads. Search results could produce the ads that users were interested in seeing. Thus, while Google's content and information is free, the company generates massive revenues from its innovative ad business. Google's algorithms dramatically transformed the advertising industry and ushered in the "Google era" along with the

company's online dominance. Like Microsoft, Google was in a position to use its expanding monopoly power in one business (search engines) to gain market share in other online industries. The company could simply adjust its secret search engine algorithms to favor its own products or services and direct users to its own websites instead of those operated by competitors. Concerned with Google's growing power and reach, the Federal Trade Commission (FTC), working in conjunction with the Department of Justice (DOJ), launched an investigation into Google's practices. The FTC considered whether Google has rigged its search ratings to promote links to its own shopping, local, travel, and finance sites over those of rivals. Google's own sites frequently showed up on the top spots of its search results. Search for a restaurant like "Capital Grille" in Dallas and it's likely that you'll be directed to Google Places, the company's local business information page. Critics of Google say that given its large market share, the company should treat its own content in the same way that it treats the contents of its competitors.[59]

Google's practices became more obvious when it entered the lucrative $110 billion

online travel business in 2011. Google conspicuously placed its own travel service atop services such as Expedia, Orbitz Worldwide, Inc., and Priceline. A search such as “Memphis to Omaha” yields a “Google-powered interactive chart” of the least expensive airfares between these two cities, and a Google flight tool links exclusively to the airlines’ websites. Further down on the list are links to the top travel websites such as Expedia. Similarly, in the past, a user’s search for a hotel might return a dozen or so conspicuous links to online travel agencies and hotel operators. But more recently the search most prominently displayed a Google shopping services page with reviews, hotel photos, and an offer to book a room.[60]

Google also favors its own comparison shopping services, known as Google Shopping. When someone initiates a product-related search such as “electric heater,” or “toaster,” Google returns ads above the organic search results that link directly to retailer sites (such as Target or Walmart) where those items can be purchased. The picture ads appear at the top of the first page under a title, such as

“Shop for electric heaters on Google.” The businesses featured in those ads pay Google each time a user clicks on their ad. Other comparison shopping sites like Nextag operate in the same way, but those sites, which also have links to retailers, are often demoted in the search results, even though they may offer better deals. Google claims that it gives its own content preference because users prefer links that send them directly to a company’s website rather than a link to a comparison shopping site.[61]

The FTC eventually concluded that while Google definitely favored its own shopping and travel services, its sincere desire to improve search results for consumers made it difficult to justify filing suit against the company. But Google hasn’t been so fortunate in Europe. In April 2015, the European Commission of the EU charged Google with abusing the power of its search engine to favor its own comparison shopping and travel services. Two years later, after negotiations failed, the European Union’s antitrust regulator fined Google $2.7 billion.[62]

As Google increases its stake in online commerce, it will continue to struggle with its

dual role in cyberspace as a search engine facilitating commerce and as a marketplace competitor. Google's core business principles include "Don't be evil." Google has interpreted this principle to mean that it would always deliver unbiased and neutral organic search results. But is Google faithful to its principles when it uses its power in the search engine market to gain advantage in other markets such as comparison shopping?

Questions

1. Is Google's monopolization of search the same potential threat to social welfare as Microsoft's monopoly of PC operating systems?
2. Should Google be prohibited from competing in other online businesses as long as it remains the dominant search engine platform?
3. How do you assess the European Commission's case against Google? If you were hired as Google's attorney, how would you defend the company's practices?

Case Studies

Social Media: Good or Bad for Democracy?

The philosopher Martin Heidegger spoke of the relentless drive of technology as the world and its objects become victim to humanity's calculations and designs. But technology's indeterminacy implies an uncertain future since we cannot predict where this drive will take us. A recent evolution of information technology has been social networking. Social networking fuses together the multimedia world described by Marshal McLuhan with virtual reality, and it displaces the real world with an artificial one. The person now dwells more extensively in an environment of texting, selfies, chats, Instagram photos, newsfeeds, and blogs. There was some apprehensiveness about the power of social media well before the immense popularity of Facebook and Twitter became a reality. But few could have foreseen that social media would also become a means for spreading misinformation and magnifying political partisanship.[63]

Techno optimists once argued that social media had the potential to become a great stimulus for democracy because it amplified the powers of free speech. When Facebook and similar platforms first appeared, many sincerely hoped that they would give voice to the marginalized in society. People with different and unconventional viewpoints could locate each other and mobilize to advance their interests. But while these results have been realized to some extent, these sites have also become purveyors of “fake news” along with vast amounts of disinformation. The term “fake news” has been popularized by President Donald Trump, but it was coined by Buzz Feed’s Craig Silverman. For some, the proliferation of all this “fake news” and other forms of online abuse has wiped away the great promise of the internet as a force for semiotic democracy.[64]

During the 2016 presidential election there was considerable disinformation on the web, along with heavy manipulation of information about the two presidential candidates, Hilary Clinton and Donald Trump. This abuse wasn’t supposed to happen on this democratizing technology, at least not on

this scale. But decentralized networks with no controls can become powerful tools in the hands of extremists and opportunists. News sites appeared printing sensational stories that were neither vetted nor verified. For these sites, which sought eyeballs to attract ads and generate revenues, there was little incentive to avoid misinformation and the diffusion of propaganda.

Consider the “fake news” entrepreneurs in Macedonia who created a number of pro-Trump websites. They adroitly imitated actual news sites and disseminated very partisan news stories that attracted Trump supporters. Their website domain names included **worldpoliticus.com** and **trumpvision365.com**. The sites published pro-Trump stories aimed at his supporters in the United States. These young Macedonians had no interest in advancing the candidacy of Mr. Trump. Rather, their sole interest was in attracting readers, since the volume of readers on their websites translated into greater advertising dollars. They also recognized that the best way to generate online traffic was to get their stories about the Trump campaign to spread on Facebook. Most of the websites had

Facebook pages with hundreds of thousands of followers. The more sensational the content, the more attention the story got among Facebook followers. And as Facebook engagements increased, so did their readers who were attracted by their outlandish propaganda stories. For example, within a week a spurious story from **Conservativestate.com**, "Hillary Clinton in 2013: I Would Like to See People Like Donald Trump Run for Office; They're Honest and Can't Be Bought," generated 480,000 reactions, comments, and likes on Facebook. Virtually all of the stories on these websites made false and misleading claims.[65]

The spread of propaganda, misinformation, and disinformation has become an epidemic in cyberspace and threatens to strike at the heart of the democratic process. Disinformation is the deliberate communication of false or misleading information, while misinformation is the communication of information without an intent to deceive. Often those who disseminate misinformation have evidence that is indirect or obscure. Democracies depend heavily on accurate and objective

information so voters can make informed choices. Fake news misleads voters and contributes to the further polarization of political parties. According to one political strategist, fake news disseminated on social media is “the biggest political problem facing leaders around the world.” This hyperbolic statement reflects the inability of governments to deal with fake news narratives except through draconian measures that are anathema to democracy.[66]

But fake news is not the only problem that bedevils social media. As the leading social media platform, Facebook found itself at the center of multiple controversies that involved the 2016 U.S. presidential election. In March 2018, the British newspaper, the *Observer*, along with the *New York Times* first revealed that a researcher had gained access to the personal data of Facebook users for Cambridge Analytica, a consulting firm hired by the Trump campaign. The researcher, Alexander Kogan, created a Facebook app and invited Facebook users to take a survey and download the app that harvested their Facebook data along with the data of their Facebook friends. That data included

names, birth dates, and location data as well as lists of every Facebook page they ever liked. And these data were downloaded without their knowledge or consent and added to a massive database being assembled for Cambridge Analytica. This political data firm has particular expertise in developing persuasive ads using "psychographic" techniques to manipulate voter preferences. By examining behavioral data such as what people "liked," it was possible to map out personality traits that could become the basis for targeted ads. The personal data of 87 million users had been mined in this way, and Facebook was aware of this activity since December 2015. However, it said nothing to its users or to U.S. regulators until the media published this story. Facebook has claimed that Cambridge Analytica collected these data under false pretenses. The scandal led to many questions about how Facebook monitors the apps deployed to collect its user information and whether data should ever be made available for psychological profiling for political purposes.[67]

Facebook has also been an unwitting catalyst for violence in vulnerable parts of

the world. Facebook entered Myanmar, a country unfamiliar with the digital world, and was unprepared to deal with its deep political and social divisions. Facebook seemed unaware of how its platform could be manipulated and abused by extremists who could easily sway a naïve population. In this country, Facebook *was* the internet, since most users only had mobile phones with Facebook already installed. Buddhist extremists wasted no time in using social media to spread disinformation in order to inflame ethnic tensions against the Muslim Rohingya minority. One of the country's leading Buddhist monks ignited a deadly riot when he disseminated a fake news story of a rape and warned of a "Jihad against us." According to one NGO, Facebook's platform was used for a "campaign of hate speech that actively dehumanize[d] Muslims." By March 2017 a million Muslims had fled Myanmar into Bangladesh. Facebook monitors missed many posts full of disinformation that helped to spark this ethnic cleansing. Moreover, when the tragedy intensified, Facebook was quite slow to react and remove hateful content, despite repeated warnings from multiple sources. It

also did little to prevent fake accounts from being created. Zuckerberg himself recognized the company's tardiness, as the people of Myanmar wondered why a company with Facebook's resources could not have reacted more expediently.[68]

In his defense to this series of crises, Zuckerberg has insisted that fakes news is much less common than people imagine. He attributes the company's mistakes and missteps to an excessive optimism and a lack of awareness of how some Facebook customers misuse their service. But some analysts are quick to point out that while this explanation has some merit, it ignores the company's fixation on rapid growth and an unwillingness to heed warnings from outsiders.[69]

The company has made some concessions. For many years Facebook did not disclose the sources of funding for political ads. But now users can find out on Facebook who paid for a political ad and whom the ad targeted. The company is also considering ways to "impose friction" to impede the spread of disinformation and misinformation. (Perhaps pop-ups with warnings such as "Do

you really want to share this item?"). However, it is exceedingly difficult to control election propaganda or slow down the spread of disinformation, short of draconian censorship measures. With 2.7 billion people using Facebook's services, monitoring content is the most difficult challenge facing the company. Yet fake news is a threat to liberal democracy, and Facebook must find a way to deal with users who share these false or barely credible news posts. On the other hand, it is perilous to have a small group of social media companies determine what kinds of political speech people will see. Hence the social media world faces a paradox: a greater emphasis on truthful news and communications will lead to limits on free speech, while too much speech opens the door for flows of disinformation and reckless propaganda. How can social media strike the right balance between these two competing objectives?[70]

Questions

1. In your estimation how serious is the problem of "fake news" or disinformation in cyberspace?
2. What are some of the moral and social problems involved in using

disinformation to generate website traffic? Be specific and refer to the theories of **Chapter 1**.

3. What policy changes would you recommend for Facebook that might help it remedy some of its past lapses and problems? What can be done about harmful, misleading content, election protection, privacy or data protection?

REFERENCES

1. Scott Shane, “From Headline to Photograph, a Fake News Masterpiece,” *New York Times*, January 18, 2017, A1, A12. See also Yochai Benkler, Robert Faris, and Hal Roberts, *Network Propaganda* (New York: Oxford University Press, 2018), 3, 268–69.
2. Damien Cave, “The Global Push to Make Social Media Accountable for Its Content,” *New York Times*, April 1, 2019, A5.
3. Stewart Brand, “Interview with Paul Baran (Founding Father),” *Wired*, March 2001, 145–53.
4. Janet Abbate, *Inventing the Internet* (Cambridge, MA: MIT Press, 1999), 11.
5. Ibid., 111.
6. World Internet Usage Statistics, Updated, June 2019, **http://www.internetworldstats.com**.
7. Ibid.
8. Dave Evans, “The Internet of Things: How the Next Evolution of the Internet Is Changing Everything,” Cisco White Paper, April 2011.

9. Christopher Anderson, “The Accidental Superhighway: A Survey of the Internet,” *The Economist*, July 1, 1995, 6.
10. Katie Hafner, “The Internet’s Invisible Hand,” *The New York Times*, January 10, 2002, E1.
11. This discussion is adapted from Rus Shuler, “How Does the Internet Work,” **http://www.theshulers.com/whitepapers/internet_whitepaper/**. See also Alexander Galloway, *Protocol: How Control Exists after Decentralization* (Cambridge, MA: MIT Press, 2004), 38–49.
12. Manuel Castells, *The Internet Galaxy* (New York: Oxford University Press, 2001), 28.
13. Jonathan Zittrain, “The Rise and Fall of Sysopdom,” *Harvard Journal of Law and Technology* 10, no. 3 (1997): 495.
14. Hafner, “Internet’s Invisible Hand,” E5.
15. Jerome Saltzer, David P. Reed, and David D. Clark, “End to End Arguments in System Design,” *ACM Transactions on Computer Systems* 2, no. 4 (1984): 277–88. See also Richard Spinello, *Regulating Cyberspace* (Westport, CN: Quorum Books, 2002), 31–33.
16. David Crow, “Strife in the Fast Lane,” *Financial Times*, November 17, 2014, 7.

17. Thomas McDonald, “Net Neutrality Needs to Be Done the Right Way,” *National Catholic Register*, March 16, 2015.

18. Gordon Crovitz, “What a Tangled Web Obama Weaves,” *The Wall Street Journal*, November 17, 2014, A11.

19. “Network Neutrality: To Be Continued,” *The Economist*, January, 31, 2015, 54.

20. Gauthem Nagesh and Andy Brody Mullins, “How White House Thwarted FCC Chief on Net Rules,” *The Wall Street Journal*, February 5, 2015, A1, A10. See also F. Fernandez, “Net Neutrality Proposal: Stairway to Heaven or Highway to Hell,” *The Bolt* (Stanford Law Review), April 15, 2015.

21. Keith Collins, “Why Net Neutrality Was Repealed and How It Affects You,” *New York Times*, December 14, 2017, B1.

22. Brian McCullough, *How the Internet Happened: From Netscape to the iPhone* (New York: W.W. Norton, 2018), 4–5.

23. Internet Systems Consortium, ISC Internet Domain Survey, June 2019, **http://www.isc.org**.

24. Alexander Halavais, *Search Engine Society* (Malden, MA: Polity, 2009), 5–6.

25. Scott Galloway, *The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google* (New York: Penguin, 2017), 131.

26. Lucas Introna and Helen Nissenbaum, "Shaping the Web: The Politics of Search Engines Matters," *The Information Society* 16, no. 3 (2000): 7.

27. See Julie Cohen, *Configuring the Networked Self* (New Haven, CT: Yale University Press, 2012), 198–99.

28. Frank Pasquale, "Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries," *Northwestern University Law Review* 104, no. 1 (2010).

29. Julia Angwin, "Putting Your Best Faces Forward," *The Wall Street Journal*, March 28, 2009, W3. See also McCullough, *How the Internet Happended*, 262.

30. "Number of Social Media Users Worldwide," June 2019, **https://www.statista.com/statisitcs/278414/number-of-worldwide-social-media-users**. See also McCullough, *How the Internet Happended*, 285–93.

31. Michael Malone, "The Twitter Revolution," *The Wall Street Journal*, April 18, 2009, A11.

32. Ibid.

33. Jonathan Mahler, “Who Spewed That Abuse? Yik Yak Isn’t Talking,” *The New York Times*, March 9, 2015, A1, B4.

34. Joe Palazzolo, “Law on Cyberbullying Challenged in Court,” *The Wall Street Journal*, June 5, 2014, A4.

35. Jennifer Preston, “Movement Began with Outrage and a Facebook Page,” *The New York Times*, June 27, 2011, A1.

36. Reed Albergotti, “Websites Wary of Facebook Tracking,” *The Wall Street Journal*, September 24, 2014, B1, B4.

37. Jeff Elder, “The Facebook Ads Teens Aren’t Supposed to See,” *The Wall Street Journal*, February 28, 2014, A1, A10.

38. Grep Ip, “The Antitrust Case against America’s Technology Behemoths,” *Wall Street Journal*, January 17, 2018, A1, A10.

39. Quoted in Howard Rheingold, *The Virtual Community: Homesteading on the Electronic Frontier* (Reading, MA: Addison-Wesley, 1993), 7.

40. Nicholas Negroponte, *Being Digital* (New York: Knopf, 1995), 12.

41. *America Banana Co. v. United Fruit Co*. 213 U.S. 347, 357(1909).

42. Jonathan Zittrain, “Be Careful What You Ask for: Reconciling a Global Internet and Local Law,” in *Who Rules the Net?*, eds. Adam Theirer and Clyde W. Crews (Washington, DC: Cato Institute, 2003).
43. Julie Cohen, “Between Truth and Power,” in *Information, Freedom, and Property*, ed. Mirielle Hildebrandt (New York: Routledge, 2016), 58–60.
44. “Regulating the Internet—The Consensus Machine,” *The Economist*, June 10, 2000, 73.
45. Mark Grabowski, “Should the U.S. Reclaim Control of the Internet? Evaluating ICANN’s Administrative Oversight Since the 2016 Handover,” *Nebraska Law Review*, August 6, 2018, **https://lawreview.unl.edu/downloads/grabowski/should-the-US-reclaim-control-of-the-Internet**.
46. Michel Foucault, *The History of Sexuality, Volume I*, trans. Robert Hurley (New York: Vintage Books, 1978), 95.
47. See Rebecca MacKinnon, *Consent of the Networked* (New York: Basic Books, 2012), 229–30.
48. David Streitfeld, “Changing the World, but not Quite the Way They Had Imagined,” *New*

York Times, November 13, 2017, A1, A11.

49. Victor Luckerson, "Here's Proof That Instagram Was One of the Smartest Acquisitions Ever," *Time*, April 19, 2016, 32–33.

50. Tim Wu, *The Curse of Bigness* (New York: Columbia Global Reports, 2018), 123.

51. "Everybody Wants to Rule the World," *The Economist*, November 20, 2014, 19–20.

52. Wu, *The Curse of Bigness*, 88.

53. Ip, "The Antitrust Case against America's Technology Behemoths," A1, A10. See also Jamie Condliffe, " Where Does Government Drew the Line," *New York Times*, March 18, 2019, B4.

54. Wu, *The Curse of Bigness*, 127–39.

55. Quoted in Felicity Barringer, "Internet Makes Dow Jones Open to Suit in Australia," *The New York Times*, December 11, 2002, C6.

56. *Dow Jones & Company, Inc. v. Gutnick* (2002) 194 A.L.R. 433, H.C.A. 56.

57. Zittrain, "Be Careful What You Ask For," 197.

58. Barringer, "Internet Makes Dow Jones Open to Suit in Australia," C6.

59. George Gilder, *Life After Google* (Washington, D.C.: Regnery, 2018), 30–32, 45. See also Thomas Catan and Amir Efrati,

"Feds to Launch Probe of Google," *The Wall Street Journal*, June 24, 2011, A1–2.

60. Rolfe Winkler, "Google Pushes Its Own Content," *Wall Street Journal*, August 19, 2014, B1, B5. See also Jack Nicas, "Google Roils Travel," *The Wall Street Journal*, December 27, 2011, A1.

61. Natalia Drozdiak and Sam Schechner, "EU Slaps Google with Record Fine," *Wall Street Journal*, June 28, 2017, A1–2.

62. Tom Fairless, "Europe Charges Google Over Searches," *The Wall Street Journal*, April 16, 2015, A1, A10. See also Brody Mullins, "FTC Staff Wanted to Sue Google," *Wall Street Journal*, March 20, 2015, A1–2 and Sam Schechner, "Google Appeals Record Fine," *Wall Street Journal*, October 10, 2018, B1.

63. William J. Richardson, *Heidegger: Through Phenomenology to Thought* (New York: Fordham University Press, 2003), 326. See also Gladden Pappin, "Liberty, Technology, and the Advent of Social Networking," *Intercollegiate Review* (Fall 2011): 39–47.

64. Benkler, Faris, and Roberts, *Network Propaganda*, 9.

65. Craig Silverman and Lawrence Alexander, "How Teens in the Balkans Are Duping Trump Supporters with Fake News,"

BuzzFeed.News, November 3, 2016, **https://www.buzzfeed.com/craigsilveman/how-macedonia-became-a-global-hub-for-protrump-misinfo**. See also Benkler, Faris, and Roberts, *Network Propaganda*, 9–10.

66. "Briefing: Social Media and Politics," *Economist*, November 4, 2017, 19. See also Benkler, Faris, and Roberts, *Network Propaganda*, 29–37.

67. Matthew Rosenberg and Gabriel Dance, "Affected Users Say Facebook Betrayed Them," *New York Times*, April 8, 2018, A1, A11. See also Evan Osmos, "Ghost in the Machine," *The New Yorker*, September 17, 2018, 35, and Benkler, Faris, and Roberts, *Network Propaganda,* 275–79.

68. Alexandra Stevenson, "Facebook Admits Role Platform Had in Fueling Violence in Myanmar," *New York Times*, November 7, 2018, B2. See also Osmos, "Ghost in the Machine," 42.

69. Osmos, "Ghost in the Machine," 43.

70. Mike Isaac, "After Zuckerberg' Invitation to Regulate Facebook, A Closer Look," *New York Times,* April 1, 2019, B3. See also Osmos, "Ghost in the Machine," 46–47 and "Social Media and Politics," 22.

ADDITIONAL RESOURCES

Abbate, Janet. *Inventing the Internet.* Cambridge, MA: MIT Press, 1999.

Benkler, Yochai, Robert Faris, and Hal Roberts. *Network Propaganda*. New York: Oxford University Press, 2018.

Borgmann, Christine. *From Gutenberg to the Global Information Infrastructure: Access to Information in the Networked World*. Cambridge, MA: MIT Press, 2000.

Castells, Manuel. *The Internet Galaxy*. New York: Oxford University Press, 2001.

Floridi, Luciano. *The 4th Revolution: How the Infosphere Is Reshaping Human Reality*. Oxford: Oxford University Press, 2014.

Galloway, Alexander. *Protocol: How Control Exists after Decentralization*. Cambridge, MA: MIT Press, 2004.

Galloway, Scott. *The Four: The Hidden DNA of Amazon, Apple, Facebook, and Google*. New York: Penguin, 2017.

Gilder, George. *Life After Google*. Washington, D.C.: Regnery, 2018.

Goldsmith, Jack, and Tim Wu. *Who Controls the Internet*? Oxford: Oxford University Press, 2008.

Hildebrandt, Mirielle, ed. *Information, Freedom, and Property*. New York: Routledge, 2016.

McCullough, Brian. *How the Internet Happened: From Netscape to the iPhone*. New York: W.W. Norton, 2018.

Naughton, John. *A Brief History of the Future*. New York: The Overlook Press, 1999.

Pasquale, Frank. *The Black Box Society*. Cambridge, MA: Harvard University Press, 2015.

Scheule, Rupert, Rafael Capurro, and Thomas Hausmanninger, eds. *Vernetz Gespalten: Der Digital Divide in Ethischer Perspektive*. München: Wilhelm Fink Verlag, 2004.

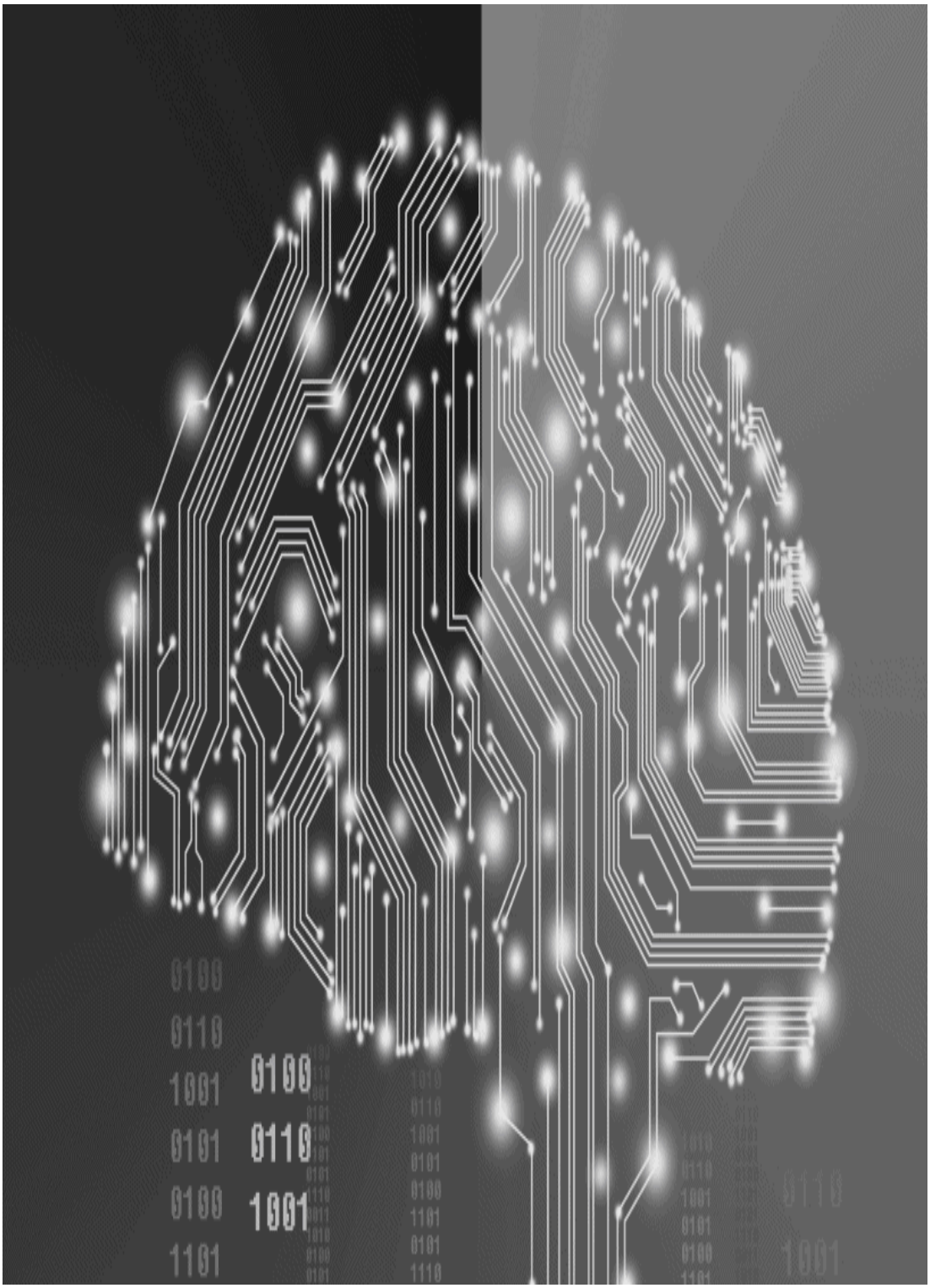
Spinello, Richard. *Regulating Cyberspace: The Policies and Technologies of Control*. Westport, CT: Quorum Books, 2002.

Vaidhyanathan, Siva. *The Googlization of Everything*. Berkeley: University of California Press, 2011.

Wallach, Wendell. *A Dangerous Master: How to Keep Technology from Slipping Beyond Our Control*. New York: Basic Books, 2015.

Wu, Tim. *The Curse of Bigness*. New York: Columbia Global Reports, 2018.

Zittrain, Jonathan. *The Future of the Internet*. New Haven, CT: Yale University Press, 2008.



CHAPTER 3

Free Speech and Censorship in Cyberspace

During its early history the internet was widely perceived as a “technology of freedom,” because of its capacity to effectively expand freedom of expression beyond the political and media elites. That perception has largely remained in effect since users can still disseminate their own blogs, create a home page on Facebook, or even initiate their own Twitter service. No longer do people have to rely solely on the mainstream media ecosystem as purveyors of information. As the Supreme Court eloquently wrote in its *Reno v. ACLU* (1997) decision, the internet enables an ordinary citizen to become “a pamphleteer . . . a town crier with a voice that resonates farther than it could from any soapbox.”[1] The internet clearly has the power to enhance political and social self-determination by opening up a plurality of new communication venues.

However, as Julie Cohen points out, this utopian vision assumes an egalitarianism and an absence of power asymmetries. It overlooks the scope and capabilities of social media platforms and government regulators who have ample means to shut down free speech for content that doesn’t fit prescribed norms. The use of software code designed to censor information gives both government and private actors considerable regulatory leverage. In addition, information technology companies have typically complied

with the demands of repressive governments like China to censor objectionable content.[2]

As a result, the issue of free speech and its regulation by both the public and private sectors persists as a contentious moral problem in the infosphere. To be sure, there are valid concerns about fringe elements of expression, like pornography, venomous hate speech, or the promotion of terrorism. Speech is not an absolute right and under certain conditions there are justifiable reasons for its curtailment when it conflicts with other fundamental rights. But some forms of censorship, even in democracies like the United States, come dangerously close to negating freedom of thought and expression, a fundamental natural right. Free speech is not only a basic right but also an indispensable social good that promotes a diversity of perspectives and serves as a restraint on government and corporate abuses of power.

In addition, while free speech is an important issue for its own sake, speech-related issues are often at the root of other major ethical and public policy problems in cyberspace, including privacy, intellectual property, and security. We will return to these issues as we further pursue the subject of free speech, but it is instructive at this point to consider how they are interconnected.

The European Union's law that forces Google to delete "irrelevant" links or references to a person's past misconduct to preserve their reputation was motivated by the desire to fortify privacy protection. However, this "right to be forgotten" collides with free speech rights. Many newspaper accounts about criminal conduct, investigations, and judicial proceedings have been deleted thanks to this law. But as

Abrams points out, it is not a trivial matter for a government to “criminalize the dissemination of truthful information” in the news media.[3] Intellectual property rights can also be construed as restrictions on free speech. If someone has property rights to a trademark, others cannot use that form of expression freely and openly. And finally, chats and messages expressed in forums such as WhatsApp are protected by unbreakable, end-to-end encryption. But strong encryption in the wrong hands could be a threat to national security, and hence many argue that encryption needs to be subject to government oversight. Thus, many of the intractable and publicized difficulties in cyberspace can be reduced to the following question: What is the appropriate scope of free expression for organizations and individuals and by what methods can that speech be protected?

Many who pioneered internet technology have consistently asserted that the right to free expression in cyberspace should have as broad a scope as possible. They argue for unrestricted access to all forms of speech in cyberspace. For many years, there was also considerable reluctance on the part of the government to restrict or filter any form of information on the network for fear of stifling an atmosphere that thrives on the free and open exchange of ideas.

But the expanded use of the internet, especially among more vulnerable segments of the population such as young children, has forced some public policy makers to rethink this laissez-faire approach. In the United States, the result has been several futile attempts to control pornographic or lewd content through poorly crafted legislation. Other countries have also entered the fray, seeking to impose tight restrictions on hate speech. Yet to allow the government to determine whose speech will be heard brings us into

dangerous territory and potentially threatens the foundation of democracy.

In this chapter, we focus primarily on those problematic forms of free expression, well known to anyone who has surfed the web, that trigger the ire of censors, both in the public and private sectors. They include pornography, hate speech, virtual threats made on platforms such as Facebook, and terrorist propaganda. In the context of this discussion, we consider whether the libertarian ethic favoring broad free speech rights still has validity despite the proliferation of offensive online content. A related theme is cyber authoritarianism and the social implications of local sovereigns regulating content based on ideology.

Speech and Internet Architecture

Content controls and censorship are alien to the original design of the internet. Thanks to the Transmission Control Protocol/Internet Protocol (TCP/IP), the internet has been designed to transmit packaged bits of information indiscriminately from one location to another. Routers and intermediate servers that support and transmit these information packets pay no attention to the enclosed content—they simply forward along a compressed packet of anonymous 1s and 0s.

Furthermore, these bits are being transported to an IP address that could be anywhere in the world. Territorial borders and boundaries are irrelevant. The internet is oblivious to geography as it mechanically transmits digital data to the destination denoted by the numeric IP address. Hence the internet's ability to "cross borders, break down barriers, and destroy distance" is often singled out as one of its most remarkable features.[4]

It becomes clear that this distinctive architecture of the Net is wholly consistent with an expansive and robust conception of free speech rights. This network has been constructed so that anyone can

send any form of digital content to any location throughout the world without interference. The Net's code supports and protects a highly libertarian ethos that gives primacy to the individual speaker.

It is also significant, of course, that this architectural design has its roots in the United States, where the Net was invented and nurtured for many years. It is not surprising that Americans committed to broad free speech ideals would construct a network that embodies this philosophy. As Lessig remarks, "We have exported to the world, through the architecture of the internet, a First Amendment in code more extreme than our own First Amendment in *law*" (emphasis in original).[5]

But what code "giveth," code can take away. Technologies are not fixed and immutable, and therefore neither is the nature of cyberspace. The internet's plasticity means that its architecture is always subject to modification. Filters, firewalls, and geolocation software, which can differentiate between users of different countries, have complicated and obscured the Net's original, simple architecture. As the Net's architecture changes, it no longer appears to be beyond the control of local sovereigns and other regulatory forces. Code itself, such as country-level fire walls,

can breathe new life into territorial sovereignty. Perhaps all of this has the force of inevitability, but is it a good idea? Should the internet, too, have borders? As we ponder this question, let us turn to how the United States has sought to control content by outlawing bits of data that are pornographic.

Pornography in Cyberspace

Before we discuss the U.S. Congress's efforts to regulate internet speech, we should be clear about legal standards pertaining to pornographic and obscene speech. Obscene speech is completely unprotected by the First Amendment and is banned for everyone. In *Miller v. California* (1973) the Supreme Court established a three-part test to determine whether or not speech falls in the category of obscenity. To meet this test, speech had to satisfy the following conditions: (1) it depicts sexual (or excretory) acts explicitly prohibited by state law; (2) it appeals to prurient interests as judged by a reasonable person using community standards; and (3) it has no serious literary, artistic, social, political, or scientific value. Child pornography that depicts children engaged in sexual activity is also illegal under all circumstances.

Pornography, that is, sexually explicit speech excluding obscene speech and child pornography, can be regulated and banned, but only for minors. The relevant legal case is *Ginsberg v. New York*, which upheld New York's law banning the sale of speech "harmful to minors" to anyone under the age of 17. The law in dispute in the Ginsberg case

defined “harmful to minors” as follows: “that quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, when it: (1) predominantly appeals to the prurient, shameful, or morbid interests of minors, and (2) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors, and (3) is utterly without redeeming social importance for minors.”[6]

Although state legislatures have applied this case differently to their statutes prohibiting the sale of material harmful to minors, these criteria can serve as a general guide to what we classify as *Ginsberg speech*, which is considered off limits to children under the age of 17.

Public Policy Overview

The Communications Decency Act

The pervasive presence of obscene and pornographic speech on the internet is a challenge for lawmakers. As the quantity of communications grows in the realm of cyberspace there is a much greater likelihood that people will become exposed to forms of speech or images that are offensive and potentially harmful. By some estimates, the internet has over 100,000 sites offering illegal child pornography, while monthly pornography downloads amount to 1.5 billion.[7] Hence the understandable impulse of governments to regulate and control this form of free expression on the internet in order to contain its negative side effects. The Communications Decency Act (CDA) represented one such futile, and some say misguided, attempt at such regulation.

The CDA included several key provisions that restricted the distribution of sexually explicit material to children. It imposed criminal penalties on anyone who "initiates the transmission of any communication which is . . . indecent, knowing that the recipient of the communication is under 18 years of age." It also criminalized the display of patently offensive sexual material "in a manner available to a person under 18 years of age."[8]

Defenders of the CDA contended that this was an appropriate way of channeling pornographic or

Ginsberg speech on the internet away from children. It did not seek to ban adults from viewing such speech. Rather, it was an attempt to zone the internet just as we zone physical environments. According to one supportive brief: “The CDA is simply a zoning ordinance for the Internet, drawn with sensitivity to the constitutional parameters the Court has refined for such regulation. The Act grants categorical defenses to those who reasonably safeguard indecent material from innocent children—who have no constitutional right to see it—channeling such material to zones of the Internet to which adults are welcome but to which minors do not have ready access.”[9] What this brief is referring to is an “out” for internet speakers provided by the CDA: if they took “reasonably effective” measures to screen out children, they could transmit indecent material.

Support for the CDA was thin, however, and it was quickly overwhelmed by strident and concerted opposition. An alliance of internet users, internet service providers (ISPs), and civil libertarian groups challenged the legislation as a blatant violation of the First Amendment right of free speech. This coalition was spearheaded by the American Civil Liberties Union (ACLU) and the case became known as *Reno v. ACLU*.

There were obvious problems with the CDA that the plaintiffs in that lawsuit immediately seized on. The most egregious weakness was that this law might cast the net of censorship too far by including works of art and literature and maybe even health-related or sex education information. The category of indecent speech was not well defined by Congress and could include forms of speech that went beyond Ginsberg speech. The law was also vague. What did it mean to take "reasonably effective" measures to screen out children? According to Lessig, "The architectures that existed at the time for screening out children were relatively crude, and in some cases, quite expensive. It was unclear whether, to satisfy the statute, they had to be extremely effective or just reasonably effective given the state of the technology."[10]

Also, of course, even if the CDA were enacted it would have a limited impact on the availability of pornography in cyberspace. It could not control sexual content on the internet originating in other countries, nor could it halt pornography placed on the internet by anonymous remailers, which are usually located off shore and beyond the reach of U.S. regulators. The bottom line is that because the internet is a global network, localized content restrictions enacted by a single national

government to protect children from indecent material would not be fully effective.

A panel of federal judges in Philadelphia ruled unanimously that the CDA was a violation of the First and Fifth Amendments. The three-judge panel concluded that “just as the strength of the Internet is chaos, so the strength of our liberty depends upon the chaos and cacophony of the unfettered speech the First Amendment protects.”[11] The Justice Department appealed the case, which then became known as *Reno v. ACLU*, but to no avail. The Supreme Court agreed with the lower court’s ruling, and in June 1997, declared that this federal law was unconstitutional. The court was especially concerned about the vagueness of this content-based regulation of speech. According to the majority opinion written by Justice Stevens, “We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another.”[12] Stevens also held that the free expression on the internet is entitled to the highest level of First Amendment protection. This is in contrast to the more limited protections for

other more pervasive media such as radio and broadcast and cable television where the court has allowed government-imposed censorship. In making this important distinction, the court assumes that computer users have to actively seek out offensive material, whereas they are more likely to encounter it accidentally on television or radio if it were so available.

Children's Online Protection Act

Most of those involved in the defeat of the CDA realized that the issue would not soon go away. Congress, still supported by public opinion, was sure to try again. And in October 1998, they did try again, passing an omnibus budget package that included the Child Online Protection Act (COPA), a successor to the original CDA, which became known in legal circles as "CDA II." The law was signed by President Clinton and, like its predecessor, it was immediately challenged by the ACLU. CDA II would make it illegal for the operators of commercial websites to make sexually explicit materials harmful to minors available to those under 17 years of age. Commercial website operators would be required to collect an identification code, such as a credit card number, as proof of age before allowing viewers access to such material.

The ACLU and other opponents claimed that the law would lead to excessive self-censorship. CDA II would have a negative impact on the ability of these commercial websites to reach an adult audience. According to Max Hailperin, "There is no question that the COPA impairs commercial speakers' ability to cheaply, easily, and broadly communicate material to adults that is constitutionally protected as to the adults

(nonobscene), though harmful to minors."[13] This law was more narrowly focused than CDA I; it attempts to define objectionable sexual content more carefully. Such content would lack "serious literary, artistic, political or scientific value" for those under the age of 17. But the law's critics contend that it is still worded too broadly. Those critics worried about what would happen if the law were arbitrarily or carelessly applied. Would some sites offering sexual education information, for instance, be accused of violating the law? Also, it could be plausibly argued that there is a problem in requiring adults to present identification to exercise their right to access speech that is protected by the First Amendment.

In February 1999, a federal judge in Philadelphia issued a preliminary injunction against COPA, preventing it from going into effect. This judge accepted the argument that the law would lead to self-censorship and that "such a chilling effect could result in the censoring of constitutionally protected speech, which constitutes an irreparable harm to the plaintiffs."[14] The ACLU won its case in Federal District Court in Philadelphia and in the U.S. Court of Appeals for the Third Circuit. In 2002, the U.S. Supreme Court remanded the case to the Third Circuit, which again found COPA unconstitutional because it did not satisfy the First

Amendment's "least restrictive means" test. But the case, now called *Ashcroft v. ACLU*, was appealed once again to the Supreme Court. That court decided in 2004 to keep in place the district court's order blocking the enforcement of COPA.[15] The Supreme Court concluded that COPA could inadvertently prevent adults from accessing legal pornography online and that minors could be adequately protected by internet filtering software.

Children’s Internet Protection Act

Despite these defeats, Congress did not abandon its efforts to contain the spread of pornography in cyberspace. This time the legislative effort was led by Senator John McCain, who worked ardently to pass the Children’s Internet Protection Act (CIPA). This bill was signed into law on December 21, 2000, by President Clinton and it took effect in April 2001. It represented a decisive change in the government’s strategy. This time the government hoped to rely on private surrogates, libraries, and schools to regulate speech harmful to minors through the use of filters that block out objectionable content. This law was linked to the federal government’s E-rate program, which provided an opportunity for schools and libraries to be reimbursed for the costs of connecting to the internet or to be subsidized for other telecommunications expenses. The law mandated that, for libraries seeking these funds, computer terminals used by all library patrons (i.e., adults and children) must have filters that block internet access to visual images that are obscene or involve any sort of child pornography. In addition, according to Kaplan, “For library computer terminals used by children under 17, libraries have to screen out these two categories of material plus a third one: visual material that is ‘harmful to

minors,' such as sexually explicit images without social or educational value that are obscene for children but legally protected for adults."[16] Public schools seeking E-funds were required to implement the same type of filtering scheme. The blocking mechanism may be overridden for valid research purposes.

Like its predecessors, CIPA was immediately challenged by libraries, educational leaders, and civil libertarians. In April 2001, a group of libraries and library associations (including Multnomah County Public Library, the Connecticut Library Association, the Maine Library Association, and the Santa Cruz Public Library Joint Powers Authority) filed a lawsuit against this legislation. This suit, *Multnomah Public Library et al. v. U.S.*, was filed in the U.S. District Court for the Eastern District of Pennsylvania where other prominent free speech cases have been heard. The suit argued that CIPA was unconstitutional: "By forcing public libraries to install such technology, CIPA will suppress ideas and viewpoints that are constitutionally protected from reaching willing patrons. CIPA thus imposes a prior restraint on protected speech in violation of the Constitution."[17] The suit also contended that CIPA was "arbitrary and irrational because existing technology fails to block access to much speech that Congress

intended to block, and thus will not protect library patrons from objectionable content."[18] Blocking mechanisms simply cannot block all speech that is obscene, child pornographic, and harmful to minors.

In the summer of 2002, a federal judicial panel of the U.S. District Court for the Third Circuit struck down the law. The court concluded that sections of this law were "invalid under the First Amendment." The government appealed the case to the Supreme Court, and in June 2003 that court vacated the district court's ruling and upheld CIPA. In its 6–3 decision the Supreme Court concluded that limitations imposed by CIPA on internet access were equivalent to limitations on access to books that librarians choose to acquire or not acquire. There was consensus that filters are inaccurate instruments for restricting the access of children to pornographic material, because those filters sometimes block sites that adults have a right to see. Nonetheless, the majority of the Supreme Court concluded that First Amendment rights were not being infringed by this law, as long as adults could request that the filters be disabled without unnecessary delay.

The CIPA statute, now the law of the land in the United States, reframed the debate about the government role in regulating the internet; the

government shifted its strategy from direct to indirect regulation, relying on the private sector to do the work of curbing pornography. But should the government offer private parties this *quid pro quo* for their role in censoring the internet because more direct regulatory efforts seem to be unconstitutional? The *Multnomah* case challenging CIPA also explicitly questioned the efficacy of using filtering technology (or code) to resolve the pornography problem. Is the negative appraisal of code put forward by the plaintiffs in this case an accurate one, or can code be a viable part of the solution? With that question in mind, we turn to a more in-depth discussion of the deployment of filtering architectures in cyberspace.

Automating Content Controls

At the heart of the debate about the CDA and content regulation is the basic question that was raised in **Chapter 2** about how the internet should be regulated. Should government impose the kind of central controls embodied in legislation such as the CDA and COPA? Or should the internet be managed and controlled primarily through code, installed at the discretion of individuals or private institutions? The latter approach would decentralize content controls so that people can develop their own solutions to offensive speech tailored to their own needs and value systems.

Thanks to the rulings against CDA and COPA, the burden of content control has shifted to parents and local organizations like schools and libraries. But the exercise of this bottom-up exertion of power has caused some anxiety due to the potential for abuse. To what extent should local communities and institutions (e.g., schools, prisons, libraries) assume direct responsibility for controlling content on the internet? Aside from the demands of CIPA, libraries must consider whether it is appropriate to use filtering software to protect young patrons from pornography on the internet. Is this a useful and prudent way to uphold local community or institutional standards? Or does this

sort of censorship compromise a library's traditional commitment to the free flow of ideas?

There are two broad areas of concern about the use of content controls that need elaboration. The first area involves the social and moral probity of censorship itself, even when it is directed at the young. There is a growing tendency to recognize a broad spectrum of rights, even for children, and to criticize parents, educators, and politicians who are more interested in imposing their value systems on others than in protecting vulnerable children. Jonathan Katz and other advocates of children's rights oppose censorship even within a private household, unless it is part of a mutually agreed upon social contract between parent and child. According to Katz, "Parents who thoughtlessly ban access to online culture or lyrics they don't like or understand, or who exaggerate and distort the dangers of violent and pornographic imagery, are acting out of arrogance, imposing brute authority."[19] Rather, Katz contends, young people have a right to the culture that they are creating and shaping. The ACLU seems to concur with this position and it too advocates against censorship as a violation of children's rights.

Lurking in the background of this debate is the question of whether or not children have a First

Amendment right to access indecent materials. There is no consensus about this among legal scholars, but if children do have such a right it would be more difficult to justify filtering out indecent materials in libraries or educational institutions. One school of thought about this issue is that a child's free speech rights should be proportionate to his or her age. The older the child, the more questionable are restrictions on indecent material.

The second area of concern pertains to the efficacy of the blocking methods and other automated controls used to accomplish this censorship. Popular blocking programs have included Cyber Patrol, N2H2 Internet Filtering, Websense Enterprise, and SmartFilter. These programs generally function by using categories of objectionable speech. Categories might include Adult/Sexually Explicit, Nudity, Pornography, and so forth. Websense Enterprise uses 75 categories, but that seems to be higher than the norm.[20] Once the categories are established, filtering companies use automated programs (including robots) to examine websites and determine candidates for each category. For example, after a bot visits the **penthouse.com** website to search for key words, the program might classify this site as "Adults Only/Pornography." For the most part the

categorization is made without human intervention, but sometimes human reviewers might make the final determination. The extent of human intervention in this process varies from company to company. If a parent installs a filtering program like N2H2 with categories such as “Adults Only/Pornography” activated, anyone trying to access the **penthouse.com** site is prevented from doing so by the software.

There are several conspicuous problems with the utilization of blocking software. The first problem is the unreliability and lack of precision that typifies some of these products—there are no perfect or foolproof devices for filtering out obscene or pornographic material. Sometimes automated programs make mistakes and this leads to over blocking, that is, filtering out sites that do not fit a particular category. For example, a report on SmartFilter exposed apparent *over blocking*, pointing out that “it blocked WrestlePages (‘The best source for wrestling news’); **MotoWorld.com**, a motorcycle sport magazine produced by ESPN; and Affirmation: Gay and Lesbian Mormons, a support site.”[21] On other occasions the problem could be under blocking, failing to find a pornographic site and leaving it off the list. Given the density and volatility of the web, this lack of precision should not be particularly surprising.

Whether these incongruities can be overcome by better software products is a matter of some dispute.

Another problem is that these blocking programs are not always transparent, and they can be furtively employed to enforce a code of political correctness or advance a social agenda, unbeknownst to parents or librarians who choose to install them. Sites that discuss AIDS, homosexuality, and related topics have been blocked by certain filtering programs, either deliberately or accidentally. Sometimes these programs are not explicit or forthright about their blocking criteria, which greatly compounds this problem.

Finally, a potential disadvantage of filtering software is that the filter can be imposed at any level in the vertical hierarchy that controls the accessibility of internet services. It can be invoked at the individual user level, the corporate or institutional level, or the ISP level. Saudi Arabia, China, Singapore, and a host of other countries have put into effect country-wide filtering systems by blocking content, usually at the level of the destination ISP, a major point of control for state intervention. In Saudi Arabia, all internet traffic is routed through a proxy server that restricts website access based on filtering criteria determined by

the state. The blocked sites include pornographic sites along with those that might offend the cultural or religious beliefs of Saudi citizens. This material includes content critical of the Islamic religion and political discourse critical of the Saudi regime. Political dissent is not welcome in Saudi Arabia, and government officials wanted to be sure that the web would not provide a new forum for fomenting such dissent.

The adoption of filtering technologies is a striking example of how “code” has become a substitute for law as a constraint on cyberspace behavior. Thanks to the nullification of the CDA, internet stakeholders in increasing numbers will resort to software that may be far more effective than the law in suppressing pornographic material.

Although we take no position on the merits of automated controls, we contend that the developers and users of code as a method of dealing with cyberporn should deploy this software responsibly to minimize any potential for collateral damage. If this code is designed, written, and used prudently, it can protect innocent children without threatening individual liberties or the common good.

What constitutes responsible use of these automated controls? First, the use of these

controls should be strictly voluntary—parents or schools should be allowed to choose whether or not to restrict web content. In contrast, a mandatory rating or filtering system administered or sponsored by the government would be imprudent and probably counterproductive. It would impose a uniform solution to what is arguably a local problem. Thus, automated controls should not be adopted as a high-level centralized solution to harmful speech. Filtering should occur only at the lowest levels, at the points of control exercised by individuals, schools, or libraries. Second, there should be an adequate transparency level in blocking software or rating schemes. Although some information may be proprietary, software companies must be as open as possible about their filtering criteria and methodologies.

Even if automated content controls are used responsibly and diligently, their use still raises some troubling questions. For example, which local institutions should assume the burden of implementing filtering technologies? What about the use of filtering devices in libraries that provide internet access? Both public and private libraries face a real dilemma: they can either allow unfettered internet access, even to their youngest

patrons, or use filtering products to protect minors from pornographic material.

Those libraries that favor the first approach argue that the use of filtering devices compromises the library's traditional commitment to the free flow of information and ideas. Some of this opposition to these filtering devices originates from the imprecise way in which they function. The public library in New York City subscribes to this philosophy and presently does not employ filtering devices. The Connecticut Library Association has articulated support for "the principle of open, free and unrestricted access to information and ideas, regardless of the format in which they appear."[22] Further, the American Library Association (ALA) is opposed to the installation of filters and endorses the idea of unrestricted internet access for both adults and minors.

A number of librarians, however, disagree with the ALA. They maintain that the internet should be censored and that filtering programs provide a way to support and reinforce local community values. According to Brenda Branch, the director of the Austin Public Library in Texas, "We have a responsibility to uphold the community standard. . . . We do not put pornographic material in our book collection or video collection, and I also don't feel

we should allow pornographic materials in over the Internet."[23]

Some libraries have a strict censorship policy that applies to both adults and minors. Others install filtering devices on children's computers but not on those in the adult areas. But the ALA and the ACLU do not favor this type of zoning strategy. Nor do libertarian groups like the American Civil Liberties Union (ACLU). As the result of an ACLU lawsuit, the library system in Kern County, California was forced to abandon such a zoning plan and to give all of its patrons, including minors, the right to use a computer without a filter. Moreover, this solution contradicts Article 5 of the ALA's Library Bill of Rights: "A person's right to use a library should not be denied or abridged because of origin, age, background, or views."[24] According to the ALA, fidelity to this principle would preclude the use of filters on any computer systems within a library.

Opponents of filtering also argue that schools and libraries which attempt to educate students and young patrons about internet use and abuse should rely on trust rather than censorship. As Richard Rosenberg argues, "If the first instinct is to withhold, to restrict, to prevent access, what is the message being promulgated?"[25] If institutions like

schools and libraries truly value the ideals of trust, openness, and freedom, imposing censorship on information is a bad idea that mocks those ideals.

But should all information be freely accessible to anyone who wants it (including children)? Is this a morally reasonable policy? What are the costs of living in a society, that virtually absolutizes the right to free speech in cyberspace and makes all forms of speech readily available even to its youngest members? Because these costs can be quite high, it is critically important to consider the other side of this issue.

Many responsible moralists contend that some carefully formulated, narrow restrictions on specific types of indecent speech are perfectly appropriate when young children are involved. They maintain that parents, schools, libraries, and other local institutions have an obligation to promote and safeguard their own values as well as the values of their respective communities. This is part of the more general obligation to help promote public morality and the public order. Freedom and free expression are fundamental human rights, but these and other rights can only be reasonably exercised in a context of mutual respect and common acceptance of certain moral norms, which are often referred to as the *public morality*. In any civilized society, some of these norms

prescribe how people, especially children, should conduct themselves sexually. Given the power of sexuality in one's life, the need for carefully integrating sexuality into one's personality, and the unfortunate tendency to regard others as sexual objects of desire (rather than as human persons), there is a convincing reason for fostering a climate where impressionable children can be raised and nurtured without being subjected to images of gross or violent sexual conduct that totally depersonalize sexuality, exalt deviant sexual behavior, and thereby distort the view of responsible sexual behavior. This is clearly an aspect of the common good and public morality and is recognized as such by public officials in diverse societies who have crafted many laws (such as the law against the production of child pornography) to protect minors and to limit the exercise of rights in this area. Hence, given the importance of protecting young children as best as we can from psychologically harmful pornographic images, parents and those institutions that function in *loco parentis* should not be timid about carefully controlling internet content when necessary.[26]

It is never easy to advocate censorship at any level of society precisely because the right to free expression is so valuable and cherished. But proponents of content controls for pornography

argue that most human rights, including the right to free expression, are limited by each other and by aspects of the common good that in this context are captured by a term like “public health.” According to this perspective, parents, libraries, and schools are acting prudently when they choose to responsibly implement filtering technologies to help preserve and promote the values of respect for others and appropriate sexual conduct, which are part of our public morality. Preserving free speech and dealing with sexually explicit material will always be a problem in a free and pluralistic society, and this is one way of achieving a proper balance when the psychological health of young children is at stake.

New Censors and Controversies

Cyberspace pornography does not get the media attention it once did when the internet was still a relatively novel phenomenon. In the United States, legislative battles have faded away after the government's modest victory with its CIPA legislation. But the issue has not gone away, as attention is now focused on the availability of porn for mobile devices and the need to control the distribution of violent video games to minors. There remains a massive amount of pornography in cyberspace and some say the computer business itself is really built on porn. That may be hyperbole, but as more people buy iPads and iPhones there is an obvious demand for a wide variety of adult entertainment apps for these devices.

However, Apple has censored these apps much to the dismay of some libertarians. Apple restricts the apps available in its app store to nonpornographic content. Steve Jobs once boasted that the app store was based on the principle of "freedom from porn." Apple's app censorship also extends to online content that is made available on its devices for a fee, such as magazines and newspapers. Apple censored an iPad app for an issue of Germany's *Stern* magazine because it published nude photos and other erotic content that could be

displayed on the iPad.[27] Apple realizes that people will continue to access adult entertainment websites through their browsers, but the company is trying to avoid the direct distribution of that entertainment through their own app store. Apple's decision seems based on a moral conviction about the unsuitability of this material for minors, but it may also be sound economics. Apple may sell more apps to children if parents don't have to worry that they will be purchasing X-rated content at the app store.

In addition to worries about porn for mobile devices, there is escalating concern about the violent content of video games, which are increasingly played with others over the internet. Some video game makers are introducing technology that streams games to internet-connected devices. States like California have sought to regulate these games in the face of strong opposition from the gaming industry and civil libertarians. The primary issue is violent and sadistic imagery, which is a different form of pornography. However, some games feature assaults with sexual overtones, which appeals to the prurient and deviant interests of young adults. Also, feminists are rightly concerned about the sexual stereotypes found in many games, which are played mostly by men.

A key question in this case is whether the same First Amendment protection that extends to books and movies also extends to video games. Latent in the video game debate about censorship and free speech is the more general concern about playing ultra-violent video games. Some philosophers and psychologists convincingly argue that playing these vivid games incessantly cultivates insensitivity to human suffering and a lack of empathy. Hence, this form of play potentially interferes with the development of one's sound moral character. Others have dismissed these concerns, observing that minors' attraction to violent entertainment (including Saturday morning cartoons) is nothing new.

In the Supreme Court case of *Brown v. Entertainment Merchants Association*, the justices ruled against California's regulations forbidding the sale of violent video games to minors. The Court held that video games qualify for First Amendment protection. The reasoning of the majority was simple enough: games communicate ideas and government lacks the power "to restrict expression because of its message, ideas, subject matter or content." Thus, despite the potential dangers of frequent exposure to these ultra-violent video games, the Court determined that children have every right to purchase and play these games.[28]

Hate Speech

The rapid expansion of hate or extremist speech on the web raises similar polemical disputes. Many groups such as white supremacists and anarchists have websites that advocate their extremist viewpoints. Some of these sites are blatantly anti-Semitic. They disparage the Jewish religion or make preposterous claims that the Holocaust never happened. Other sites take aim at religions like Islam. On occasion, these sites can be especially virulent and outrageous, such as the website of the Charlemagne Hammerskins. One scene reveals a man disguised in a ski mask bearing a gun and standing next to a swastika.

Social media has become rife with various forms of hate speech along with borderline offensive speech that deals with the themes of race and ethnicity. Twitter, which is committed to openness and free speech, has helped many bottom-up movements like Black Lives Matter and the Tea Party to mobilize their members. But it has also become a popular venue for expressing hate speech. One series of anti-Semitic tweets by a pseudonymous account attacked Judaism and showed a series of lampshades with the caption, “This is your family when Trump wins. Get your

Israel passport ready." Some hate speech is linked with the promotion of terrorism. In the infamous Easter attack in Sri Lanka by a radical, anti-Christian Muslim group, Facebook postings revealed an escalation from contempt for Christians to a call for bombings at Christian churches. Despite repeated complaints from the broader Muslim community, Facebook did not remove the controversial postings.[29]

What can be done about this growing subculture of hate and extremism on the internet? The great danger is that the message of hate and bigotry, once confined to reclusive, powerless groups, can now flow unimpeded throughout the online terrain. Unlike obscenity and libel, hate speech is not illegal under U.S. federal law and it is fully protected by the First Amendment. This protection was recently reaffirmed by the U.S. Supreme Court which decided 8–1 that the graphic "hate speech" (e.g., "God hates fags"; "Pope in Hell"; "Thank God for 9/11") by Westboro Baptists at military funerals was protected by the First Amendment. According to Chief Justice Roberts, who wrote the majority opinion, "Such speech cannot be restricted simply because it is upsetting or arouses contempt." The decision was not without controversy since it put the United States

at one extreme on the global spectrum for hate speech protection.[30]

On the other hand, in European countries like Germany and France, anti-Semitic, Nazi-oriented websites are illegal, along with other forms of hate speech. In Germany, the government has required ISPs to eliminate these sites under the threat of prosecution. Critics of this approach argue that it is beyond the capability of ISPs to control content in such a vast region as the World Wide Web. It is also illegal for internet companies located in other countries to make available Nazi materials in Germany. American companies have tried to be as accommodating as possible. For example, **Amazon.com** no longer sells copies of Hitler's autobiography, *Mein Kampf*, to its German customers, that is, customers who access the German-language site.

Hate speech can be dealt with through the same methods used to control pornography, especially law and code. Some sovereignties, like France and Germany, prefer regulation and explicit laws that forbid most forms of hateful or extremist speech. There is always the problem of regulatory arbitrage, however. Some extremist site servers have relocated to the United States or other countries, where those laws do not apply. An alternative to government regulation is greater

reliance on user empowerment through code. Hate speech can usually be suppressed through responsible filtering that does not inadvertently exclude valid forms of political speech. Given the limitations of the law, parents and certain private and religious institutions can turn to technology to shield young children and sensitive individuals from some of this offensive material.

Social media platforms are not required under the First Amendment to protect the speech of their users since they are not government entities. Also, thanks to section 230 of the Communications Decency Act, online platforms have immunity from legal liability for user-generated content. Nonetheless these platforms seek to target extremist or abusive speech for the safety and welfare of their user base. The “Twitter Rules,” for example, prohibit abusive behavior by Twitter users as well as “hateful conduct.” The process of removing extremist content including hate speech is known as commercial content moderation. It usually relies on “community policing,” with users of a service such as Twitter flagging a certain piece of content that they believe is in violation of the rules. Some platforms utilize a process of “automatic flagging” by which their own proprietary tools identify extremist content that violates their rules. Once identified, the content is then

subjected to a human reviewer before a final determination is made.[31]

But how can these platforms identify which forms of speech should be targeted and singled out as examples of “hateful conduct” or extremism? Can hate speech be properly defined in order to avoid arbitrary and subjective decisions? And what separates real hate speech from speech that is politically incorrect and perhaps only borders on being offensive? It is difficult for Google or Twitter algorithms and also for human censors to make these distinctions. While a comprehensive definition of hate speech is difficult to formulate, Andrew Sellars proposes the main common traits of hate speech that should help establish the parameters of censorship:

1. Targeting of a Group, or individual as a member of a Group (race, ethnicity, and religion appear most frequently)
2. Content in the message that expresses hatred (e.g., speech that promotes “racial inferiority” or denies the dignity of target group members)
3. The speech causes harm (especially speech that seeks to induce physical violence or terrorism)

4. The speech incites bad actions beyond the speech itself
5. The context makes violent response possible
6. The speech has no redeeming purpose (i.e., the speech has no relevance or social value that goes beyond the expression of hatred toward another group).

Questions remain, of course, about how best to put this framework into practice so that speech restrictions are warranted and not based on arbitrary standards or political bias. The challenge for private censors, such as Twitter and Facebook, is to handle hate speech in an objective manner by applying these or similar norms as prudently and fairly as possible.[32]

Online Threats

Sometimes extremist speech that incites hatred can take the form of a threat, and threats are generally not protected by the First Amendment. However, differentiating a threat from constitutionally protected hate speech is no easy matter. Consider the case of the “Nuremberg Files” website, which was the product of the American Coalition of Life Activists (ACLA), a fringe antiabortion group that appeared to advocate the use of violent tactics against abortion providers. Doctors who provided abortions were listed on the website and they were declared to be guilty of crimes against humanity. In addition, the names of murdered doctors were crossed out, and the names of those doctors who had been wounded were printed in gray.

The website was replete with radical antiabortion statements and it included links to other antiabortion sites that defended the murder of abortion providers as morally justified. There was also a call for information about abortion providers to assist in collecting dossiers on abortionists to hold them accountable until abortion was declared illegal. The site’s imagery was also gruesome with images of dripping blood and aborted fetuses.

Planned Parenthood filed suit against the ACLA, the operators of this site. They argued that the material on this website (along with other activities of the ACLA) violated a 1994 law called the Federal Freedom of Access to Clinics Entrances Act, which makes it illegal to use “force or threat of force” against those who provide or seek out abortions. Lawyers representing the ACLA argued that there was no explicit advocacy of violence. In 1999, a jury ruled in favor of the plaintiffs and demanded that ACLA pay a fine of $100 million. However, in March 2001, the Ninth Circuit Court of Appeals overturned this decision on the basis that this speech was protected by the First Amendment. According to the appeals court ruling, the defendants did not threaten to commit violent acts, but only encouraged such acts by others, so their words were protected by the First Amendment.

Some legal scholars think that this ruling was abetted by recent Supreme Court decisions, which have stipulated that threats must be explicit and likely to cause “imminent lawless action.” For the three-judge panel on this appeals court, the speech found on the Nuremberg website, however unappealing and extreme, did not meet this heavy burden.

A more recent case has focused attention on threatening rap lyrics posted on Facebook by a rapper known as Tone Dougie (Anthony Elonis). These posts were full of vicious language directed at Mr. Elonis's estranged wife. For example, in some of his rants, Elonis proclaimed that he would like to see a Halloween costume that included his wife's head on a stick. The rapper was convicted under federal law of transmitting communications containing threats and sentenced to 4 years in jail. However, Elonis contended that he never *intended* to threaten anyone and that his menacing Facebook posts were merely a "therapeutic way" to deal with his anger. Defenders of Elonis argue that people should have wide latitude for free, creative expression online and that there must be proof of subjective intent in order to classify speech as a true threat. The case was appealed to U.S. Supreme Court, which threw out the conviction primarily because the jurors failed to focus on the critical matter of Elonis's intentions. The Supreme Court ruling was regarded as a setback for law enforcement, victims' rights groups, and valid efforts to preserve civility in online discourse.[33]

Anonymous Speech

Anonymous communication in cyberspace is enabled largely through the use of anonymous remailers, which strip off the identifying information on an email message and substitute an anonymous code or a random number. By encrypting a message and then routing that message through a series of these remailers, a user can rest assured that his or her message will remain anonymous and confidential. This process is known as “chained remailing.” The process is usually effective because none of the remailers has the key to read the encrypted message; neither the recipient nor any remailers (except the first) in the chain can identify the sender; the recipient cannot connect the sender to the message unless every single remailer in the chain cooperates.

New anonymizer tools such as Tor have also emerged, thanks to the work of a group of open source engineers. Tor is known as an “onion router,” because it layers internet traffic like an onion. Tor’s ProtonMail enables anonymous email communications, while the Tor browser isolates websites from the snooping gaze of advertisers or other third parties engaged in online surveillance.

But should digital anonymity be promoted and encouraged, since it is sometimes abused as a shield for subversive activities? It would be difficult to argue convincingly that anonymity is a core human good, utterly indispensable for human flourishing and happiness. One can surely conceive of people and societies where anonymity is not a factor for their happiness. However, although anonymity may not be a primary or basic human good, it is surely an instrumental good or value. For some people, under certain circumstances, a measure of anonymity is quite important for the exercise of their rational life plan and for human flourishing. The proper exercise of freedom, and especially free expression, does require the support of anonymity in some situations. Unless the speaker or author can choose to remain anonymous, opportunities for free expression become limited for various reasons and that individual may be forced to remain mute on critical matters. Thus, without the benefit of anonymity, the value of freedom is constrained.

We can point to many specific examples in support of the argument that anonymous free expression deserves protection. Social intolerance may require some individuals to rely on anonymity to communicate openly about an embarrassing

medical condition or an awkward disability. Whistleblowers may be understandably reluctant to come forward with valuable information unless they can remain anonymous. And political dissent even in a democratic society that prizes free speech may be impeded unless it can be done anonymously. Anonymity has an incontestable value in the struggle against repression or even against more routine corporate and government abuses of power.

Thus, although there is some social cost to preserving anonymity in cyberspace, its central importance in human affairs is certainly beyond dispute. It is a positive good, that is, it possesses positive qualities that render it worthy to be valued. At a minimum, it is valued as an instrumental good, as a means of achieving the full actualization of free expression.

Anonymous communication, of course, whether facilitated by remailers or by other means, does have its drawbacks. It can be abused by criminals or terrorists seeking to communicate anonymously to plot their crimes. It also permits cowardly users to engage in calumny or to libel someone without accountability. Anonymity can also be useful for revealing trade secrets or violating other intellectual property laws. In general, secrecy and anonymity are not beneficial for society if they are

overused or used improperly. According to David Brin, “anonymity is the darkness behind which most miscreants—from mere troublemakers all the way to mass murderers and would-be tyrants—shelter in order to wreak harm, safe against discovery or redress by those they abuse.”[34]

Although we admit that too much secrecy is problematic, the answer is not to eliminate all secrecy and make everything public and transparent, which could be the inevitable result of this loss of digital anonymity. Nonetheless, it cannot be denied that anonymity has its disadvantages and that digital anonymity and unrestricted internet access can be exploited for many forms of mischief. Hence the temptation of governments to sanction the deployment of architectures that will make internet users more accountable and less able to hide behind the cloak of anonymity.

Despite the potential for abuse, however, there are cogent reasons for eschewing the adoption of those architectures and protecting the right to anonymous free speech. A strong case can be put forth that the costs of banning anonymous speech in cyberspace are simply too high in an open and democratic society. The loss of anonymity may very well diminish the power of that voice that now resonates so loudly in cyberspace. As a result,

regulators must proceed with great caution in this area.

Government Censorship and the Fate of Political Speech

So far in this chapter we have been considering deviant forms of speech such as pornography, hate speech, and online threats. We have seen how governments have tried to restrict the free flow of pornographic speech to keep it out of the hands of minors. Government censorship, however, is not always confined to pornographic speech considered harmful to minors or to violent video games. Some authoritarian governments have also sought to censor political speech by stifling dissent in their countries. Dissident websites and many foreign news sources are blocked by sophisticated filtering systems. In China, for example, these filtering systems are installed on routers manufactured by Cisco and controlled by ISPs such as China Telecom.

This censorship infrastructure has become known as the “Great Firewall of China,” and it is designed to help the country limit political activism and expressions of dissent. The firewall blocks many foreign websites including Voice of America, the *New York Times*, and Human Rights Watch. Wikipedia has been completely blocked since May, 2015. Social media platforms such as Facebook

and Twitter are banned in China. In September, 2014, the Chinese government blocked Instagram after it became a popular tool during Hong Kong's pro-democracy protests. Through deep packet filtering the Great Firewall can block specific web pages and images. References to the Tiananmen Square incident, China's human rights record, religious freedom in China, or Tibet are blocked unless some type of coded language is used.[35]

The Chinese government has also pressured internet gatekeepers like Yahoo and Google to comply with its strict censorship laws. Let us briefly consider the case of Google, the ubiquitous search engine company that dominates markets throughout the world. Google's famous values such as "technology matters" and "don't be evil" have guided the company in its ambitious expansion efforts. When it entered the Chinese market to compete with Baidu (China's search engine company), Google conceded to China's demands that it follow local law. Hence it reluctantly agreed to self-censor and to purge its search engine results of any links to politically "offensive" websites and other content not approved by the Chinese government. These included websites supporting the Falun Gong cult or the independence movements in Tibet and Taiwan. As one reporter indicated,

> If you search for ‘Tibet’ or ‘Falun Gong’ most anywhere in the world on **google.com**, you’ll find thousands of blog entries, news items and chat rooms on Chinese repression. Do the same search inside China on google.cn and most, if not all, of these links will be gone. Google will have erased them completely.[36]

In order to avoid further complications, the company did not host user-generated content, such as blogs or email, on its computer servers in China for fear of the government’s role in restricting their content. In this way, it avoided the plight of companies like Yahoo who were compelled by Chinese law to hand over information about dissidents using Yahoo’s email. Unlike its local competitors, Google alerted users to censored material by putting a disclaimer at the top of the search results indicating that certain links have been removed in accordance with Chinese law. Also, Chinese users could still access **Google.com** with its uncensored search results (though links to controversial sites would not work thanks to the firewall). After several years, Google decided to stop censoring its web search and news services in China. The company reluctantly came to the conclusion that complicity in censorship violated its values. As a result, in March 2010 Google quietly announced that it

would redirect Google.cn users to an uncensored site hosted in Hong Kong.

Microsoft has also admitted that when it introduced its “MSN Spaces” to China, enabling users to set up their own blogs, all blog titles containing words such as “freedom” or “democracy” would be disabled. If a Chinese user sought to create a blog called “Democracy in Today’s China,” he would receive an error message, warning him that he is using “forbidden language,” and must “delete the prohibited expression.”[37]

Of course, given the magnitude of internet use in China, the best the government can hope for is “porous censorship.” According to Margaret Roberts this type of incomplete censorship is actually China’s overt strategy, since more obvious repression would likely ignite a popular backlash. Incomplete censorship, on the other hand, is more easily concealed by authoritarian governments like China, and gives the government the cover of plausible deniability.[38]

According to Roberts, China relies on three basic mechanisms, *fear, friction, and flooding*, to modulate information flows in the country. Fear originates not only from the consequences of flouting China’s censorship laws, but also from intimidation of journalists and social media users

who operate within the law. When the censors at Sina Weibo, China's largest social media network, did not promptly remove posts about a liberal newspaper editorial, the company's executives were summoned before government officials and admonished about the importance of "running the Internet in a civilized manner." Friction is the cost imposed on accessing or sharing information. The most conspicuous source of friction is the Great Firewall itself, which blocks out foreign websites the government regards as objectionable. This restriction can be circumvented by downloading a virtual private network (VPN), but sometimes they are shut down by the Chinese government, so users must search for an alternative VPN before they can scale the firewall. Also, very few Chinese citizens take advantage of VPNs. Friction can take several other forms such as the throttling of Google in 2010 (so users could connect only some of the time) when it redirected traffic to its Hong Kong website that did not abide by China's censorship rules.[39]

Finally, authorities rely on the technique of flooding. Flooding is defined as the "coordinated production of information by an authority with the intent of competing with or distracting from information the authority would rather consumers not access." Some governments, for example, rely

on “Twitter armies,” a coordinated effort to promote and propagate their version of certain political events. Roberts describes how in August 2014, shortly after a major earthquake in Yunnan province, Chinese official media began posting coordinated stories about a controversial internet personality Guo Meimei who had become entangled in a Red Cross scandal several years earlier. Credible foreign media sources alleged that this coordination of news was a distraction from the earthquake, which had the potential to reveal flaws in the government’s earthquake preparedness programs. These subtle strategies of friction and flooding tend to drive Chinese citizens away from activist agendas or alternative political viewpoints that are a threat to the regime.[40]

Despite these challenges, U.S. technology companies have certainly not given up on China. The social media network for professionals called LinkedIn is convinced of the importance of the lucrative China market to its business. Hence, it has sought a presence in China by following the example of Google and compromising its free speech standards. On both its Chinese and English language sites in China, the company censors (for its Chinese users) any content that is judged to be politically sensitive or inflammatory by

the Chinese government. It uses a combination of computer algorithms and human reviewers to accomplish this censorship. In addition, LinkedIn deprives its Chinese users of tools to create groups, to post long essays, or to create forums for public discussion. The company is optimistic about its prospects in China and claims that its principal goal is to provide the opportunity "for millions of Chinese professionals to significantly expand their economic opportunities."[41]

When companies refuse to censor objectionable content from their sites, they can easily risk a confrontation with the local government. In India, both Google and Facebook have been taken to court for not blocking content that is forbidden by an austere Indian censorship law (at least by Western standards). That law prohibits blasphemy, ethnic disparagement, and any threats made to the public order. Google, which owns YouTube, ran afoul of Indian law because it failed to remove a video showing someone relating a Hindu story that had been edited to incorporate obscene language. Civil libertarians object that India's Information Technology Act (2008) represents a stifling of free speech, but others argue that India has a right to set its own speech standards and that internet companies must follow the local laws of the land.[42]

Countries like Iran have followed China's lead in their aggressive filtering of unwanted internet content. In February 2011, young Iranians belatedly joined in the "Arab spring," and took to the streets to protest the Iranian government's repressive politics. Some of these collective activities were planned online, especially in popular internet cafes. Iran responded with a new wave of restrictions. Cameras were installed in these cafes and user registration was made mandatory. In the spring of 2012, the Iranian government decided to centralize its censorship activities by forming the Supreme Council of Cyberspace dedicated to purging the internet of websites that threaten Islamic morality or national security. The Iranian government has used many different tactics such as "friction" to constrain technology and limit internet use during times of political turmoil. In one instance, in order to control the use of smartphone technologies, mobile operators in Iran were required to limit internet speeds to a "sub-snail's pace," rendering it unfeasible to make video calls or transmit images.[43]

The internet was supposed to be a liberating force, destined to become an unfettered and nonterritorial global network beyond the reach of local governments. Many believed that the spread

of this technology around the world would mean the waning of state sovereignty. *New York Times* columnist Tom Friedman wrote that the internet and globalization would "act like nutcrackers to open societies."[44] So what happened? What accounts for this confrontation between authoritarian politics and online freedom of expression in countries like Iran and China? Governments have retaken control of the internet by blocking objectionable content with the aid of intermediaries like Google and by reestablishing borders that were initially erased by networking technology. As Goldsmith and Wu point out, the internet is becoming a collection of "nation-state networks—networks still linked by the internet protocol, but for many purposes separate."[45] China has virtually segregated its national network by creating its "great firewall," and Iran has threatened to create its own national internet disconnected from the rest of the world. The enforcement of national laws in cases like *Gutnick* (see **Chapter 2**) has also contributed to this phenomenon of a bordered and closed internet.

Those who support this reemergence of national government control in cyberspace might cite the experience of France in the *LICRA v Yahoo* case to defend their reasoning. Its local laws directed at Yahoo better reflected the needs and history of its

people than some set of uniform global standards. There is something to be said for preserving the role of territorial governance even in cyberspace as countries try to sustain their cultural identity in the face of the uniformity imposed by globalization. On the other hand, if there is a universal right to free expression, it is difficult to justify the coercive activities of countries like Iran. Will Iran's Orwellian "Supreme Council of Cyberspace" really reflect the best interests of the Iranian people and promote social welfare?

Postscript

Pornography, violent video games, hate speech, and threats are all problematic forms of free expression that pose formidable challenges to cyberspace jurisprudence, which seeks to balance individual rights with the public good. Ideally, of course, individuals and organizations should regulate their own expression by refraining from intimidating and mean-spirited hate speech, refusing to disseminate pornography to children, and repressing the temptation to use spam as a means of advertising goods or services. But in the absence of such self-restraint, internet stakeholders must make difficult decisions about whether or not to shield themselves from unwanted speech, whether it be crude obscenities or irksome junk email.

Top-down government regulations such as COPA represent one method for solving this problem. Sophisticated filtering devices, which will undoubtedly continue to improve in their precision and accuracy, offer a different but more chaotic alternative. As we have been at pains to insist here, whatever combination of constraints is utilized—code, law, market, or norms—full respect must be accorded to key moral values such as

personal autonomy. Hence the need for nuanced ethical reflection about how these universal moral standards can best be preserved as we develop effective constraints for aberrant behavior in cyberspace. Otherwise, our worst apprehensions about the tyranny of the code or the laws of cyberspace may be realized.

Another option, of course, is to refrain from the temptation to take any action against these controversial forms of speech in cyberspace. Some civil libertarians argue convincingly that internet stakeholders should eschew regulations and filtering and leave the internet as unfettered and open as possible. We should tolerate all forms of nuisance speech on the internet just as we tolerate them in the physical world. The challenge with any form of censorship is the difficulty of separating constructive speech from harmful speech. As John Perry Barlow writes, “We cannot separate the air that chokes from the air upon which wings beat.”[46]

If a decision is made to suppress extreme forms of speech, the ethical challenge is to find a way to preserve the liberties of cyberspace while removing speech that is not constitutionally protected or restricting access to speech that is harmful to minors. The internet has created a “new marketplace of ideas” with “content [that] is as

diverse as human thought."[47] And neither law nor code should disrupt the free flow of ideas and information in this democratic marketplace.

DISCUSSION QUESTIONS

1. What is your assessment of the Children's Internet Protection Act (CIPA)? Do you support the ACLU's views against this legislation?
2. Are automated content controls a reasonable means of dealing with pornographic material on the internet? At what level(s)—e.g., parent, school/library, ISP—should those controls be deployed?
3. What sort of First Amendment protection do websites filled with hate speech or racist speech deserve?
4. Is the right to free speech universal? That is, should everyone have the right, within reason, to criticize their government and freely express their political views, or is the right to free speech culturally conditioned, as some countries like China have assumed?

Case Studies

When Is a Facebook Post a Real Threat?

Offensive and threatening language has become all too common in the infosphere and especially in interactive social media. In the United States the right to free expression, protected by the First Amendment of the U.S. Constitution, is quite broad. However, that right to free expression does not include the right to make a hostile threat directed at another person. A “true threat” is illegal even in the free-wheeling realm of cyberspace. The issue has taken on greater salience due to the rise of social media and microblogging, where many more people have a forum to use threatening and abusive language. But how much latitude should people have to express themselves on Facebook, Twitter, or YouTube or on other social media sites?

The case of an aspiring rapper, Anthony Elonis, has crystallized the issue in cyberspace jurisprudence and has also raised several moral questions. Elonis

posted a series of menacing remarks on Facebook about his estranged wife. Some of those remarks included threats against her life. In one particularly virulent post he wrote, “I’m not going to rest until your body is a mess, soaked in blood and dying from all the little cuts.” Several of the most serious threats took the form of rap lyrics: “Little Agent Lady stood so close/Took all the strength I had not to turn the bitch ghost/Pull my knife, flick my wrist, and slit her throat.”

Mr. Elonis was arrested and indicted under federal law of allegedly transmitting communications across state lines that incorporate a threat. A motion was filed to dismiss the indictment based on the argument that these statements were protected speech (rather than “true threats”) under the First Amendment, particularly because there was no proof of any subjective intent on Elonis’s part to threaten his wife. But in rejecting this motion, the court noted the application of an “objective speaker test,” under which a communication is a true threat (and therefore not protected by the First Amendment) if a defendant intentionally made the statement and a reasonable person would foresee that such

a statement would be interpreted by those to whom the speaker communicates the statement as a serious expression of an intention to inflict bodily harm.[48]

The courts dealing with this and other cases have grappled with the appropriate legal standard for what constitutes a “true threat.” Should prosecutors have to prove that there was a subjective intent to threaten someone? Or is it adequate to demonstrate that a “reasonable person” would regard the words in question as a threat or that the victim *feels* threatened in some way? The lawyers for Mr. Elonis have argued that a prosecutor must show that the individual accused of making threats clearly intends to put the victim in a state of fear or intends to do psychological or physical harm. Also, to what extent does context matter? Rap songs by Eminem, no matter how vile, are a form of entertainment, but Mr. Elonis’s random posting and amateur rap lyrics on his personal Facebook page could not really be considered entertainment.[49]

During the trial, Elonis, through his lawyers, argued that his words were misinterpreted—they weren’t really a threat, he claimed, but a

“therapeutic” way of working out his anger and frustration. These incendiary lyrics were just “fictitious,” and not meant to be taken seriously.[50] But those arguments fell on the deaf ears of an unsympathetic jury.

In 2012, Elonis was convicted and sentenced to 4 years in jail. Elonis’s lawyers quickly appealed his conviction, but in 2013 it was upheld by the 3rd Circuit Court of Appeals. The appeals court strongly rejected the argument that proof of subjective intent is required by the First Amendment, and Elonis’s conviction was not overturned as he had hoped. Meanwhile, the case began to attract national attention.

Free-speech activists expressed their serious reservations about this case and about the implications for people who post on Facebook and other forms of social media. Those concerns became increasingly evident as the legal drama continued. In their petition to the Supreme Court to take their client’s case, Elonis’s lawyers argued that online communication makes it more difficult than ever to interpret the meaning of a statement. Hence, this means that it is vital for a jury to take into account Elonis’s *intent*

in writing his posts rather than just consider how a hypothetical reasonable person might evaluate a threatening statement. According to Elonis's lawyers, the "impersonal nature of online communication makes such messages inherently susceptible to misinterpretation."[51]

The case of *Elonis v. U.S.* was heard by the U.S. Supreme Court in 2015. The Court, seeking to resolve a complicated web of free speech issues, threw out the Elonis conviction because the jury did not take into account Elonis's intentions.

Questions

1. What is the right standard for determining an online threat, and why is this issue more complicated in the world of interactive social media?
2. Did the Supreme Court make the right decision in this case? If you were one of the nine justices, would you uphold Elonis's conviction or toss it out?

Case Studies

Are Video Games Free Speech?

The video game industry dates back to 1972, when Magnavox first introduced a game console called Odyssey. The industry grew rapidly in the 1980s and 1990s in parallel with the explosive expansion of the PC industry. Companies like Atari and Nintendo fueled that growth thanks to popular games such as *Super Mario Brothers* and *The Legend of Zelda*.

Nintendo was overtaken by Sega's popular consoles, beginning with Genesis in 1988. But 7 years later Sony launched PlayStation and became the industry leader within a few years. Worried that game consoles could become a substitute for PCs, Microsoft entered this competitive industry in 2001 with its Xbox console. Microsoft, Sony, and Nintendo now dominate the $11 billion dollar industry. Popular games include *Grand Theft Auto*, *Manhunt*, and the mature-rated *Fallout* series. New-generation consoles include advanced functionality. PlayStation 3, for example, plays high-definition DVDs, stores photographs and music, and even permits video conferencing. Both PlayStation 3 and

Microsoft's Xbox 360 support online gaming so that users can play video games with their friends over the internet.

Some video games have questionable content. They are laced with graphic violence or sexual aggressiveness. Like the movie industry, the video game industry has adopted its own voluntary internal rating system that informs consumers about the content of games. Video games are rated by the Entertainment Software Rating Board on a scale from EC (early childhood) to M (mature). Dealers are encouraged to refrain from renting or selling M-rated games to minors under the age of 17 without parental consent.

In 2005, the state of California prohibited the sale or rental of violent video games to minors. The state believed that the voluntary industry rating system was inadequate, so it established a law preventing persons under the age of 18 from purchasing games labeled as violent by state authorities. Violent games were defined as those that gave players the opportunity to "kill, maim, dismember or sexually assault the image of a human being." For example, a game is

considered violent if there is “needless mutilation of the victim’s body.”[52] One game covered by the new law “involves shooting both armed opponents, such as police officers, and unarmed people, such as school girls; girls attacked with a shovel will beg for mercy—the player can be merciless and decapitate them.”[53] The reasoning behind this legislation was grounded in the conviction that interactive, ultraviolent video games increase aggressive thoughts and feelings.

The California law was immediately challenged in court by the video game industry, represented by the Video Software Dealers Association. The industry maintained that this law stifled their creative expression and so violated its First Amendment rights. The plaintiffs argued that these games are entitled to First Amendment protection and that attempts to regulate their content are not allowed. The plaintiffs also contended that the state’s definition of violence was too vague. For example, according to the statute, violence meant to “virtually inflict a serious injury upon images of human beings or characters with substantially human characteristics.”

But what about zombies, centaurs, or other nonhuman characters with magical powers that still possess some “human characteristics”?[54] The State of California, on the other hand, argued for the need for its involvement to ensure the health and well-being of the state’s children.

The U.S. District Court of California issued an injunction barring California from enforcing the law. The Ninth Circuit concurred, arguing that the law was invalid because it amounted to content-based restriction on speech. The law was presumptively unconstitutional because “the State, in essence, asks us to create a new category of non-protected material based on its depiction of violence.”[55] The Ninth Circuit claimed that California failed to exhibit definitive proof of any causal connection between violent video games and the aggressive behavior of minors. Although the First Amendment does not protect obscene speech, violent imagery or content does not fall under the category of obscenity. Also, the Ginsberg ruling protecting minors from pornography does not apply, because that case involved a subcategory of obscenity, that is, obscenity for minors, which is not an

issue in this case. The case was then sent to the U.S. Supreme Court, where a central issue emerged: Are games entitled to First Amendment protection in the same way as other forms of speech, such as music or books?

In 2011, the Supreme Court concurred with the Ninth Circuit. It held that video games are no different from protected books, plays, and movies. They, too, communicate ideas and so qualify for First Amendment protection. The Court rejected what it called California's attempt to "shoehorn speech about violence into obscenity."[56] It dismissed California's claims that video games present special problems because of their interactive nature that enables a minor's participation in violent action in the virtual world created by the game. Thus, because the proposed California law imposes restrictions on the content of this protected speech in violation of the First Amendment, it is invalid.

Questions

1. Do you agree with the Supreme Court's ruling in this case?
2. In your view, is there a causal connection between playing violent

video games and aggressive behavior, and, if so, what should be done about it?

Case Studies

Twitter, Free Speech, and Terrorism

The rise of terrorism throughout the world during the past decade has caused enormous problems for the world of interactive social media. Social media and the internet were supposed to spread freedom and democracy, but instead they have also often spread fear and violence. Terror attacks in Paris and Denmark, the rise of ISIS in the Middle East, and the tactics of authoritarian governments, have all put high-tech companies in a difficult position. At the same time, the problems of hate speech and anti-Semitism continue to persist, along with demands for action. European regulators, for example, want U.S. companies like Google or Facebook to cleanse their sites of extremist postings, including anti-Semitic hate speech. There are also demands from governments to open their encryption technology so that government surveillance could be more easily facilitated.

The mobile and social media phenomenon Twitter is at the center of many of these controversies and conflicts. Twitter was founded in 2006 and incorporated 1 year

later in 2007. The company provides a service that enables users to send and read “tweets,” short messages limited to 140 characters. Registered users can read and post tweets, but unregistered users can only read them. Users access Twitter through the company’s website or by using an app on mobile devices. In 2010, Twitter introduced “Promotional Tweets” to generate revenues. The San Francisco company has over 300 million Twitter users, with 77% of its accounts outside the United States. There are over 500 million tweets sent out every day.[57]

In its short lifespan, Twitter has already been a tool for democracy. It has been used to organize protests, sometimes referred to as “Twitter Revolutions,” which include the Egyptian uprising in 2011. But Twitter has also become a platform for terrorists and others who spread messages of violence and hate. Twitter, along with Facebook and Google, has pledged to help governments in their fight against terrorism, but they must walk a fine line between protecting users’ free speech and privacy rights and cooperating with a government’s crackdown on terrorism. Twitter must contend with two

problems: censorship by authoritarian governments and the need for self-censorship when the tweets of its users involve extreme forms of speech that violate social norms.

Let's first consider the matter of external censorship. Some governments have tried with varying degrees of success to stifle Twitter. It has been blocked on occasion in several countries, including Egypt, Iran, Iraq, and Turkey. Twitter remains unavailable in China because it will not comply with the country's strict censorship rules. This policy represents a departure from gatekeepers such as Yahoo and Google, who did comply with those rules when they entered the Chinese market. According to company CEO Dick Costolo, "We are not going to make the kinds of sacrifices we might have to currently make to be unblocked in China."[58]

Turkey's President, Mr. Erdogan, attempted to block Twitter before the country's most recent election. Turkey has tried to rein in the internet and this includes free speech platforms like Twitter. Erdogan reopened the website quickly as the protests persisted, but the number of formal government requests

to remove objectionable content has increased dramatically. If Twitter doesn't comply, it risks further blackouts, but to what extent should Twitter compromise its principles?[59]

What about self-censorship? Twitter, along with most other microblogging and social media sites, has a broad free speech policy. It allows pornographic images in tweets so long as they do not constitute some type of sexual harassment. Some so-called "sensitive images" are now accompanied by a warning. Twitter's liberal policies also allow for the depiction of violence. But there are limits to what can be tweeted. Among its "content boundaries," Twitter lists the following:

> **Violence and Threats**: You may not publish or post threats of violence against others or promote violence against others.
>
> **Serial Accounts**: You may not create multiple accounts for disruptive or abusive purposes, or with overlapping use cases. Mass account creation may result in suspension of all related accounts. Please note that any violation

of the Twitter Rules is cause for permanent suspension of all accounts.

Targeted Abuse: You may not engage in targeted abuse or harassment. Some of the factors that we take into account when determining what conduct is considered to be targeted abuse or harassment are:

- if you are sending messages to a user from multiple accounts;
- if the sole purpose of your account is to send abusive messages to others;
- if the reported behavior is one-sided or includes threats

Graphic Content: You may not use pornographic or excessively violent media in your profile image, header image, or background image.[60]

Twitter suspends accounts or removes content only when something is flagged and brought to its attention by another user. Twitter does not proactively search the Net for content or images that violate its rules. As a result of its broad free speech policy, Twitter has been called “home to the profound and profane,” and the “Wild West of social media.”[61]

Critics of Twitter argue that it is too slow to take action and not proactive enough in dealing with abuses, such as terrorist threats or abusive and sadistic language. They claim that Twitter must do a much better job "of protecting its users from the dark underbelly of the Internet."[62] In their view, Twitter should be more proactive and if possible expunge extremist or hateful content before it is ever seen by users. It is also essential to expediently remove graphic images such as beheadings or other brutal acts that have been tweeted by terrorists (such as ISIS) before they do additional damage as they circulate in cyberspace. Sensitivity to the victims' families is particularly important in these situations. But Twitter's policy has remained unchanged: The company will not actively search for content that violates its boundaries, including these graphic images. Rather, it will disable the unique web address associated with such content only when it is brought to Twitter's attention by another user. However, a user can easily upload that contraband material to a different account and a new web address.[63] In a violent and sometimes

callous world, some wonder whether this policy needs to be substantially revised.

Questions

1. Is there ever any basis for a country, such as Turkey or China, to ban Twitter?
2. How do you assess Twitter's broad free speech policies? Visit **Twitter.com/rules** and take a look at the company's "content boundaries." Do you think these are too broad, too narrow, or just right?
3. Should the company be more proactive in removing objectionable content that violates its policies by adopting a process of "automatic flagging"?

Case Studies

LinkedIn Goes to China

Multinational corporations sometimes face complex interactions with their host governments. This has been particularly true for internet firms like Google and Yahoo, along with social media firms like Facebook and Instagram. These firms present themselves as models of free expression and openness, and yet they have sought to do business with China, one of the most authoritarian nations on the planet. As these firms assess the Chinese marketplace, they face a painful choice: either abide by China's burdensome censorship rules, which requires the blocking of dissident political speech and the stifling of virtual organizing, or stay out and abandon this lucrative market of 700 million internet users. Yet Facebook has repeatedly tried to penetrate this relatively isolated space of the internet. In 2016, Facebook took some tentative steps toward embracing China's censorship policies by developing tools that would suppress postings in certain geographic areas. However, for various reasons, these

censorship tools were never used. But it continues to test the waters in China.[64]

This case examines the professional website LinkedIn and its choice to enter the Chinese marketplace in 2014. The prime focus is the company's controversial decision to be "culturally sensitive" and fully comply with China's censorship demands.

What Is LinkedIn?

One of the major success stories in the world of social networking is undoubtedly LinkedIn.

LinkedIn describes itself as a business-oriented social networking service. It allows users, both workers and employers, to create profiles and "connections" to each other in an online social network. LinkedIn was founded on December 14, 2002, by Reid Hoffman when the social media industry was still in its infancy. Unlike Facebook or Google, this platform is used primarily for professional networking.

LinkedIn grew steadily, and, by early 2006, the networking company generated its first profits. The company enabled the creation of public professional profiles that were

indexed into Google, and this made it easier for users to appreciate the value of this service. By 2016, it was estimated that LinkedIn had more than 500 million users in over 200 countries. The company's global mission is ambitious but simple: "To connect the world's professionals to make them more productive and successful." And the company's vision is to create opportunities for every member of the global workplace and to help those individuals "work smarter." The company prides itself on being the most extensive, accurate, and accessible professional network. Its strategy is to build the capabilities that will allow its members to stay connected and informed and to advance their careers.[65]

When a person joins LinkedIn, he or she gets access to people, jobs, news, updates, and insights that will help them in their professional lives. LinkedIn enables its members to search for business contacts and to join industry groups that will advance their careers. Anyone can become a member, but most people enroll when they receive an invitation from a LinkedIn member to become one of their connections. When a new member joins LinkedIn he or

she creates a profile that includes their educational background, work history, and any professional affiliations. Once this person becomes a LinkedIn member she can invite others to become part of her network. That network, which consists of direct connections along with secondary and tertiary connections (that is, connections of a user's connections, etc.), will most likely reflect and imitate professional relationships in the real world. Thus, a lawyer will have connections with other lawyers, jurists, and legal professionals.[66]

Once someone becomes a member of LinkedIn it is possible to contact other LinkedIn members in one's circle of contacts with the help of the site's search functionality. In addition, users can search for professional groups, job postings, universities, and published content. The network can be used to find jobs recommended by someone in one's contact network. Employers can utilize LinkedIn to search for potential candidates for their job openings. Users can also post content and do things such as "like" and "congratulate" each other for a promotion or new employment, and endorse each other's

skills. LinkedIn provides ubiquitous access through LinkedIn Mobile and a robust set of apps.

Most LinkedIn members pay no fees to list the details about their education and their careers or to be informed about suitable employment opportunities. Some members, however, pay a premium subscription fee, which enables them to post a customized profile, a bigger photograph, and an open profile that allows anyone on the network to contact them without any charges. Premium subscriptions account for about 20% of LinkedIn's revenues. Another source of revenue comes from Marketing Solutions, a service that allows advertisers to display ads on the LinkedIn website. But recruiters are the primary source of LinkedIn's revenue. Through a service called LinkedIn Hiring Solutions companies purchase licenses in order to search for likely job candidates and to email them about job vacancies. Recruiters can search every profile on the network. It seems fair to say that LinkedIn is changing the market for labor: both how candidates find jobs and how employers find them.[67]

The China Gamble

LinkedIn has expanded into many international markets, including China. In February 2014, it launched its local Chinese website called Ling Ying and established operations in China. According to a company spokesperson, “connecting global professionals” was the motivating force behind LinkedIn’s controversial decision to enter the Chinese market. That market is quite substantial with 140 million professional workers as potential users. LinkedIn has two local partners, which have a 7% stake in the business: China Broadband Capital, and a Chinese affiliate of American venture capital firm known as Sequoia Capital. LinkedIn, however, is in full control of the operation and retains the bulk of profits generated.

Growth in the Chinese marketplace has accelerated over the last several years. In 2015, LinkedIn had doubled its user base in China from 4 to 8 million. And by mid-2017, the social network site had over 32 million Chinese users. LinkedIn credited the head of its China operations, Deng Shen, with transforming the business from a startup into a viable business. The company has

updated its Chinese platform with a new mobile version designed for Chinese users along with other innovations.[68]

Analysts say that this early success is a positive sign for LinkedIn, since other U.S. internet firms, including Google and eBay, have struggled mightily to succeed in China. Fierce local competition and government regulation have often been tough roadblocks to overcome. Progress has been especially difficult for social media firms. Both Twitter and Facebook have been blocked for their potential to spread antigovernment or dissident political views to the Chinese people. Facebook was blocked in 2009 in an "information lockdown" after riots in China's Muslim Xinjiang region—riot leaders had used Facebook and other social media to stir unrest.[69] Chinese users can turn to RenRen for a social media experience similar to Facebook's. LinkedIn, however, has been undeterred by these events. The head of LinkedIn's China operations has affirmed that the company is committed to China "This is a very long-term investment, it's not an experiment."[70]

LinkedIn clearly takes advantage of the rise of the middle class in China, which is the result of its booming economy. Many of LinkedIn's newest Chinese users may speak English, and want to connect to career opportunities outside the country. But the company realizes that in order to court non-English-speaking Chinese users, it will have to develop more customized, local services. Otherwise the website might be destined to become a social media tool for the country's upper middle-class citizens.[71]

LinkedIn was convinced that it needed a presence in China to sustain its long-term growth and fulfill its mission of connecting the global workforce. It was also convinced that it would have to adapt to local Chinese cultural norms and customs if it was going to succeed there. It was well aware of the travails of other internet companies, such as Google and Facebook. But LinkedIn has found the formula for success since, unlike Facebook and Twitter, the Chinese government has never blocked access to the website. What's the secret of LinkedIn's good fortune? The company's willingness to self-censor and filter objectionable content. In an extensive interview with *The Wall*

Street Journal, LinkedIn Chief Executive Officer, Jeff Weiner, said the company expected "there will be requests to filter content," adding, "we are strongly in support of freedom of expression and we are opposed to censorship…[but] that's going to be necessary for us to achieve the kind of scale that we'd like to be able to deliver to our membership."[72]

Thus, on both the Chinese and English language sites in China, LinkedIn censors any content that is politically controversial in the eyes of Chinese authorities, including links to blacklisted websites. LinkedIn relies on software algorithms and human reviewers to determine which content will be blocked. When a user posts content that is unacceptable, he or she receives an email message stating that what they have written is prohibited expression in China and "will not be seen by LinkedIn members located in China." Any subject matter or content considered off limits in China will be filtered by LinkedIn.[73]

In June 2014, shortly after LinkedIn launched the Chinese version of its service, users in China reported that posts about the

25th anniversary of the Tiananmen Square incident were blocked even in Hong Kong, which lies outside of China's firewall. LinkedIn said that although the content was blocked in China, it would remain "accessible elsewhere in the world."[74] A law student at the Chinese University of Hong Kong, said he was "really shocked" to receive a notification from LinkedIn that a video he linked to on the social network expressing support for relatives and friends of those killed during the Tiananmen crackdown had been blocked within China. The message from LinkedIn indicated that the questionable video "has been visible globally, with the exception of the People's Republic of China."[75]

Jeff Weiner claims that concerns over the China censorship decision are mitigated by LinkedIn's progressive policies, especially its transparency. He explained that the company was guided by three principles for this complex situation. First, LinkedIn will implement government censorship restrictions but only to meet "minimum requirements." Second, LinkedIn is committed to transparency, so users will be notified of their practices and informed

whenever content is censored. Third, the company will take “extensive measures” to safeguard user data to the extent possible under Chinese law. LinkedIn believes that its absence in China would curtail the ability of Chinese citizens to realize vital economic opportunities.[76]

In addition to censorship, LinkedIn imposes other restrictions on its Chinese users. They are denied access to important tools, such as the ability to create and join groups or to post long essays. The purpose is to placate Chinese authorities by limiting in-depth online discussions and preventing the formation of virtual communities that can organize for political purposes or mold public opinion.[77] Moreover, despite its third guiding principle, LinkedIn had to agree to store all data about its Chinese users on servers located within China and consent to allow Chinese authorities to access these data whenever legally necessary. Finally, it has agreed to follow all present and *future* internet regulations imposed by the Chinese government.[78]

Despite the company’s initial success in China, there are demonstrable risks. Like

almost every internet company, LinkedIn is presumably committed to free expression, openness, and free market principles. Too much censorship could risk alienating users in Western countries, such as the United States and Europe. LinkedIn has already been heavily criticized for its China strategy and depicted as a multinational that will do anything for market access to China. Also, if LinkedIn's presence in China continues to grow and the social network becomes a more visible presence in cyberspace, the government will have greater leverage to make more stringent demands about LinkedIn's operations.[79]

While LinkedIn has been subject to considerable criticism for its decision to self-censor and dutifully follow all of China's internet regulations, the company has not wavered in its commitment to the rapidly expanding Chinese market. But LinkedIn may soon face demands from Chinese authorities other than censoring content. What if the government insists on getting information about dissident students or workers who use the service as evidence to prosecute them for treason or crimes against the state? Will LinkedIn simply comply with

such requests? Or will LinkedIn reach a point where its presence in this authoritarian country is untenable and “pull a Google” just like its illustrious predecessor, which pulled out of China in 2010 because it could no longer justify censoring its search results?

Exhibit One: LinkedIn’s Core Values

Members First	Know and understand LinkedIn’s members
Relationships matter	Foster trust with colleagues and partners, and do what is right
Be open, honest, and constructive	Communicate with clarity and provide feedback with consistency
Demand excellence	Lead by example and solve big challenges
Take intelligent risks	Never lose startup mentality
Based on U.S. Securities and Exchange Commission. LinkedIn 10-K Report, 2016.	

Questions

1. LinkedIn’s mission is to connect the global workforce and this is the prime reason for its entry into China. Do you accept this humanitarian mission as the reason for going to China? Does the

company need to reconsider that mission?

2. Is LinkedIn acting responsibly by censoring content to comply with local Chinese law?
3. This case gives us an opportunity to explore the tensions that arise when a business has operations in places where domestic law appears to be at odds with certain human rights. Is there a universal right to free expression, and, if so, how can it be justified? If you disagree with the universality of such a right, what are your *specific* arguments and what are the implications for doing business in countries like China?

REFERENCES

1. *Reno v. ACLU* 521 U.S. 844 [1997]. See also Ithiel de Sola Pool, *Technologies of Freedom* (Cambridge, MA: Harvard University Press, 1984).
2. Julie Cohen, "Between Truth and Power," in *Information, Freedom and Property*, ed. Mireille Hildebrandt (New York: Routledge, 2015), 57–62.
3. Floyd Abrams, *The Soul of the First Amendment* (New Haven, CT: Yale University Press, 2017), 76. See also Daniel Shuchman, "A Fundamental Liberty," *Wall Street Journal*, May 1, 2017, A15.
4. "Geography and the Net," *The Economist*, August 11, 2001, 18.
5. Larry Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999), 167.
6. *Ginsberg v. New York*, 390 U.S. 15 (1973).
7. See **http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html**.
8. See *Communications Decency Act*, 47 U.S.C. # 223 (d) (1) (B).

9. Zittrain et al., Brief for Appelants, *Reno v. ACLU*, no. 96–511.
10. Lessig, *Code and Other Laws of Cyberspace*, 175.
11. *Reno v. ACLU* 929 F. Supp 824 (E.D. Pa [1996]).
12. Ibid.
13. Max Hailperin, "The COPA Battle and the Future of Free Speech," *Communications of the ACM* 42, no. 1 (January 1999): 25.
14. Pamela Mendels, "Setback for a Law Shielding Minors from Smut Web Sites," *The New York Times*, February 2, 1999, A10.
15. Linda Greenhouse, "Court Blocks Law Regulating Internet Access to Pornography," *The New York Times*, June 30, 2004, A1.
16. Carl Kaplan, "Free-Speech Advocates Fight Filtering Software in Public Schools," January 19, 2001, **www.nytimes.com**.
17. Plaintiff's Complaint, *Multnomah Public Library et al. v. U.S*. 402 E.D. PA [2001].
18. Ibid.
19. Jonathan Katz, *Virtuous Reality* (New York: Random House, 1997), 184.
20. See "About Websense Enterprise," **http://www.websense.com/products**.

21. Jennifer Lee, “Cracking the Code of Online Filtering,” *The New York Times*, July 19, 2001, E9.

22. Plaintiff’s Complaint, *Multnomah Public Library et al. v. U.S*. 402 E.D. PA [2001].

23. Quoted in Amy Harmon, “To Screen or Not to Screen: Libraries Confront Internet Access,” *The New York Times*, June 23, 1997, D8.

24. See the American Library Association website, **www.ala.org**.

25. Richard Rosenberg, “Free Speech, Pornography, Sexual Harassment, and Electronic Networks,” *The Information Society* 9 (1993): 289.

26. I am indebted to John Finnis’s insightful discussion of these issues in *Natural Law and Natural Rights* (Oxford: Oxford University Press, 1980), 216–18.

27. Eric Pfanner, “Publishers Question Apple’s Rejection of Nudity,” *The New York Times*, March 14, 2010, D1.

28. *Brown v. Entertainment Merchants Association* 564 U.S. 148 (2011). See also Jeroen van den Hoven, “The Use of Normative Theories in Computer Ethics,” in *The Cambridge Handbook of Information and Computer Ethics*, ed. Luciano Floridi

(Cambridge, UK: Cambridge University Press, 2010), 69–70.

29. Jim Rutenberg, “Hate Speech Bounded by Character Limit Alone,” *New York Times*, October 3, 2016, B1, B5. See also Newley Purnell, “Call for Easter Attack Stayed on Facebook,” *Wall Street Journal*, May 1, 2019, A7.

30. *Snyder v. Phelps* 131 U.S. 1207 (2011). See also Adam Liptak, “Foreword: Hate Speech and Common Sense,” in *The Content and Context of Hate Speech* eds. Michael Herz and Peter Molnar (New York: Cambridge University Press, 2012), xix–xxii.

31. Abdul Rahman Al Jaloud et al., “Caught in the Net: The Impact of ‘Extremist’ Speech Regulations on Human Rights Content, Electronic Frontier Foundation,” May 2019.

32. Andrew Sellars, “Defining Hate Speech,” Berkman Klein Center Research Publication, December 8, 2016, **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2882244**.

33. Vauhini Vara, “The Nuances of Threats on Facebook,” *The New Yorker*, December 3, 2014, 16. See also Brent Kendall, “Web-Threat Conviction Tossed,” *Wall Street Journal*, June 2, 2015, A2.

34. David Brin, *The Transparent Society* (Reading, MA: Addison-Wesley, 1998), 27.

35. Zixue Tai, "The Great Firewall," in *The Internet in China: Cultural, Political, and Social Dimensions*, eds. Ashley Esarey and Randolph Kluver (Great Barrington, MA: Berkshire Publishing Group, 2014), 67–70. See also Margaret Roberts, *Censored: Distraction and Diversion inside China's Great Firewall* (Princeton, NJ: Princeton University Press, 2018), 109–10, 177–82.

36. Clive Thompson, "China's Google Problem," *New York Times Magazine*, April 23, 2006, 51.

37. Mark Magnier and Joseph Menn, "As China Censors the Internet, Money Talks," *Los Angeles Times*, June 17, 2005, A1.

38. Roberts, *Censored*, 8–9.

39. James Griffiths, *The Great Firewall of China* (London: ZED Books, 2019), 75–76. See also Roberts, *Censored*, 41–44, 109–10.

40. Roberts, *Censored*, 80, 175–85.

41. Paul Mozur and Vindu Goel, "To Reach China, LinkedIn Plays by Local Rules," *The New York Times*, October 6, 2014, A1, B5.

42. Amol Sharma, "Google, Facebook Fight India Censors," *The Wall Street Journal*, March 18,

2012, B1–2.

43. Thomas Erdbrink, “Tehran Unfetters Cellphones, and the Pictures Start Flowing,” *The New York Times*, September 3, 2014, A4.

44. Thomas Friedman, “Foreign Affairs; Censors Beware,” *The New York Times*, July 25, 2000, A27.

45. Jack Goldsmith and Tim Wu, *Who Controls the Internet?* (New York: Oxford University Press, 2008), 149.

46. John Perry Barlow, “A Declaration of the Independence of Cyberspace,” **https://projects.eff.org/~barlow/Declaration-Final.html**.

47. *Reno v. ACLU* 521 U.S. 885 [1997].

48. *United States v. Elonis* 3rd Cir. 730 F. 3d. 321 (2013).

49. Jess Bravin, “When Is Free Speech Illegal,” *The Wall Street Journal*, November 24, 2014, B5.

50. “What Is a True Threat on Facebook,” *The New York Times*, December 2, 2014, A22.

51. Vara, “Nuances of Threats on Facebook.”

52. California Civil Code § 1746 (d) (3).

53. Petition for Writ of Certiorari, *Schwarznegger v. Entertainment Merchants Association* 130

S. Ct. 2398 (2010).

54. Brief for Appellee, *Video Game Dealers Assoc. v. Schwarzneger*, 556 F.3d 950 (9th Cir. 2008).

55. *Video Game Dealers Assoc. v. Schwarzneger*, 556 F.3d 950 (9th Cir. 2008).

56. *Brown v. Entertainment Merchants Association* 564 U.S. 148 (2011).

57. See **http://about.twitter.com/company**.

58. Shira Ovide, "Free Speech a Test for Twitter," *The Wall Street Journal*, August 5, 2013, B1–2.

59. Joe Parkinson, "Turkey Builds New Model for Censorship," *The Wall Street Journal*, May 2, 2014, A13.

60. See **twitter.com/rules**.

61. Yoree Koh and Reed Albergotti, "Twitter Faces Free-Speech Dilemma," *The Wall Street Journal*, August 22, 2014, B1, B4.

62. Yoree Koh, "Twitter Safety Officer on Building Trust," *The Wall Street Journal*, February 18, 2015, B4.

63. Koh and Albergotti, "Twitter Faces Free-Speech Dilemma," B1.

64. Paul Mozur, Mark Scott, and Mike Isaac, "Facebook Is Navigating a Global Power

Struggle," *The New York Times*, September 18, 2017, A1, A7.

65. David Yoffie and Liz Kind, *LinkedIn Corporation, 2012* (Boston, MA: Harvard Business School Publishing, 2015), 5–6.

66. "Workers of the World, Log In," *The Economist*, August 16, 2014, 51–53. See also Yoffie and Kind, "LinkedIn Corporation, 2012," 5–6.

67. Ibid.

68. Xinhua, "LinkedIn China Users Top 32 Million," *China Daily.Com*, April 27, 2017, **www.chinadaily.com/2017-4-27/content_2017768?**. See also Iris Leung, "LinkedIn Waves Goodbye to China Chief, Derek Shen," *TECHWIRE*, June 28, 2017, **http://techwireasia.com/2017/06/linkedin-waves-goodbye-china-chief-derek-shen**.

69. Abkowitz, "Facebook's Big China Comeback," A8.

70. See Michael Kan, "LinkedIn's China Bet Starts Paying Off with Increase in Users," *PC World*, February 6, 2015, **www.pcworld.com/article/28810121/linkedins-china-bet**.

71. Ibid.

72. Reed Albergotti, “LinkedIn’s CEO: We’re Going to Expand in China; Goals ‘Aligned’ with Government,” February 24, 2014, **blogs.wsj.com/digits/2014/02/24**.

73. Paul Mozur and Vindu Goel, “To Reach China, LinkedIn Plays by Local Rules,” *The New York Times*, October 6, 2014, B1, B5.

74. William Wan and Xu Jing, “LinkedIn Thinking Twice about Its Adoption of China’s Aggressive Censorship,” *The Washington Post*, September 3, 2014, B1, B5.

75. Wall Street Journal Blog, “China Real Time,” June 4, 2014, **www.blogs/wsj.com/chinarealtime/2014/06/04**.

76. Lily Hay Newman, “Surprising No One, LinkedIn for China Will Be Subject to Government Censorship,” ***Slate.com***, February 25, 2014, **www.slate.com/blogs/future_tense/2014/02/25/linkedin_for_China_wiil_be_censored**.

77. Mozur and Goel, “To Reach China, LinkedIn Plays by Local Rules.”

78. Charlie Smith, “LinkedIn: Technological and Financial Giants but Moral Pygmies,” *Huffington Post*, July 15, 2016, **https://www.huffingtonpost.com/charlie-**

smith/linkedin-in-china-technol_b_7791126.html.

79. Mozur and Goel, “To Reach China, LinkedIn Plays by Local Rules,” B5.

ADDITIONAL RESOURCES

Abrams, Floyd. *The Soul of the First Amendment*. New Haven: Yale University Press, 2017.

Balkin, Jack. “Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society.” *New York University Law Review* 79, no. 1 (2004): 22–86.

Electronic Privacy Information Center. *Filters & Freedom*. Washington, DC: EPIC, 1999.

Esarey, Ashley and Randolph Kluver, eds. *The Internet in China: Cultural, Political, and Social Dimensions*. Great Barrington, MA: Berkshire Publishing Group, 2014.

Godwin, Michael. *Cyber Rights*. New York: Random House, 1998.

Griffiths, James. *The Great Firewall of China*. London: ZED Books, 2019.

Herz, Michael and Peter Molnar, eds. *The Content and Context of Hate Speech*. New York: Cambridge University Press, 2012.

MacKinnon, Rebecca. *Consent of the Networked*. New York: Basic Books, 2012.

Pool, Ithiel de Sola. *Technologies of Freedom*. Cambridge, MA: Belknap Press, 1983.

Roberts, Margaret. *Censored: Distraction and Diversion inside China's Great Firewall*. Princeton, NJ: Princeton University Press, 2018.

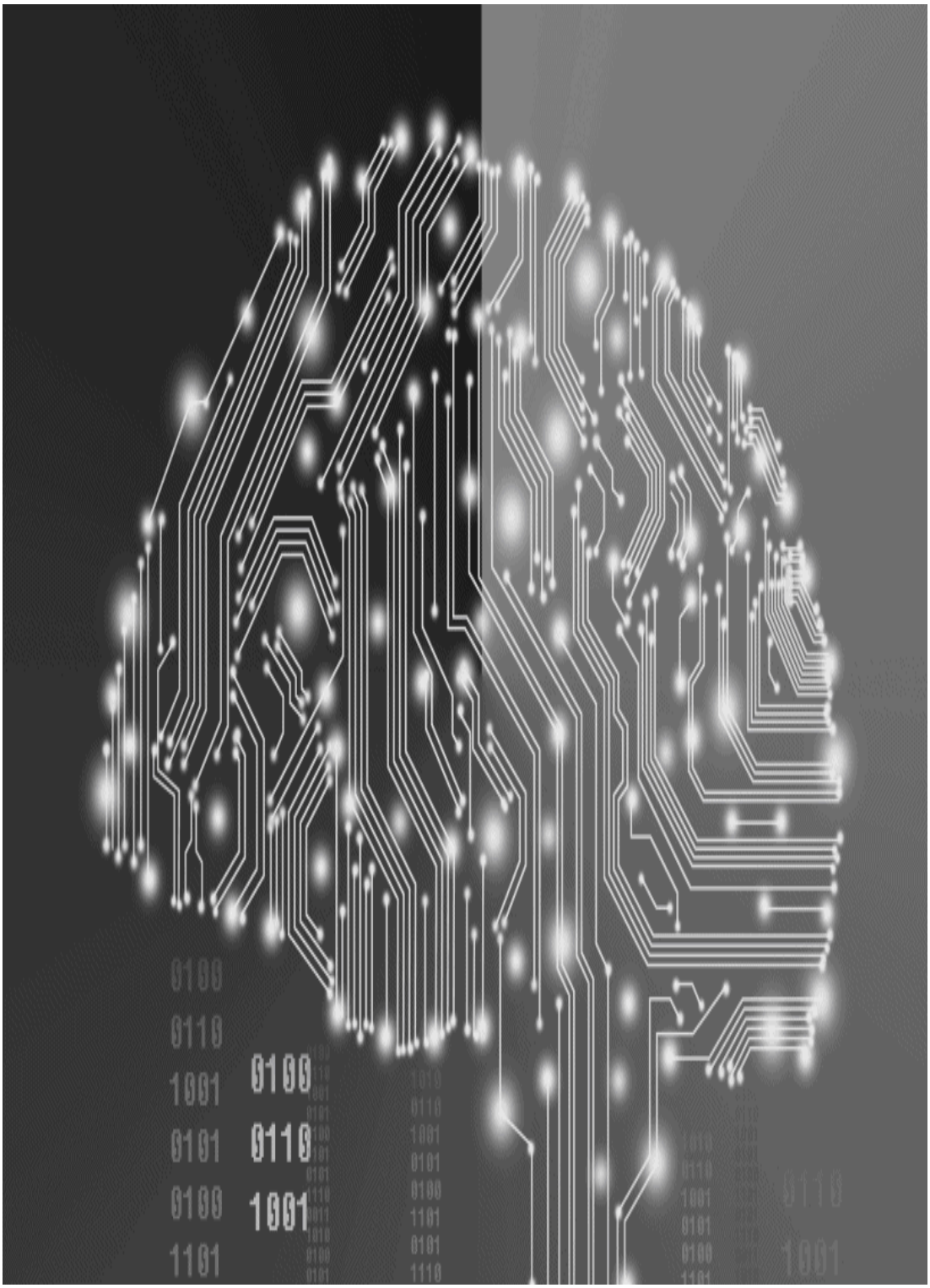
Rosenberg, Richard. "Controlling Access to the Internet: The Role of Filtering." *Ethics and Information Technology* 3, no. 1 (2001): 35–54.

Sandin, Per. "Virtual Child Pornography and Utilitarianism." *Journal of Information, Communication & Ethics in Society* 2, no. 4 (2004): 217–24.

Sellars, Andrew. "Defining Hate Speech." Berkman Klein Center Research Publication, December 8, 2016, **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2882244**.

Sunstein, Cass. ***Republic.com***. Princeton, NJ: Princeton University Press, 2001.

Weckert, John. "What Is So Bad about Internet Content Regulation?" *Ethics and Information Technology* 2, no. 2 (2000): 105–11.



CHAPTER 4

Intellectual Property in Cyberspace

Background on Intellectual Property

Digital and networking technologies have reshaped our artistic and intellectual culture through opportunities for collective creativity and a lack of dependency on established channels of distribution and production. According to some scholars, however, the full potential of this technology has been constrained by intellectual property rights, which should be adapted for this digital milieu. On the contrary, control over copyrighted content seems to be expanding along with the scope of patent protection. As a result, these laws no longer appear to strike the proper balance between the interests of content providers and the needs of users. This excessive protection has prompted a call for sweeping revisions in copyright and patent law, along with strident opposition to the enforcement of those laws in cyberspace.

The issue is further complicated because some legal scholars are convinced that copyright law as currently configured misinterprets the nature of creativity and cultural progress. Nor does it appreciate the complex interrelationships between authorship and usership. Julie Cohen, for example, has reminded us that authors are users

of cultural works before they are creators. She has also argued that broad copyright laws interfere with the good of creative play, which requires "meaningful access to the resources of a common culture."[1] The upshot of her analysis is that more attention should be given to the valid demands of readers and users instead of the exclusive focus on the "romantic author" that shapes the contours of copyright law.

The result of this opposition to the status quo has been a series of well-publicized disputes from Napster and the Digital Millennium Copyright Act (DMCA) to abortive efforts to deal with antipiracy, such as the Stop Online Piracy Act (SOPA). There are repeated calls for a new networked space that gives far greater latitude to the consumers of intellectual property. Lessig, a longtime champion of digital creativity and "free culture," has maintained with some insistence that users should be given broader fair use rights in order to blunt the encroachment of a "permission culture."[2] This less restrictive regime will enhance creativity in the long run. The current legal restraints on "sampling" and remixing music, for example, could have lasting negative effects on musical creativity.

At the core of these controversies is a deep-running conflict between a "free culture" and a culture that continues to give ample recognition to

the rights of creators and content providers. *Which culture should a regime of intellectual property rights seek to favor?* Many supporters of the “free culture” movement suppose that there is a sharp discontinuity between the predigital and digital eras. They see intellectual property law as encumbering the openness and creative energies unleashed by the Net. While sympathetic to some of these arguments, traditionalists maintain that it would be misguided to allow this new technology to determine the structure and moral requirements of intellectual property law. To do so is to fall victim to a form of technological determinism that does not take adequately into account the reasonable ownership claims of creators. The rationale for intellectual property policies should not be determined by the technological imperative of digital systems that facilitate the production and distribution of information. We cannot lose sight of the creator, the laborer, who still has to expend time and energy to create new content in this digital environment and who still deserves limited property rights for his efforts.[3]

In this chapter, we will provide some perspective on all of these matters from both a moral and a legal vantage point. It seems fitting that we begin by providing an overview of the framework of relevant laws that protect intellectual property

along with an account of the most plausible moral grounding of those laws. There are several normative frameworks for conceptualizing these issues that serve as a foundation for intellectual property law. Economic analysis is also important, but it must be supplemented by these theories because it lacks normative sufficiency. These frameworks are based on the work of philosophers such as Locke, Hegel, and Mill. In addition, we must consider what combinations of law, code, market forces, and social norms are most appropriate in order to effectively regulate property in cyberspace without undermining the common good.

What Is Intellectual Property?

It is logical to begin this analysis with a workable definition of property and an overview of its central role in a well-ordered society. Property is at the cornerstone of most legal systems, yet it is a murky and complex concept that defies a simple definition.

Most philosophical analyses equate the notions of *ownership* and *property.* Hence, the statements “I own that house,” and “That house is my property,” are equivalent because they convey the same information. Further, those analyses define ownership as “the greatest possible interest in a thing which a mature system of law recognizes.”[4] More simply, ownership of property implies that the owner has certain rights and liabilities with respect to this property, including the rights to use, manage, possess, exclude, and derive income. This is consistent with our legal tradition, which has long recognized that ownership encompasses a number of rights known as the “Blackstonian Bundle,” named after William Blackstone, who summarized these rights in his famous 18th-century *Commentaries.* According to Blackstone, the owner has the right to exclude anyone from the property, to use it as he or she sees fit, to receive income derived from that property, or to transfer the property to someone else.

Intellectual property consists of “intellectual objects,” such as original musical compositions, poems, novels, inventions, product formulas, and so forth. Although the use of physical objects is a zero-sum game in the sense that my use of an object prohibits others from using it, the same cannot be said of intellectual objects. They are nonrival goods because they can be used by many people simultaneously and their use by some does not preclude their use by others. My appropriation of a special recipe for pasta primavera does not preclude others from enjoying that same recipe. Furthermore, although the development and creation of intellectual property objects may be time consuming and costly, the marginal cost of making copies is usually negligible.

Some of these characteristics make intellectual property rights more difficult to define and justify, especially in open democratic societies that prize free expression and the free flow of ideas. Assigning property rights to nonrivalrous intellectual objects seems antithetical to many of the goals and traditions of a free society. Those who oppose strong copyright protections often appeal to the First Amendment, along with the need for maximum vitality in the marketplace of ideas as a rationale for their opposition.

Nonetheless, for reasons that should become obvious as this chapter proceeds, there is strong warrant for extending limited property rights to the intellectual realm. On its face, an intellectual property right appears to be inappropriate, because it implies that someone has the right to certain concepts, knowledge, or ideas. Assigning a property right to an idea excludes others from using and building upon those ideas. But this problem is resolved by distinguishing between the idea and its expression, and granting copyright protection to the expression of an idea but not to the idea itself. If we can make these important distinctions and develop intellectual property rights with reasonable limits, it should be possible to protect individual authors without depleting the public domain.

Legal Protection for Intellectual Property

In the United States, the roots of intellectual property law can be traced back to the Constitution. The Founding Fathers recognized that such protection was necessary for commercial and artistic advancement. Consequently, the U.S. Constitution confers upon Congress the power “to promote the Progress of Science and the useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.”[5] Specifically, Congress has traditionally chosen to follow this mandate by granting limited copyright and patent protection. We review next how copyright and patent protection applies in cyberspace, and we include in this résumé a third category of trademark protection, because it is pertinent for many of the property conflicts that have surfaced in cyberspace.

Copyright Laws

Copyright laws give authors exclusive rights to their works, especially the right to make copies. Copyrights now last for an author's lifetime plus 70 years. Copyright protects a literary, musical, dramatic, artistic, architectural, audio, or audiovisual work from being reproduced without the permission of the copyright holder. Copyright law also gives the copyright holder the right "to prepare derivative works based upon the copyright works" and "in the case of literary musical, dramatic, choreographic works, pantomimes, and motion pictures and other audiovisual works, to perform the copyrighted work publicly."[6]

To be eligible for copyright protection, the work in question must be original, that is, it must be independently created by its author. Originality does not mean that the work has to be novel or possess any aesthetic merit. The work must also be fixed in some tangible medium of expression. Thus, a dance such as the tango cannot be copyrighted, but a visual recording of that dance is eligible for copyright protection. Also, it is important to underscore that copyright protection extends to the actual concrete expression of an idea, but not to the idea itself. Copyright laws, therefore, do not protect ideas, concepts, facts,

generic plots or characters, algorithms, and so forth.

Copyright protection has certain limitations considered to be in the public interest. One such limitation or “safety valve” is the “fair use” provision.[7] For example, copyrighted literary works can be quoted and a small segment of a video work can be displayed for limited purposes, including criticism, research, classroom instruction, and news reporting. Fair use would probably allow a teacher to reproduce and distribute several pages from a book to her students, but it would not allow reproduction and distribution of the whole book. Parody is another form of fair use. In *Campbell v. Acuff-Rose* the court ruled that a rap parody of “Pretty Woman” constituted fair use.[8] Also, making private copies of certain material is considered fair use. For example, in *Sony v. Universal* the U.S. Supreme Court affirmed that consumers can engage in “time shifting,” that is, making a video copy of a television program to watch at another time.[9]

Another restriction is the first sale doctrine. The first sale provision allows the purchaser of a copyrighted work to sell or lend that copy to someone else without the copyright holder’s permission. These limits on copyright law are

designed to balance the rights of the copyright holder with the public’s interest in the broad availability of books and other artistic works.

Patents

Whereas copyright protection pertains to literary works, patents protect physical objects like machines and inventions, along with the inventive processes for producing some physical product. A *patent* is "a government grant which confers on the inventor the right to exclude others from making, using, offering for sale, or selling the invention for what is now a period of 20 years, measured from the filing date of the patent application."[10]

To be eligible for a patent, the invention must be novel, that is, unknown to others or unused by others before the patent is awarded; also, it cannot be described by others in a printed publication. It must also satisfy the criterion of "nonobviousness," that is, it cannot be obvious to anyone "skilled in the art" or it is not patentable. The invention must also be useful in some way. The proper subject matter for a patent is a process, machine, or composition of matter. Laws of nature, scientific principles, general algorithms, and so forth belong in the public domain and are not eligible for patent protection.

The scope of patent protection has been expanded significantly over the last several decades. For example, patents are now awarded for new plant varieties developed through experimentation. Patents are also awarded for

surgical procedures under certain circumstances. Although software was previously considered ineligible for patent protection, thanks to the case of *Diamond v. Diehr*, that has changed. In that landmark case, the court ruled that a patent claim for a process should not be rejected merely because it includes a mathematical algorithm or computer software program. In this case “the majority opinion of the Court concluded Diehr’s process to be nothing more than a process for molding rubber products and not an attempt to patent a mathematical formula.”[11] In other words, the process itself (in this case one for curing rubber) must be original and hence patentable, and if computer calculations are part of the process, then they are included in the patent protection. Subsequent cases have affirmed that any software program is patent eligible.

Patents have been the subject of some concern and criticism in certain circles. Because a patent gives the patent holder virtual monopoly power for a long period of time, it enables the producer to charge high prices and reap monopoly rents. This has been a source of contention, especially for the pharmaceutical industry. Indigent patients sometimes cannot access life-saving drugs because the price is too high. On the surface, patent protection may seem anticompetitive, but,

without it, would companies have the financial incentive to invest hundreds of millions of dollars to discover new drugs or invent other innovative products? Western capitalism has assumed that these incentives are essential in order to ensure a steady supply of breakthrough inventions that will benefit society in the long run.

Trademarks

The final form of legal protection for intellectual property objects is the *trademark,* which is a word, phrase, or symbol that pithily identifies a product or service. Examples abound: the Nike “swoosh” symbol, names like Pepsi and Dr. Pepper, and logos such as the famous bitten apple image crafted by Apple Computer. To qualify for the strongest trademark protection, the mark or name must be truly distinctive. In legal terms, *distinctiveness* is determined by several factors, including the following: Is the trademark “arbitrary or fanciful,” that is, not logically connected to the product (e.g., the Apple Computer logo has no connection to a computer); and is the trademark powerfully descriptive or suggestive in some way?

A trademark is acquired when someone is either the first to use the mark publicly or registers it with the U.S. Patent Office. Trademarks do not necessarily last in perpetuity. They can be lost if one squanders a trademark through excessive or improper licensing. They can also become lost if they eventually become generic and thereby enter the public domain. According to the terms of the Federal Trademark Act of 1946 (the Lanham Act), trademarks are generally violated in one of three ways: infringement, unfair competition, or dilution. *Infringement* occurs when the trademark is used

by someone else in connection with the sale of its goods or services. If an upstart athletic shoe company tried to sell its products with the aid of the “swoosh” symbol, it would be violating Nike’s trademark. The general standard for infringement is the likelihood of consumer confusion. Trademark owners can also bring forth legal claims if their trademarks are diluted. *Dilution* is applicable only to famous trademarks that are distinctive, of long duration, and usually known to the public through extensive advertising and publicity. Dilution is the result of either “blurring” or “tarnishment.” *Blurring* occurs when the trademark is associated with dissimilar products—for example, using the Disney trademark name to sell suits for men. *Tarnishment* occurs when the mark is portrayed in a negative or compromising way or associated with products or services of questionable value or reputation.

Trademark law does allow for fair use of trademarks and also use for purposes of parody. In fair use situations the trademark name normally assumes its primary (vs. commercial) meaning; for example, describing a cereal as comprised of “all bran” is different from infringing on the Kellogg’s brand name “All Bran.” Parody of trademarks is permitted as long as it is not closely connected with commercial use. Making fun of a well-known brand in a Hollywood skit is probably acceptable,

but parodying that brand to sell a competing product would most likely not be allowed.[12]

Moral Justifications for Intellectual Property

We have considered the various forms of legal protection for intellectual property, and we now turn to the underlying philosophical and moral justifications for these laws. It is important to understand the foundation for the legal infrastructure supporting intellectual property rights. Certainly many theories of property have been put forth, but those with the greatest intellectual resonance can be found in the philosophical writings of Locke and Hegel and in the philosophy of utilitarianism. Locke is credited with providing the philosophical underpinnings of the labor desert theory and aspects of Hegel's thought form the basis for the so-called "personality theory." Utilitarianism provides the most pragmatic philosophical approach that has been particularly appealing to economists who support robust intellectual property rights. We briefly review the main principles of each framework.

Locke's Labor Theory

Locke's labor theory of "appropriation" has undoubtedly been the most influential property theory in the entire philosophical tradition. He defends private property rights on purely normative grounds and without utilitarian considerations. According to Locke, a person has a property right, that is, the right to exclude others, in himself, in his labor, and therefore in the products of that labor. Locke relies on this theory, justified by this thesis of self-ownership, to demonstrate why a claim to ownership is warranted when someone adds his or her labor to common resources. As Locke explains,

> Man has a Property in his own person. This no Body has any right to but himself. The Labor of his Body and the Work of his Hands we may say are properly his. . . . Whatsoever then he removes out of the State that Nature had provided . . . he hath mixed his Labor with and joined to it something that is his own, and makes it his Property.[13]

At the core of Locke's argument is the principle that a person, who possesses her own body and the labor produced by it, validly claims a property right by virtue of his or her transformation of pre-existing, common resources through the expenditure of that labor. Labor transforms this unorganized material into a useful, creative

product and provides the ground for a valid appropriation of that product. As Merges observes, “labor, directed to a useful end, justifies private appropriation,” which removes objects from the tangible commons and brings them under a person’s control so they can be of more use.[14]

Locke’s theory applies both to physical and intellectual property, because production of the latter also involves creative effort and labor. In this case, the relevant resource is the common knowledge available to all that exists in the unorganized public domain (facts, ideas, plots, algorithms, and so forth). Through intellectual labor, an author crafts an original work by transforming these starting materials into a new creation. This transformative labor entitles the author to have a property right in the finished product such as a novel, a software program, or a musical composition. According to this Lockean perspective, it is fair and just that an author “appropriate” and exclude others from her literary work that she has created through her labor.

However, although Locke believed in property rights based on labor he did not support unlimited rights. Locke insists on an important condition limiting the acquisition of property, which is referred to as the sufficiency proviso. According to this principle, one cannot appropriate an object

from the commons through labor unless there remains enough resources of the same quality for others to appropriate. As Locke explains, “For this Labor being the unquestionable Property of the Laborer, no Man can have a Right to what that is once joined to, at least where there is enough, and as good, left in common for others.”[15] This proviso, which should apply to both physical and intellectual property, clearly limits the right to appropriate property. Appropriators, therefore, must leave sufficient resources and “equal opportunity” for others, though some commentators on Locke have suggested a more flexible limitation such that an appropriation should not worsen the situation of others.[16]

Adam Moore frames this proviso in terms of weak Pareto superiority, which permits individuals to better themselves through a claim of ownership as long as no one is made worse off in the process. In cases where no one is harmed by such a claim, it is “unreasonable to object to a Pareto-superior move.”[17] If the appropriation of an intangible work makes no one worse off in social welfare terms, compared to how they were before the appropriation, then an intellectual property right is valid. Thus, for intellectual property, an author’s property right cannot diminish the ideas and concepts in the public domain—the same “starting

materials” must be left for other creators to use. For the vast majority of intangible or literary works, such as novels, musical scores, or software programs, the proviso is satisfied by the current legal structure: no one is made worse off by awarding the author a property right, since that right is given to the fresh expression of an idea and not to the idea itself.

The Lockean theory may seem archaic, a source of hoary debates about the moral worth of work, but it echoes through many U.S. court decisions about intellectual property. Listen to the eloquent words of Justice Reed, who served on the U.S. Supreme Court in the 1950s: “Sacrificial days devoted to . . . creative activities deserve rewards commensurate with the services rendered.”[18]

Personality Theory

The basis of the second approach is that property rights are essential for proper personal expression. This theory has its roots in Hegel's philosophy, which describes how "a person must translate his freedom into an external sphere."[19] Hegel argued that property was necessary for the realization of freedom, as individuals put their personality into the world by producing things and engaging in craftsmanship. According to Reeve, "Property enables an individual to put his will into a 'thing.'" Property rights enable the will to continue objectifying itself in the world by insulating its "self-actualization from the predation of others."[20]

Property, then, is an expression of one's personality, a means of self-actualization. This theory seems particularly apt for intellectual property. As human beings freely externalize their will in various things such as novels, works of art, poetry, music, and even software source code, they create property to which they are entitled because those intellectual products are a manifestation of their personality or selfhood. One recognizes oneself in these productions. They are an extension of a person's being and as such they belong to that person. Although not all types of intellectual property entail a great deal of personality, the more creative and individualistic

are one's intellectual works, the greater one's "personality stake" in that particular object and the more important the need for some type of ownership rights.[21]

Utilitarianism

The final approach assumes that utilitarian or instrumental arguments should be the basis for determining property entitlements. The main thesis is that copyright and patent protection maximize social welfare. This theory has several variations, but the underlying premise is that society must offer premium rewards to creators and inventors of certain works or those works will not be created. According to the Landes/Posner model, because most intellectual products have very low costs of production, there is a risk that creators will not be able to cover the "costs of expression" (e.g., the high upfront expense involved in writing a novel, producing a music album, or writing the source code of a software product). Creators will be reluctant to author such socially valuable works unless they have ownership rights or the exclusive prerogative to make copies of their productions. Through financial incentives, intellectual property rights induce creators to develop works they would not otherwise produce without this protection, and this contributes to the general good of society.[22]

The problem is that these information-based products that are the subject of intellectual property rights have the characteristic of nonexcludability, that is, it is difficult to exclude those who haven't paid. Novels and movies can be

copied and pharmaceutical products can be reverse-engineered. Thus, without the protection of intellectual property rights, free riders can appropriate the value created by innovators and thereby undermine the incentive to innovate. For example, without a patent, company Y could reverse engineer company X's new drug, developed at great expense, and drive down the market price to the marginal cost of production. At that low price, company X would be unable to recover those big upfront research and development costs. Hence, without the prospect of patent protection, company X will not develop the new drug. The U.S. Supreme Court has clearly enunciated the utilitarian rationale underlying intellectual property law, whose purpose is "to afford greater encouragement to the production of literary [or artistic] works of lasting benefit to the world."[23]

Others have stated the utilitarian theory more simply: we should provide enough intellectual property protection to serve as an inducement for future innovation. It is unlikely that Microsoft will invest $2 billion in an operating system, that Disney will make expensive movies, or that pharmaceutical companies will invest hundreds of millions of dollars in new drug development unless they can be guaranteed the right to get a return on

their investment by controlling access to their innovations, at least for a limited time. Hence the need for some type of protection to spur creativity, especially when creative innovations require a large initial investment.

Recent Legislation

The Digital Millennium Copyright Act (DMCA)

The Digital Millennium Copyright Act (DMCA) is undoubtedly one of the most significant pieces of intellectual property law to be passed within the 25 years. This law was enacted by the U.S. Congress in September 1998. The heart of this bill is its anticircumvention provision, which criminalizes the use of technologies that circumvent technical protection systems, such as an encryption program.

There are two types of anticircumvention rules in the DMCA. The first rule [§1201(a)(1)(A)] outlaws the act of circumventing “a technical measure that effectively controls access to a [copyrighted] work.” For example, if a copyright owner uses a digital rights management system or some type of encryption code to protect a digital book from unauthorized users, it is illegal for anyone to break the encryption and access the book without the copyright holder’s permission.

The DMCA also makes it illegal to manufacture or distribute technologies that enable circumvention. As Section 1201(a)(2) indicates: “No person shall . . . offer to the public, provide, or otherwise traffic in any technology that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected [under the Copyright

Act].” According to Ginsburg, “if users may not directly defeat access controls, it follows that third parties should not enable users to gain unauthorized access to copyrighted works by providing devices or services (etc.) that are designed to circumvent access controls.”[24] A Moscow company, Elcom, Ltd., ran afoul of the DMCA with a software program called Advanced eBook Processor that enabled users to remove security restrictions on Adobe’s eBook files. Once those restrictions were removed, an eBook file could be easily copied and transmitted throughout cyberspace.

The DMCA carefully distinguishes *access* controls from *use* controls. Section 1201(b) proscribes the provision of technologies that enable one to bypass a technology measure (such as a use control) protecting the “right of a copyright owner under [the Copyright Act] in a work or portion thereof.” But there is no counterpart to section 1201(a)(1)(A) for circumventing these copy controls. Thus, although it is unlawful to circumvent to gain unauthorized access to a work, one can apparently circumvent to make fair use of a work that one has lawfully acquired.

There are narrowly tailored exceptions to this statute for legitimate encryption research and for computer security testing. In both cases the

acquisition of the content involved must have been lawful. There is also an exception for interoperability: Companies can circumvent technical measures if it is necessary to develop an interoperable computer program (see DMCA, §1201[f]).[25]

Another issue addressed in the DMCA is *intermediary liability,* that is, the liability of third parties for the copyright infringements of others. There have been some adjustments made in the law of contributory infringement for Online Service Providers (OSPs). According to the DMCA (§512), these OSPs qualify for immunity or "safe harbor" from secondary liability, that is, for copyright infringement committed by their users. They must be willing to terminate service to repeat copyright infringers and remove material from their sites once they are put on notice that the material infringes copyright.

Criticism of the DMCA has been vociferous since the bill became law. Experts claim that the regulations are ambiguous, complicated, and imprecise. One apparent problem with this law is that it makes access to copyrighted works for fair use purposes difficult. Although it appears that the DMCA allows circumvention of a technical protection system for the sake of fair use, "it is less clear whether fair use circumventors have an

implied right to make software necessary to accomplish fair use circumventions."[26]

The Sonny Bono Copyright Term Extension Act
Another controversial piece of legislation signed into law in 1998 is the Copyright Term Extension Act (CTEA). Some cynics say that this law was a response to Disney's anxiety about the famous cartoon character Mickey Mouse. Mickey Mouse was scheduled to become part of the public domain in 2004. To prevent this, Disney, along with other media companies like Time Warner, heavily lobbied for this legislation. The CTEA extends the term for copyright protection for 20 years, so Mickey is safe once again—at least until 2024.

Initially, copyright protection as provided by the U.S. Copyright Act of 1790 was for a 14-year term, renewable for an additional 14-year term. In 1909 the term for copyright became 28 years with a one-term extension for a possible total of 56 years. The 1976 Copyright Act established the term of life of the author plus 50 years for individual authors and 75 years for corporate authors (e.g., for companies such as Disney). The CTEA extends these terms by 20 years, so protection for individual authors is now the life of the author plus 70 years and for corporate authors 95 years. When the copyright expires, the work enters the public domain. Once in the public domain, works can be reproduced and distributed without permission and derivative works can be created

without the need for the copyright holder's authorization.

Proponents of the CTEA argued that passage of this legislation was noncontroversial and would have a positive impact on the industry. But critics claimed that it hurts the public domain, where almost no new works will be transferred thanks to this extension. That criticism and dismay culminated in a lawsuit filed by Eric Eldred, who owns Eldritch Press, which makes works in the public domain freely available over the internet. The case, known as *Eldred v. Ashcroft* (2003) became a *causew celebre* for lawyers at the Harvard Law School, who pursued it all the way to the U.S. Supreme Court. The plaintiff's main argument is that the CTEA hurts individuals like Mr. Eldred, who depend on the public domain. Popular culture itself also depends heavily on a public domain that is being renewed with new creative works for others to draw upon as inspiration. Leonard Bernstein, for example, was clearly inspired by Shakespeare's *Romeo and Juliet* when he composed the musical *West Side Story.* Disney itself has benefited immensely from works in the public domain such as Hans Christian Andersen's *The Little Mermaid*. Great art and literature also depend on the commons, and on the ability of the artist to dynamically recreate past

traditions. As T. S. Eliot wrote, no artist or poet "has his complete meaning alone."[27] These arguments did not prevail at the Supreme Court, however, which ruled in 2003 that Congress had the prerogative to extend copyright protection by an additional 20 years.

Nonetheless, when the CTEA is examined through the lens of intellectual property theory, its justification is dubious. The current term seems like an ample reward for one's work, and utilitarian reasoning is unlikely to yield positive arguments on behalf of the CTEA. It is difficult to argue that this retrospective increase in copyright protection will provide a further inducement to creativity. Does an individual or author have a bigger incentive if the copyright on her creative work extends for 70 years after her death instead of 50 years? According to one court decision, "[a] grant of copyright protection after the author's death to an entity not itself responsible for creating the work provides scant incentive for future creative endeavors."[28] Further, the damage done to the public domain seems to far outweigh any "scant" incentives created by this law. One could certainly argue that this law overprotects property and that it is not in the best public interest. Given the importance of the public domain's vitality for the common good, there is a moral imperative to

ensure that this supply of cultural resources is not disrupted by laws that go too far in protecting individual rights.

Issues for the Internet and Networking Technologies

Copyright and the Digital Dilemma

Now that we understand the legal framework for intellectual property protection along with its philosophical underpinnings, we can turn to a description and assessment of the most salient issues in cyberspace.

We begin with the challenge to copyright protection and the problem of the digital dilemma. Music and movies are particularly vulnerable because they can be represented in digital format, and they are in great demand by young audiences.

Digital Music and Movies

The rise of digital music has been made possible by a protocol known as MP3. MP3 is an audio compression format that creates near CD-quality files that are as much as 20 times smaller than the files on a standard music CD. Whereas standard music files require 10 megabytes for each minute of music, MP3-formatted files require only 1 megabyte. Thanks to MP3, digital music can now be accessed and transmitted over the internet without a physical container such as a compact disk.

This revolutionary distribution method has propelled the music industry into chaos, but it does have certain key advantages. Authors, composers, and performers can publish and distribute their music online without the assistance of recording companies. This low-cost distribution method creates benefits for both the creators of music and their customers. Downloading digital music is certainly more convenient for customers than purchasing it in retail stores or through mail order. And, as Fisher points out, this mode of music distribution tends to promote “semiotic democracy.” The “power to make meaning, to shape culture” will no longer be so concentrated.[29] Rather, it will be more dispersed among a broader range of musicians and artists who do not need to

sign a contract to produce and distribute their music.

The downside of this system, of course, is the potential for piracy. Because MP3 files are unsecured, they can be effortlessly distributed and redistributed in cyberspace. The music industry's response to this problem of "containerless" music has been predictable. They have doggedly pursued the operators of websites that promote digital music file sharing like **MP3.com**, along with intermediaries like Napster or peer-to-peer (P2P) networks, such as KaZaA.

It is instructive to consider the case of Napster, where many of the moral and legal issues about sharing digital music first surfaced. Napster was the creation of Shawn Fanning, a Northeastern University student, who left after his freshman year to write this celebrated piece of software. This software operated by allowing a Napster user to access the systems of other Napster users to search for a particular piece of music as long as they had installed Napster's free file-sharing software. Once that music was located, it could be downloaded directly from that system in MP3 format and stored on the user's hard drive. Napster did not store or "cache" any digital music files on its own servers, and it was not involved in any copying of music files. Napster did, however,

maintain a central directory of the music available among all Napster users.

In December 1999, the Recording Industry Association of America (RIAA) sued the company for vicarious and contributory copyright infringement, demanding $100,000 each time a song was copied by a Napster user. Several months later, the rock band Metallica also sued Napster. The RIAA was particularly anxious about the precedent of allowing copyrighted music to be exchanged so freely and openly. In its main brief, the RIAA summed up the problem quite clearly: “If the perception of music as a free good becomes pervasive, it may be difficult to reverse.”[30]

Despite a superb legal team led by David Boies, Napster did not fare well in these legal proceedings. In the summer of 2000, Judge Mona Patel granted the RIAA’s request for a preliminary injunction ordering the company to shut down its file-sharing service. But 2 days later, the U.S. Court of Appeals for the Ninth Circuit stayed the injunction so that Napster could have its day in court.

During the trial, the plaintiffs argued that a majority of Napster users were downloading and uploading copyrighted music. They estimated that 90% of the music downloaded by Napster users was

copyrighted by one of the recording labels that were a party to this lawsuit. These actions constituted direct infringement of the musical recordings owned by the plaintiffs. And because Napster users were culpable of direct copyright infringement, Napster itself was liable for contributory copyright infringement for facilitating the illegal copying. Also, because Napster stood to profit from the actions of its users (through advertising or monthly charges), it incurred liability for vicarious copyright infringement, which applies when one "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities."[31] Both contributory and vicarious infringement are considered forms of secondary liability for copyright violations.

In its defense Napster presented several key arguments. It invoked the protection of the 1998 DMCA, which provides a "safe harbor" against liability for copyright infringement committed by customers of intermediaries or "information location tools" (e.g., search engines). Napster contended that it was merely a search engine and therefore deserved to be protected by the DMCA (§ 512). Napster also argued that a significant percentage of the system's use involved legally acceptable copying of music files. According to Napster, many songs were not copyrighted and

others were being shared between users in a way that constituted fair use. According to trial documents, “Napster identifies three specific alleged fair uses: sampling, where users make temporary copies of a work before purchasing; space-shifting, where users access a sound recording through the Napster system that they already own in audio CD format; and permissive distribution of recordings by new and established artists.”[32] There are four factors that help the court determine fair use: (1) the purpose and character of the use (e.g., commercial use weighs against the claim of fair use); (2) the nature of the copyrighted work (e.g., creative works receive more protection than factual ones); (3) the “amount and substantiality of the portion used” in relation to the work as a whole; and (4) the effects of the use on the market for the work (“fair use, when properly applied, is limited to copying by others which does not materially impair the marketability of the work which is copied”[33]). All of these factors are weighed together and decisions are made on a case-by-case basis.

Napster argued that its users often downloaded MP3 files to sample their contents before making a decision about whether to make a purchase. Hence, according to this line of reasoning, Napster’s service could even help promote sales

of audio CDs. *Space shifting* occurs when a Napster user downloads MP3 files to listen to music they already own on an audio CD. Napster was analogizing its technology to the videocassette recorder. In the 1984 case of *Sony v. Universal City Studios,* the U.S. Supreme Court exonerated Sony from liability for the illegal copying that could occur by means of its VCR technology. It also held that in general VCRs did not infringe copyright because viewers were engaged in *time shifting*, that is, recording a television show for viewing at a later time. According to Greene, "Relying on the Sony decision, Napster attempted to establish that its service has substantial noninfringing uses and that Napster users who download copyrighted music, like VCR users who record copyrighted television programming, are entitled to a fair use defense."[34]

Despite the ingenuity of Napster's defense, these arguments did not persuade the U.S. Court of Appeals for the Ninth Circuit, which found that "the district court did not err; Napster, by its conduct, knowingly encourages and assists the infringement of plaintiffs' copyrights."[35] It rejected the fair use claim, concluding that Napster had an adverse effect on the market for audio CDs, especially among college students. However, the appeals court found that the preliminary injunction

was “overbroad,” and it placed a burden on the plaintiff to provide Napster with proper notice of copyright works and files being shared on the Napster system “before Napster has the duty to disable access to the offending content.”[36] In light of this ruling, Napster changed its business model by converting to a subscription music service similar to Apple iTunes.

Another architecture that has facilitated this new mode of music distribution is the peer-to-peer or P2P network. These networks can also be used to share digital movies and other copyrighted content. Unlike the server-based technology, where distribution to clients emanates from a central server, with P2P any computer in the network can function as the distribution point. In this way, the server is not inundated with requests from multiple clients. For example, a user can prompt his or her personal computer to ask other PCs in a P2P network if they have a certain digital file. With a typical P2P program, one simply enters the name of a movie, song, or other type of content into the search box. That request is passed along from computer to computer within the network until the file(s) are located; what’s returned is a directory of all the computers that have the requested content. A few more clicks and the file is downloaded and stored on the user’s

hard drive in a folder that might be called “shared files.” Any digital content file stored in the shared files area becomes available for other users to download, unless this feature is disabled. This functionality is known as *uploading.*

P2P networks require some method of indexing or cataloguing the information available across the network so that user requests for files can be matched with what is available on the network. There are three different methods of indexing: a centralized index system where the index is located on a central server (this was Napster’s method); a decentralized indexing system in which each user maintains his or her own index of the files available for copying by others; and a supernode system, in which a select number of powerful computers within the network act as indexing servers. A *supernode* is a user computer selected by the software provider that has enough power to store the index of available music and provide search capabilities. The centralized method was abandoned after Napster lost the court case defending its technology. The supernode system, developed as part of KaZaA’s FastTrack technology, has become the preferred solution among P2P network providers. There has been some decrease in the use of P2P networks, but they still account for a significant percentage of

downloading and uploading traffic on the Net. These systems facilitate the expedient transmission of all forms of content, including photographs, music, movies, e-books, data files, and documents. The problem with P2P software, however, is that it has enabled massive copyright infringement.

For the entertainment industry, this lethal combination of easily reproducible digital music and movie files and peer-to-peer networks has been a recipe for disaster. As a result, they have intensified efforts to pursue P2P suppliers such as Bit Torrent and LimeWire, claiming that they are no different from Napster, and hence are guilty of contributing to or introducing the copyright infringement of their users. LimeWire was a widely used P2P network with almost 4 million users per day, but in 2010 a U.S. district court held that the company induced copyright infringement and issued a permanent injunction to shut it down.[37] This ruling was consistent with *MGM v. Grokster* in which the Supreme Court held that a P2P network (such as Grokster) can be guilty of contributory infringement if it distributes software used primarily for copyright violations.

The U.S. Justice Department has been aggressive in pursuing the most popular file-sharing sites, such as Megaupload. This site became a primary

conduit for sharing unauthorized copies of movies and videos. Top executives of this company, including Kim Dotcom, were arrested in 2012. The Justice Department has also ordered another file-sharing site, called Hotfile, to pay $80 million in damages to the Motion Picture Association. But critics of these actions insist that the Justice Department is putting the interests of Hollywood over consumers.[38]

What about the moral accountability of those who so unabashedly copy copyrighted files? Is there anything morally wrong with such behavior? Perhaps Kant's moral philosophy can shed some light on this question. If we assume that the theories justifying intellectual property, though indeterminate, have some validity, we must conclude that common ownership of intangible property is impractical and inconsistent with the public good. Property is a practice, and it is "difficult to imagine an economic system in which the means of production and action were not guaranteed to the use of particular persons at particular times."[39] This practice is reasonable for both physical property and intellectual property. For example, if we want to see blockbuster movies from Disney that cost $150 million to produce, it is essential to give Disney some copyright protection. Although some libertarians resist this way of

thinking, most admit that collective ownership of intellectual property, where all creations belong to the intellectual commons immediately, is not feasible. Thus, given the pragmatic necessity of private intellectual property, a universalized maxim that permits stealing of such property as a standard procedure is self-defeating. That maxim would say, “It’s acceptable for me to steal the intellectual property validly owned by the creators or producers of that property.” Such a universalized maxim, which would make it acceptable for everyone to take this property, entails a contradiction because it would lead to the destruction of the entire practice of private intellectual property. Because the maxim allowing an individual to freely appropriate another’s intellectual property does not pass the test of normative universalization, a moral agent is acting immorally when he or she engages in the unauthorized copying of digital movie or music files.

Critics may argue that certain aspects of intellectual property protection make no sense. For example, although they admit that it’s logical to protect big-budget movies with a copyright and pharmaceutical products with a patent, they disagree with giving copyright protection to music. They may be right about this, but every legal

system or practice has what appear to be incongruities or imperfections to some individuals. We cannot pick and choose which laws to follow and which to flout or the practice would disintegrate as everyone followed his or her own idiosyncratic interpretation of the law. It's like saying that I believe that a house is someone's property but things of lesser value like bicycles or clothing are fair game. One can work to modify the copyright laws, but as long as that system has practical significance, one cannot steal another's intellectual property; that act disrespects the whole institution of private intellectual property.

The introduction of the Kantian moral argument into this debate does not preclude other legitimate moral perspectives on the issue. It might be possible for a strict utilitarian to reason that such copying is acceptable when all costs and benefits are calculated. However, if one accepts the set of assumptions we have delineated, the moral argument for respecting all intellectual property rights has considerable persuasive force.

The DeCSS Lawsuit and the “Durable Goods” Cases[40]

In January 2000, eight major Hollywood studios, including Paramount Pictures, Universal Studios, and MGM Studios, filed a lawsuit against three New York men who operated websites distributing DeCSS. The DeCSS program allows a user to circumvent a DVD file’s encryption protection system, known as the content scramble system (CSS) so that the user can copy the DVD file to his or her hard drive. (Movies in digital format are stored on disks known as DVDs.) The suit contended that DeCSS was little more than a “piracy tool” that would be used to produce decrypted copies of DVD movies for distribution over the internet. The lawsuit alleged that DeCSS violated section 1201 of the DMCA, which makes it illegal for anyone to provide technology that is intended to circumvent access controls (such as encryption) that protect literary or creative works.

DeCSS, the plaintiff’s lawyers argued, defeated the purpose of the CSS encryption system by enabling the decryption of copyrighted DVDs without the permission of the copyright holder. All DVDs contain digital information, and digitization allows copies of a motion picture contained on a DVD to be stored on a hard disk drive in the computer system’s memory or to be transmitted

over the internet. Moreover, there is no degradation of quality and clarity when such digital copies are produced. Given that DVDs are so vulnerable to illicit copying, they have been protected with an access control system (CSS) that encrypts the contents. All movies in this digital format are distributed on DVDs protected with CSS. These movies can be viewed only on a DVD player or specially configured PC that has a licensed copy of CSS, which contains the keys for decryption.

If computer users wanted to watch DVD movies on their personal computers instead of a dedicated DVD player, those computers had to be running a Mac or Windows operating system. CSS did not support any other operating system, such as Linux.

In the fall of 1999, Jan Johansen of Larvik, Norway, decided that he wanted to watch DVD movies on a computer that ran the Linux operating system. With the help of two friends he set out to create a software program that would play DVDs on a Linux system. This meant, of course, that it would be necessary to crack the CSS encryption code. Johansen had little trouble doing this, and when he finished writing the DeCSS program he posted it to the web for rapid distribution. Once the

code was released, it was widely distributed, especially among hackers.

The movie industry decided to seek injunctions against certain offenders, and it filed a lawsuit against Eric Corley and two other individuals. Corley operated the 2600 Hacker website, where both the source code and object code of DeCSS were made available. In February 2000, Judge Lewis Kaplan issued a preliminary injunction prohibiting the defendants from posting DeCSS on their respective websites, pending the trial. Following this court order, two of the defendants settled with the movie studios. But the third defendant, Eric Corley, refused to settle and the case continued. Mr. Corley removed the DeCSS code from his website, **www.2600.com**; however, he added links from his site to a number of other target sites that contained the DeCSS software.

In April 2000, lawyers for the movie studios filed a petition with Judge Kaplan urging him to amend his previous order and prohibit Corley from linking to websites that posted the DeCSS code. They argued that although the 2600 website no longer contained a copy of DeCSS, the site was functioning as a virtual distribution center for the DeCSS code by virtue of these links.

As the case, known as *Universal City Studios v. Remeirdes et al.*, continued into the early summer months, the actual trial began. The plaintiffs reasserted their contention that by posting DeCSS on their websites, the defendants violated the DMCA; CSS is a technological measure controlling access to these works. The defense challenged the absolute right of the movie industry to control how DVDs are played. It argued that DeCSS simply preserves “fair use” in digital media by allowing DVDs to work on computer systems that are not running Mac or Windows operating systems. Consumers should have the right to use these disks on a Linux system, and this required the development of a program such as DeCSS. Their contention was that DeCSS existed to facilitate a reverse-engineering process that allows the playing of movies on these unsupported systems. It was not written, they maintained, to facilitate copying or transmitting these disks in cyberspace. In addition, the defense argued that the ban on linking was tantamount to suppressing an important form of First Amendment expression. Links, despite their functionality, are a vital part of the expressiveness of a webpage; therefore, their curtailment violates the First Amendment.

The defense team presented the constitutional argument that computer code itself, including

DeCSS, is a form of expressive free speech that deserves full First Amendment protection. This includes both the source code and object code. A computer scientist appearing as an expert witness proclaimed that an injunction against the use of code would adversely affect his ability to express himself. The opposition countered that computer software is more functional than expressive; that is, it functions like a machine that happens to be "built" by means of source code.

On August 17, 2000, Judge Kaplan ruled in favor of the movie industry, concluding that DeCSS clearly violated the DMCA. A permanent injunction was issued prohibiting the defendants from posting DeCSS or linking to websites containing DeCSS code. In his ruling, Judge Kaplan rejected the notion that the DMCA curtailed the "fair use" right of consumers. He did agree that source code is a form of expressive speech. But, on the other hand, DeCSS does more than convey a message—"it has a distinctly functional, non-speech aspect in addition to reflecting the thoughts of programmers."[41] Hence, it is not worthy of full First Amendment protection.

The case was appealed to the U.S. Court of Appeals for the Second Circuit. In November 2001, that court concluded that there was no basis for overturning the district court's judgment.

Beyond the narrow legal question addressed in this case there are obviously much larger issues pertaining to the First Amendment and its apparent conflict with property rights. To what extent should the First Amendment protect computer source code? Is that code expressive enough to deserve such protection? Is an injunction against DeCSS prior restraint of a public discussion about the functionality of CSS? Does the First Amendment also support a basic “freedom to link,” an unrestricted right to link to other websites, including sites that contain rogue code such as DeCSS?

This case also raises questions about the DMCA law itself. How can “fair use” be preserved if copyrighted material is in encrypted form and programs like DeCSS are outlawed? According to Harmon, critics of the anticircumvention provision “worry that it goes far beyond the specific copyright challenges of the digital age to give copyright holders broad new powers over how the public uses their material.”[42] Is there a better way to balance the rights of copyright holders who rely on protective devices with free speech rights and the fair use concept?

In several more recent cases the courts have sought to limit the scope of the DMCA. In the so-called “durable goods” cases, federal courts have

refused to apply the DMCA to prevent circumvention of access control software embedded in products like printers. In the Lexmark International case, for example, the company sought to protect access to its printers so that non-Lexmark toner could not be installed. But the court ruled that because Lexmark did not encrypt its access control software, it did not “effectively control access” to its printer authentication program. Hence its conclusion that the DMCA did not apply.[43]

Software Patents and Open Source Code

Software is a special form of intellectual property that can be protected by a patent or copyright. Congress included computer software under the category of “literary works” in the Copyright Act of 1976, which was amended in 1980 to include a definition of a computer program. In keeping with copyright jurisprudence, this copyright law protects the expression of an original software program but not general algorithms or ideas that are the basis of that expression.

However, software is different from other forms of intellectual property because it doesn’t fit neatly under any form of intellectual property protection. The source code of software, written in languages such as C++ or Java, is a type of literary creation, implying that copyright protection is most fitting. But software is also functional, and this functionality seems to make it incompatible with copyright law and more suitable for patent protection. On the other hand, software is somewhat different from the type of invention that typically qualifies for a patent because it is not a physical object. The problem, of course, is that software is both useful and literary; it functions like a machine when it processes inputs and outputs, and it is also expressive like a work of art. Its source code resembles a literary work that

deserves copyright protection, but unlike other literary works, it has a functional nature.

Some argue that given its method of derivation and unusual nature, software should not be eligible for patent protection. Opponents of software patents contend that they do not stimulate innovation. They point to companies, like Microsoft and Google, who stockpile patents not to protect products but to discourage competitors from using them. For the courts, the difficulty has always been distinguishing innovative software designs from common ideas or algorithms that are simply embedded into software code. In the 2014 Supreme Court case of *Alice Corp. Ltd v. CLS Bank*, the court did not invalidate software patents but affirmed that "abstract ideas," such as mitigating settlement risk, are not patent eligible merely through "generic computer implementation."[44]

Similarly, Richard Stallman, President of the Free Software Foundation, has argued with great insistence that copyrights should not apply to code. Stallman claims that traditional ownership of software programs is obstructive and counterproductive. Hence, software should be freely available to anyone who wants to use, modify, or customize it. He regards software licensing fees as an enormous disincentive; those

fees exclude worthy users from enjoying the use of many popular programs. The patent and copyright protection regime also interferes with the evolution and incremental improvement of software products. According to Stallman,

> Software development used to be an evolutionary process, where a person would take a program and rewrite parts of it for one new feature, and then another person would rewrite parts to add another feature; this could continue over a period of twenty years. . . . The existence of owners prevents this kind of evolution, making it necessary to start from scratch when developing a program.[45]

Stallman concludes that because the ownership of proprietary programs is so obstructive and yields such negative consequences, the practice should be abolished.

Thanks in part to Stallman's efforts and the ascendancy of the internet, many internet stakeholders have reassessed the propriety and utility of software ownership. As a result, the "open source" movement, once on the fringe of the industry, gained considerable momentum. The open source software model generally means that software is distributed free along with the "source code," which is accessible for modification. Idealists like Stallman believe that proprietary software is immoral because it deprives society of

the knowledge embedded in the source code. Most proponents of this movement, however, do not look at the issue in moral terms. In their view, open source code is not necessarily morally superior to conventional software.

Rather, the open source approach leads to the development of better software code, that is, source code with fewer bugs and more features contributed by the talented programmers who have access to the program.

During the past few decades there has been a noticeable trend among major software vendors to make their code more openly accessible. The prime example is Google's Android system that is used in cellphones made by companies like HTC and Samsung. In addition, the open source code movement has been energized by the limited success of programs such as Apache for web server development, the MySQL database, and the Linux operating system. Any user can download Linux free of charge or purchase Linux for a nominal sum from vendors such as Red Hat. Linux was written by Linus Torvalds when he was an undergraduate at the University of Helsinki.

Open source software (OSS) should be carefully differentiated from so-called freeware, that is, software such as Adobe's Acrobat Reader, which

is distributed to users at no charge. OSS is also usually distributed at no charge, but, unlike freeware, this type of software is distributed with its source code (as well as the executable object code), and the license allows for modifications of that source code and the development of derivative products. A typical open source license includes five key provisions: (1) the freedom to run the program, for any purpose; (2) the freedom to access the source code and modify it; (3) the freedom to redistribute copies of the program; (4) the freedom to release modifications to the public; and (5) copyleft provision.

A *copyleft license* allows a user to redistribute the open source code with modifications or enhancements, but only under the same open source license under which that user received that code. The purpose of this requirement is to prevent users from privatizing that source code, that is, from distributing that code for a fee according to a proprietary licensing scheme. The most widely used license endorsed by Stallman's Free Software Movement is called the GNU GPL (General Public License), which includes this copyleft provision.

The social benefits of open source code derive primarily from its transparency. As we observed, Stallman claims that because OSS exposes the

knowledge contained in source code, it is morally superior to closed software that conceals this knowledge. This argument has begun to resonate with many policy makers throughout the world. The European Commission, for example, has extolled the virtues of open source, noting that its lack of opacity will mean that there are no "backdoors or electronic spy[s] . . . hidden somewhere in the software."[46] Other scholars think that OSS can go a long way to mitigate the digital divide by making software products more readily available in developing countries.[47]

Some promoters of OSS also point to its technical superiority over proprietary code. They presume that the collective programming wisdom available on the internet will help to create software that is of better quality than any single individual or group of individuals in a company could construct. In a highly influential essay entitled "The Cathedral and the Bazaar," Eric Raymond illustrates why a dispersed group of hackers and programmers working on their own ("the bazaar") can develop higher quality software than a more cohesive group of professional, high-paid programmers employed by companies such as Microsoft or Oracle ("the cathedral"). The former approach is far superior because it can tap into the decentralized intelligence of many talented

individuals loosely connected to a program by means of the internet. The core difference underlying the cathedral versus bazaar approach is the latter's capacity for finding and fixing bugs more rapidly. According to Raymond,

> In the cathedral-builder view of programming, bugs and development problems are tricky, insidious, deep phenomena. It takes months of scrutiny by a dedicated few to develop confidence that you've wrinkled them all out. Thus the long release intervals, and the inevitable disappointment when long-awaited releases are not perfect. In the bazaar view, on the other hand, you assume that bugs are generally shallow phenomena—or, at least, that they turn shallow pretty quick when exposed to a thousand eager co-developers pounding on every single new release. Accordingly you release more often in order to get more corrections, and as a beneficial side effect you have less to lose if an occasional botch gets out the door.[48]

What about the future of OSS? Is this a sustainable business model? To some extent, sustainability depends on the availability of programmers willing to contribute their efforts to open source projects. Eric Raymond characterizes the open source community as a "gift culture," because many of its members are motivated by altruistic tendencies.[49] Other proponents of OSS claim that open source programmers are motivated "by love, not money." In addition,

according to Benkler, if open source projects are to be successful, they must offer the prospect of "social-psychological" rewards.[50] They must also manifest modularity so that the work can be divided into smaller, more manageable segments. Finally, there must be some authoritative leadership in the community, someone who can make judgments about which contributions will be accepted and which ones will be rejected.

Digital Rights Management (DRM)

Throughout this chapter we have expressed how difficult it is for intellectual property laws to keep pace with the power and capabilities of the internet. As more and more people gain access to electronic distribution, intellectual property is being devalued through illicit copying in cyberspace. It is difficult for laws to keep up with technology advances, but code itself can complement the law to protect intellectual property.

Digital technology makes it much easier to reproduce, distribute, and publish information. But thanks to code such as encryption, it is also possible to control or enclose digital information to a degree never before possible. When buttressed by laws such as the DMCA that forbid circumvention of these protection systems, the digital content can become hermetically sealed.

One prominent technology that gives content providers enhanced control over their material is known as “trusted systems.” According to Mark Stefik, “trusted systems can take different forms, such as trusted readers for viewing digital books, trusted players for playing audio and video recordings, trusted printers for making copies that contain labels (watermarks) that denote copyright status, and trusted servers that sell digital works on the Internet.”[51] Content providers would

distribute their work in cyberspace in encrypted form in such a manner that they would be accessible only by users with trusted hardware or software.

Rights management systems can also be utilized to determine what rights a user has with regard to content. According to Ku, “used in conjunction with a trusted system, rights management is the ability of a publisher of a work to define what rights subsequent users of her work will have to use, copy, or edit the work.”[52] The combination of these technologies is usually referred to as digital rights management (DRM). DRM secures content by encryption (or some other method) and it stores instructions outlining uses (or rights). Apple’s popular iTunes website relied on DRM (known as Fair Play) to prevent songs from being played on MP3 players other than the iPod.

DRM continues to play a major role in the distribution of content over networked information technologies in the infosphere. These “digital locks” have already proliferated in new but predictable ways. Thanks to the lobbying of content providers like Netflix and the BBC, the World Wide Web Consortium has mandated that browsers contain DRM protocols to ensure that a Netflix movie will be watched only when connected to its service.[53]

Although the trusted system or DRM approach may seem like an ideal solution to the problem of intellectual property protection on the internet, it also poses some unique challenges, such as those that surfaced in the DeCSS case. How can fair use coexist with trusted systems? Do critics, researchers, and teachers need to go through elaborate mechanisms to access and use selected portions of protected material? Further, these systems enable content providers to choose who will access their digital works, and it's possible that some groups might be excluded from viewing or listening to certain material. If DRM is not constructed properly, it could eviscerate the fair use provisions of copyright laws and make creative works less accessible to the general public.

Another problem with DRM is the potential for invasions of privacy. These systems allow content creators to keep precise tabs on who is accessing and purchasing their material. This raises the Orwellian specter of demands for this information from lawyers, government officials, or other curious third parties. Do we really want anyone to keep tabs on which books we read or what kind of record albums we purchase?

DRM systems perfectly illustrate the thesis that code can be more powerful and comprehensive

than law in regulating the internet. Code allows for more foolproof control that is beyond the capability of a more fallible legal system. However, code threatens to privatize copyright law, without the appropriate checks and balances (such as fair use and limited term) that we find in public copyright law.

This problem can be mitigated, however, if these systems are designed and implemented with the proper ethical awareness, that is, with sensitivity to ethical values such as privacy rights. If this code can be developed responsibly and avoid the excesses of overprotection, it could ease the burden on the legal system’s efforts to enforce property protection in cyberspace and minimize future state regulations.

Business Method Patents in Cyberspace

As we observed, the scope of patent protection has broadened considerably during the last several decades. Software, surgical procedures, plant variations, and so forth are now eligible for a patent. But until a few years ago business methods were off limits for this proprietary right. Examples of business methods might include Federal Express's famous hub and spoke delivery system or a bank's money market account. The notion of patenting such things seemed to be folly, an abuse of the patent system.

In the 1990s, however, the Patent and Trademark Office (PTO) began granting patents for some business methods, treating them as process patents. In 1998, the U.S. Court of Appeals for the Federal Circuit ratified the general business method patent in the *State Street Bank and Trust Co. v. Signature Financial Group, Inc.,* case. The *State Street* case upheld a controversial patent granted to Signature Financial Group for a data processing system that was designed to churn out mutual fund asset allocation calculations. The appeals court overturned a lower court ruling and held that the transformation of data by a machine into a final share price was a practical application of an algorithm (and not an abstract idea), because it produced "useful, concrete, and

tangible results."[54] The court stated that business methods were not different from other methods or processes that were traditionally eligible for patent protection. It concluded that "patentability does not turn on whether the claimed method does 'business' instead of something else, but on whether the method, viewed as a whole, meets the requirements of patentability as set forth in Sections 102, 103 and 112 of the Patent Act."[55] The upshot of this case was quite clear: software-enabled business methods (or processes) can be patented as long as they meet the criteria for a patent such as novelty and nonobviousness.

This ruling opened the flood gate for business method patents, and because many of these patents were for online business methods, they became known as "cyber patents." Two of the most prominent examples of such patents included **Priceline.com**'s "name your price" model, and **amazon.com**'s single-click method, which allows qualified customers to make their purchase with one click of a mouse. Priceline's patent has been the subject of intense scrutiny because it is so broad and general. Despite the criticism, Priceline has zealously defended its patent, which it regards as one of the most strategically important assets of the company.

In the fall of 1999, Expedia, Inc., owned by Microsoft, offered its Hotel Price Matcher service. This service bore a strong similarity to Priceline's. The Expedia consumer could name his or her price for a room in a certain locale and Expedia would look for a match among the hotels participating in this service. Priceline promptly sued Microsoft, claiming that Microsoft's Expedia travel service infringed on the Priceline patent, allegedly copying the methods and processes set forth in that patent.

According to Priceline, the patent protection for the "name your price" model was essential to attract "venture capital investment."[56] Lewis suggests a similar argument: "For new businesses attempting to engage in e-commerce, a solid patent can be the determining factor as to whether a venture capitalist invests or does not invest in the entrepreneur's business."[57] In the information age, intellectual assets take on far greater import than physical ones and they become the basis for a corporation's differentiation strategy. It stands to reason that corporations want to protect those valuable assets from being replicated by free riders through patents or other legal mechanisms.

In its complaint for ***Priceline.com*** *v. Microsoft,* the company argued that its invention was the result of an "extended effort" to solve a recurrent

management problem—“the inability of buyers and sellers properly to connect supply and demand.” The Priceline invention helps to resolve the intractable problem of “unfilled demand and unused supply” through a system of buyer-driven electronic commerce.[58] Further, according to Priceline, no one had been able to practically solve this problem until its “name your price” methodology was introduced.

In another case that also attracted considerable attention, a company called MercExchange sued eBay for alleged patent infringement. MercExchange contended that eBay’s “Buy It Now” feature (a button that enables buyers who don’t elect to bid to make an immediate purchase at a higher price) infringes its patent for a similar feature. In 2003, a judge ordered eBay to pay $29.5 million, though it did not enjoin eBay from using the controversial feature. The U.S. Court of Appeals ruled that the lower district court should have granted MercExchange injunctive relief. But, in 2006, the Supreme Court ruled that the lower court was correct in not granting the injunction, signaling that “a more flexible approach is required because of the changing technological landscape.”[59]

Critics of business method patents argue that these methods do not deserve a patent because

they do not require major capital investments. There is a big difference between investing in the process to develop a new pharmaceutical product, which can sometimes cost up to $1 billion, and investing in a method for an online business. Patents also limit competition on the web. Expedia's situation is a case in point—its foray into the online travel business was delayed by the Priceline lawsuit, and a Priceline victory could have created a monopoly in this segment of internet commerce. In addition, companies developing new business models must be constantly on the alert so that they do not inadvertently infringe on a registered business patent. These administrative transaction costs amount to a waste of resources and an impediment to innovation.

The future of cyber patents is unclear because of their controversial nature. In 2010, the Supreme Court denied a patent to the inventors of a mathematical algorithm that enables commodity traders to hedge weather risks, but concluded that business methods were not "categorically excluded" from patent protection.[60] The critical question is whether these patents are really necessary to stimulate innovation in cyberspace. Will future internet companies be constrained by the lack of patent protection for their innovations?

Will investors and venture capitalists be less forthcoming unless they can be assured that the companies in which they invest have exploited patent protection and safeguarded their intellectual assets?

Patents and Smartphones

Users connect to the internet not just by PCs and Apple computers but through many different mobile devices such as computer tablets and smartphones. The patent wars have spread to these popular devices, which usually involve thousands of patents that often lead to chaos and costly litigation for innovators. There are an estimated 50,000 patents involved in the design of both tablets like the iPad and smartphones. Those patents cover the computer chips, the display screen features, and communications features such as the interaction that occurs between the touch of the screen and the underlying operating system. Given the high quantity of patents, it is difficult for innovators to know when or if they have inadvertently infringed on a competitor's patent. Particularly problematic are broad patents awarded for the components of these devices. In order to minimize the potential for expensive litigation, companies often purchase a competitor's or potential competitor's patents.

In the volatile smartphone industry, this contentious patent issue took center stage in a legal confrontation between two giant corporations, Apple, Inc. and Samsung Electronics. In 2011, Apple filed a lawsuit against Samsung, alleging that Samsung's smartphones

and computer tablets were “illegal knockoffs” of Apple’s popular iPhone and iPad products.[61] Apple claimed that Samsung’s products infringed on both its design patents and trademarks. According to Apple’s opening brief, “Samsung is on trial because it made a deliberate decision to copy Apple’s iPhone and iPad. Apple’s innovations in product design and user-interface technology resulted in strong intellectual property rights that Samsung has infringed.”[62] Apple sought $2.5 billion in damages from the South Korean company, an award that would be the largest patent-related settlement in the history of patent litigation.

Samsung claimed that Apple’s designs were not unique and that Apple itself infringed on Samsung’s own patents for transmitting information. It also insisted that Apple was merely attempting to thwart any competition for its iPhone. According to Samsung, “In this lawsuit, Apple seeks to stifle legitimate competition and limit consumer choice to maintain its historically exorbitant profits.”[63]

Some believed that a verdict in Apple’s favor would send a message to consumers that any product (such as the Samsung Galaxy) that has adopted as its platform Android’s open source

operating system (OS) is in some legal jeopardy. They saw the case as a “proxy” for the bigger war between Apple and Google, the company that makes the Android OS.

The issues are complex, but certainly a superficial look at the two products at the center of this dispute, Samsung’s Galaxy 5 and Apple’s iPhone 4, reveals a strong similarity. Accordingly, Apple sought to convince the Court that Samsung had violated its intellectual property rights, including those that determined the “look and feel” of its iPad and iPhone. In a landmark case in the 1990s, Apple lost a similar lawsuit when it claimed that Microsoft’s Windows OS copied the look and feel of the Mac OS. In this case, Apple claimed that the Android OS used by Samsung infringed on patents for Apple’s OS because Android runs apps and accesses information by way of icons that closely resembled the iPhone.[64] For example, Apple contended that Samsung infringed on its 163 “tap-to-zoom” patent and its 915 “scroll vs. gesture” patent. Apple also contended that Samsung directly copied its “rubber banding” technique (patent 381), that is, the functionality that determines how smartphone images “pull away” from the edge and “bounce back” when a user scrolls beyond the edge of the page with his or her finger.[65] Apple argued that infringement of these

features was obvious from using the Samsung products and reviewing the source code.

In support of its case, Apple introduced evidence that Samsung was warned by a panel of outside experts that its smartphones and tablets bore too much similarity to the iPhone and iPad. In addition, Google itself supposedly warned Samsung that its devices were “too similar to Apple” and should be “redesigned” so that they would be more “noticeably different” from Apple’s devices.[66]

Apple was motivated to file this momentous lawsuit by the late Steve Jobs’ public claims that companies using Android to create smartphones and other products were blatantly stealing Apple’s intellectual property. As Jobs confided to his biographer shortly before his death, “I will spend my last dying breath if I need to, and I will spend every penny of Apple’s $40 billion in the bank, to right this wrong. I’m going to destroy Android, because it’s a stolen product.”[67]

The merits of Apple’s case are certainly a matter of some debate, although there is strong evidence to support at least some of Apple’s claims. In August 2012, a California jury found Samsung liable for patent infringement and awarded the Silicon Valley company $1.05 billion in damages. This decision, however, did not end the

smartphone patent wars. Samsung appealed the court's decision and the case was eventually heard by the U.S. Supreme Court. In December 2016, that Court reversed the lower court rulings and sent the case back to a federal appeals court to be relitigated. But in 2018 Apple and Samsung settled their differences, though the terms of that settlement were not disclosed. The larger question, which also surfaces in business method patent cases, is whether or not patents should be awarded for such minor innovations.[68]

Domain Names

Every internet website is identified by a unique domain name such as **www.disney.com**. A domain name is equivalent to a telephone number or an electronic address. Domain names were originally distributed by a company called Network Solutions on a first-come, first-served basis for a small fee. But the oversight of domain name distribution was recently handed over to the Internet Corporation for Assigned Names and Numbers (ICANN), an international, nonprofit organization (see **Chapter 2**). ICANN itself does not actually distribute domain names. That task is delegated to domain name registrars such as VeriSign, but ICANN determines the policies for domain name distribution and selects those firms that qualify as registrars.

There has already been a wide variety of domain name disputes. One of the major problems has been the persistence and ingenuity of cyber squatting. Cyber squatters typically register certain domain names to resell them to organizations that have a claim to the same name for which they own the legal trademark. The activity of cyber squatting is formally defined as “registering, trafficking in, or using domain names . . . that are identical or confusingly similar to trademarks with the bad-faith intent to profit from the goodwill of the

trademark."[69] One of the earliest examples of cyber squatting was Dennis Toeppen's registration of **panavision.com**. Toeppen offered to sell the domain name to Panavision for $13,000, along with his promise not to "acquire any other Internet addresses . . . alleged by Panavision to be its property."[70] Panavision refused to pay the $13,000 and Toeppen responded by registering additional domain names incorporating the Panavision mark. But the court found him liable for trademark infringement and compelled him to relinquish the **panavision.com** domain name. Thus, the typical cyber squatter seeks to register domain names in bad faith to extort a trademark owner.[71]

Even if there is no extortion, cyber squatting can occur through other methods, such as misleading consumers about the origin of goods sold at a particular website (often called "initial interest confusion"). If a new company registers the domain name **www.talbots.biz** and sells a line of women's clothing, consumers might presume that these goods are affiliated with the well-known Talbot's brand, even if the website itself makes no mention of such a connection.

Also, in addition to cyber squatting, reverse domain-name hijacking has emerged as another challenge for regulators. In these cases, a

trademark owner makes an unjustified claim of cyber squatting, and forces a legitimate domain name owner to transfer his or her domain name through legal means. Archie Comic Publications, for example, sought to prevent a family from registering the domain name "**veronica.org**" even though that family planned to use the website for posting material about their daughter whose name was Veronica.[72]

But the most difficult cases involve the registration of a domain name for the purposes of "cyber griping." At the center of these disputes is a conflict between legitimate claims of trademark owners and the free speech rights of critics, or "gripers," who register a trademark to protest an organization's policies or practices. For example, someone might register a domain name such as **www.microsoftsucks.com** to protest Microsoft's behavior. Many companies have objected to these derogatory domain names on grounds that they are dilutive of their trademark, but a persuasive moral case can be made that reasonable (or "unconfusing") noncommercial use of trademarks for criticism and other forms of free expression must be allowed.

The issues generated by these domain name controversies tend to be mired in legal niceties, but there are certainly moral considerations at stake.

At the core of most disputes is a conflict between legitimate claims of trademark owners and the free speech rights of aspiring domain name owners. Should the property right in a trademark hold sway in cyberspace as it does in real space? And, if so, at what point does that right begin to encroach upon free speech rights?

The issues are complicated, but we can begin to sort them out by the examination of a famous paradigm case. The website called **www.scientology-kills.net** carries some trenchant criticism of the Scientology movement and peddles T-shirts with the same epithet. Scientology sued this Colorado website owner for trademark violation claiming that this domain name "dilutes the distinctiveness of the mark," which could "tarnish the reputation of the owner."[73] The free speech issue at stake is whether the domain name itself expresses a viewpoint or opinion. In this case does "scientology-kills.net" constitute an editorial comment about Scientology that should not be suppressed?

The normative and legal issues in this case are difficult to disentangle. The legal issue is dilution, but whether this sort of criticism amounts to dilution is a matter of debate. Should domain names be allowed to express a negative opinion as long as they do not deceive or mislead visitors

to their site? Is this a reasonable place to draw the line in these disputes?

A strong case can be made that suppressing the “scientology-kills” domain name would set a dangerous precedent. The domain name is becoming a medium for expressing one’s editorial opinions and this should be acceptable as long as one does so within certain parameters, that is, without being deceptive or defamatory, and without seeking commercial gains by the unfair leveraging of another’s trademark. The domain name in question is making an observation that Scientology is a dangerous movement; it is an inflammatory remark expressing a debatable and controversial opinion, but it seems to be within the bounds of one’s right to free expression.

To be sure, a trademark is an important property right, a valuable social good that is one side of this moral equation. But on the other side is the normative starting point of the First Amendment right to free speech. Arguably, a website that is (1) not deceiving visitors or seeking commercial gain through its parody of a trademark and (2) responsibly expressing an opinion without defamation should be allowed to use trademarked names like *scientology* as part of a domain name that expresses an idea or particular viewpoint. There may be cases where dilution is so material

that it does become morally relevant, and those cases must be judged accordingly, but overall the common interest seems to be served by giving the benefit of the doubt in some of these disputes to the weightier claim of free speech.

In a different case, Mr. Steve Brodsky, an orthodox Jew from New Jersey, established a website called **www.jewsforjesus.org**. The site had no affiliation with the Jews for Jesus movement, which embraces Jesus as the Messiah and seeks to convert Jews to Christianity. Brodsky's site, however, proclaimed the following message: "The answers you seek are already within your faith." It also provided a link to a site called Jewish Outreach, which reinforces the theological principles of the Jewish faith. The Jews for Jesus organization, whose actual website has the domain name, **www.jews-for-jesus.org**, sued for trademark infringement and won the case. Brodsky was enjoined from using his domain name.

Although this is similar to the Scientology domain name case, it has some new wrinkles and is fraught with a certain degree of moral ambiguity. In the Scientology case, there was no allegation that the domain name itself was deceptive. But according to the Jews for Jesus organization, Brodsky's domain name was blatantly deceptive

and had undoubtedly been chosen for the sole purpose of intercepting those looking for the legitimate website of Jews for Jesus. The organization maintained that this was akin to false advertising because Brodsky was representing a site as something it wasn't. But defenders of Brodsky argue that his use of this domain name should be protected by the First Amendment. Brodsky is not selling a product or a service, but expressing an idea. They contend that in this case trademark law is being invoked to quash free expression. It is difficult to see, however, how this domain name, which is confusingly similar to the Jews for Jesus domain name, expresses an opinion, and hence the free speech defense appears to be on shaky ground.

These two cases are representative of the many disputes that will continue to arise as users stake out and defend property rights in their domain names. One of ICANN's first major initiatives was to develop a procedure for handling trademark disputes, called the Uniform Dispute Resolution Procedure (UDRP). The UDRP has established certain criteria to determine whether an organization has the right to a domain name. The complainant must prove that "the domain name is identical to or confusingly similar to a trademark or service mark to which it has rights." The

complainant must also demonstrate that the registered domain name is being used in bad faith. Paragraph 4(b) of the UDRP lists four circumstances as evidence of bad faith:

i. the domain name was registered primarily for the purpose of selling it to the complainant or a competitor for more than the documented out-of-pocket expenses related to the name; or
ii. the domain name was registered in order to prevent the mark owner from using it, provided that the registrant has engaged in a pattern of such registration; or
iii. the domain was registered primarily to disrupt the business of a competitor; or
iv. by using the domain, the registrant has intentionally attempted to attract users for commercial gain by creating a likelihood of confusion as to source or affiliation.[74]

UDRP seems like a reasonable response to the cyber squatting problem as long as the definition of “bad faith” is not interpreted too broadly so that legitimate free speech rights are impaired. Many credit the UDRP with eliminating the most blatant cases of cyber squatting, and the procedures are generally regarded as equitable. Nonetheless, according to a recent study, 81% of the cases

have been decided in favor of the complainant, that is, the party that holds the trademark.[75] It is difficult to draw any real conclusions from this study without looking at each individual case, but it suggests one requires a pretty convincing case to prevail against the trademark holder.

In addition to the UDRP, the U.S. Congress amended the Lanham Act to deal explicitly with the problem of cyber squatters. The purpose of the Anticyber squatting Consumer Protection Act (ACPA), enacted in 1999, is to make it easier for trademark holders to protect their marks in cyberspace. The ACPA states that:

> A person shall be liable in a civil action by the owner of a mark, if without regard to the goods or services of the parties that person
>
> i. has a bad faith intent to profit from that mark . . .; and
> ii. registers, traffics in, or uses a domain name that is confusingly similar to another's mark or dilutes another's famous mark.[76]

There are nine factors to be considered by a court for determining "bad faith intent" (e.g., was there an intent to divert consumers from the mark owner's website; has the alleged infringer registered multiple domain names confusingly similar to other marks; and so forth).

Like the UDRP, the ACPA seeks to prevent cyber squatters from commercial trafficking in domain names. Its goal is also to stop those who attempt to “defraud consumers [by] engag[ing] in counterfeiting activities.” The scope of the ACPA is broader than the UDRP, because it protects famous marks from dilution, “as well as a person’s private name from bad faith registration.”[77]

The ACPA does not necessarily forbid the registration of domain names including trademarks that are used to mock or criticize an organization as long as there is no commercial motivation. In a recent lawsuit, the Utah Lighthouse Ministry (ULM), founded in 1982 to criticize the Mormon Church, sued the Foundation for Apologetic Information and Research (FAIR) for trademark infringement under the auspices of the ACPA. FAIR’s founder, Mr. Wyatt, registered several domain names incorporating the ULM mark that directed visitors to Wyatt’s website, which parodies the ULM website. Wyatt’s website contains no advertising and offers no goods or services for sale. It includes links to FAIR’s website and welcomes web surfers with the message “welcome to an official website *about* the ULM.” Because the Wyatt website did not use the ULM mark in connection with the sale of goods or services and because there is little likelihood of consumer

confusion, the court rejected ULM's claim of trademark infringement.[78]

Digital Books and E-Books

Related to the general theme of intellectual property is the issue of new publishing formats for books and the availability of those books on the internet. Several ethical and social questions have arisen as digital books and e-books (the digital version of books for sale online through distributors like Amazon) become more common. Can selected and extended excepts from books be made digitally available without violating copyrights or the “moral rights” of authors? What is the optimum way to distribute e-books to ensure adequate compensation for authors and publishers and to stimulate future innovation? Unfortunately, the future of both digital books and e-books has been clouded to some extent by copyright claims and other legal issues that have involved major internet companies like Google, Apple, and Amazon.

Let us first briefly review Google’s book project. In keeping with its mission to organize the world’s information and make it universally accessible and useful, Google launched its ambitious digital “books” project. The plan was to create a vast library of digital books. Some books would be reproduced in their entirety, while for others only a

portion of the book would be digitized. Users who located a specific book through a Google search could examine its table of contents and some of its actual content; links to online booksellers would be provided so that users could purchase the book in its print or electronic format. By 2013 Google had digitized 20 million volumes.

This project, however, was met with formidable opposition from American and European book publishers. In France, Google was sued for violating the “moral rights” of authors. When Germans followed France’s example with their own lawsuits, books from France and Germany were removed from the project. In the United States, Google had reached a settlement with authors and publishers, but that settlement was rejected by Judge Chin in 2011. However, in 2013, a new decision by Judge Chin allowed Google to continue its digitizing of books and to show small portions online of copyrighted books (unless the book was in the public domain, in which case it was available in its entirety). According to Baldwin, Google’s digitization has become “an ingrained part of online culture.”[79]

E-books have also raised some contentious problems. A particularly troublesome issue in recent years has been the pricing of e-books and the obstruction of their digital distribution. What’s

the best way to reward authors for their creative work and compensate publishers? And how can these books be priced and sold in a way that will encourage the development of creative new formats like e-books with video, audio, and web links that will benefit both authors and consumers alike?

Electronic books have been available for many years but have grown in popularity thanks to the emergence of readers such as Amazon's Kindle and Apple's iPad. It's not a surprise that Amazon, the leading online bookseller, has sought a dominating presence in the e-book marketplace. E-books are frequently offered along with print copies for the millions of titles sold on the Amazon website.

Apple decided to sell e-books in 2010 and it created the iBookstore. But Apple, which chose a different approach to pricing its books, was soon accused of price fixing and found liable for violating U.S. antitrust laws. The merits of the government's case, however, are debatable, and the central issues revolve around the different business models adopted by Apple and Amazon.

In order to understand these issues, we must discuss the basics of these two models. Amazon first entered the nascent e-book market in 2007.

The major book publishers such as HarperCollins and Random House licensed Amazon to distribute their books according to the terms of the so-called “wholesale model.” According to this model, the retailer pays a wholesale price for the book and then sets its own retail price. This is the “bricks and mortar” way of selling books, and Amazon wanted to preserve this pricing method for all of the book formats it offered on its website. Amazon would often sell these e-books below the wholesale price as a loss leader to generate other sales. For example, it might pay the publisher of the newest Harry Potter book a wholesale price of $12.50, but then sell the e-book for $9.99. Publishers worried that these discounted e-book prices would erode their hard-copy book business, but had little recourse. Amazon is a powerful distribution channel and the company often took retaliatory action against publishers who challenged their pricing. As a result of its pricing strategies, Amazon took a commanding 90% share of the e-book market.[80]

When Apple entered the e-book market to ensure a steady supply of books for its iPad, it chose a completely different model, which was much more favorable for the profit margins of book publishers and for author royalties. Apple believed that if publishers could control pricing there would be

more innovative product development in e-books, such as electronic books that included web links and other enhancements. Apple's pricing strategy allowed publishers to set their own retail prices, and Apple would take a fixed 30% commission on each sale. This is known as the "agency model," whereby Apple functions as an agent which simply resells a publisher's books. Apple worked out this deal with all of the major publishers, including HarperCollins, Macmillan, and Simon & Schuster (Random House was the only exception). Once the deal with Apple was finalized, the publishers confronted Amazon and demanded the same terms. Unless Amazon agreed to endorse the "agency model" the publishers would withhold new releases from Amazon for 7 months. By acting in concert, the publishers had gained leverage over Amazon, and the online retailer had no choice but to go along. However, since the publishers communicated among themselves and Apple coordinated those communications, there were accusations of illegal price-fixing and anti-competitive behavior.[81]

The U.S. Department of Justice (DOJ) sued Apple and the five publishers for fixing the prices of electronic books in violation of federal antitrust law (*United States v. Apple*). The DOJ cited ample proof of an illegal conspiracy among the publishers

along with Apple's coordination of that conspiracy. In accusing Apple of antitrust violations and branding its actions as "uncompetitive," the Justice Department seemed to be implicitly favoring Amazon's wholesale approach. The publishers settled with the DOJ, but Apple, convinced it had done nothing wrong, wanted its day in court. The initial ruling in federal court was in the government's favor: a U.S. District Court judge in Manhattan concluded that evidence against Apple was "overwhelming." Hence the company was liable for conspiring with major book publishers to drive up the cost of e-books. The case was appealed, but the Second Circuit federal appeals court upheld the original decision. In 2016, the U.S. Supreme Court refused to hear Apple's case, and Apple was forced to pay out $500 million, most of it to e-book consumers, to finally settle the case.[82]

Supporters of Apple have argued that Apple's actions actually increased competition by finally constraining Amazon's monopolistic power in the volatile e-book market. Many authors and formal author groups were opposed to the government's case, arguing that authors suffered substantial lost royalties thanks to Amazon's discount e-book strategy. The plight of authors, allegedly exploited by Amazon's greed, was the major reason why

some on the more liberal side of America's public opinion opposed the government's lawsuit. But were authors better served by Apple's arrangement with the trade publishing industry? It's far from evident that allowing publishers to bargain collectively with Amazon would have enhanced compensation for authors or subsidized more higher quality literature, as the defendants in this case had contended.[83]

Postscript

The astute reader will recognize something paradoxical about the trends in intellectual property protection. On the one hand, digital information is easily duplicated and transmitted in cyberspace. The internet's original architecture, predicated on content-blind packet switching, is largely responsible for this. This open architecture has posed a great threat to the movie and music industries, which remain quite anxious about their ability to protect their intellectual investments. On the other hand, new technologies and laws are conspiring to enclose information, to contain it more thoroughly than ever before. Laws like the DMCA and the Sonny Bono Copyright Term Extension Act overprotect intellectual property, to the chagrin of those who want openness and free-flowing information in the realm of cyberspace. Some smartphone patents reflect the expanding scope of patent protection in a way that threatens to stifle innovation. And digital rights architectures can control the distribution of digital information so tightly that they virtually preclude fair use.

As we have implied, these laws are misconceived and need some revision, and digital rights architectures must be sensitive to well-established

values such as fair use. At the same time, a strong case can be put forth that we still need reasonable intellectual property protection. For many reasons it would be impractical to transform cyberspace into a copyright-free zone as some have proposed. But we need laws that have a sense of measure and proportionality. In Aristotle's terminology, the goal of regulators should be to "hit the mark" and not to fail through excess (*hyperbole*) or defect (*ellipsis*), that is, to avoid overly strong or feeble protections. In a world where intellectual property has such exceptional value, the challenge to get it right could not be more important.

DISCUSSION QUESTIONS

1. What is your assessment of the Digital Millennium Copyright Act (DMCA)?
2. What is the significance of the open code movement? Comment on the pros and cons of open source software.
3. Explain how trademark ownership can conflict with free speech rights. How should these competing claims be resolved?
4. Comment on this observation from Esther Dyson's essay entitled "Intellectual Property on the Net": "The issue isn't that intellectual property laws should (or will) disappear; rather, they will simply become less important in the scheme of things."[84]

Case Studies

Readers' Rights, Remixing, and Mashups

A number of prominent legal scholars have recently expressed support for a copyright system in the United States that gives rights not just to authors and creators of content but also to those who read, view, and listen to that content. These limited user rights would go well beyond fair use and typically encompass broad access and distribution rights, including the right to share digital content with others. The idea of a "law of user's rights" is not new, although there has always been a measure of resistance. Yet this idea has gained considerable traction among intellectual property scholars, especially within the last decade. They see copyright as far too heavily tilted toward enriching owners of content; hence the law must be reconfigured to offer more concrete benefits and opportunities to the consumers of content. Jessica Litman, for example, ardently insists that we must take readers' interests more seriously and "reclaim

copyright for readers."[85] What specific rights should readers have? While some argue for a modest set of user rights, others propose a thick set of rights including the right to share works with others along with the right to recode or transform a work to give it a different meaning, even if the new product is highly derivative of the original work.

Among the readers' rights proposed is the prerogative to engage in remixing or creating mashups without getting permission from the original copyright holders. Specifically, users would be allowed to remix digital content by recombining pieces from different preexisting cultural works, such as music, photos, books, and movies, even if those objects have a copyright. Under this system, filmmakers would be allowed to construct new movies out of substantial clips compiled from digital movies located on computer systems around the world. Such a creative mashup, of course, is currently illegal, unless it falls within the restrictive parameters of fair use. But Larry Lessig and others maintain that the law must be changed, so that ordinary people become "producers" of culture, not just "consumers" of culture. In this way we can return to an "amateur"

creative culture that supports the participation of the multitude instead of just an elite few.[86]

Where might the public stand on this issue? Litman claims that we are on “the verge of reaching a social consensus that mashing up is an important copyright liberty,” that even copyright owners should not want to prevent.[87] She goes on to stipulate that the law should allow for the creation and sharing of mashups as long as this is done noncommercially.

Without a change in the law and some recognition of users’ remixing rights, creative remixers like DJ Danger Mouse will continue to be thwarted by the structure of the current copyright system. This particular remixer is known for the Grey Album, a coalescing of the Beatle’s White Album and Jay-Z’s The Black Album. Copyright owners, however, fought vigorously to prevent online distribution of the Grey Album. Many cite this as an example of an oppressive copyright system interfering with the potential of a robust, creative remix culture. Some mashup artists, like the creator of “Girl Talk,” Gregg Gillis (he recombines music snippets from

Bruce Springsteen, Jay-Z, and Miley Cyrus), take small samples that appear to be covered by fair use provisions of the copyright law. However, it's not completely clear that Girl Talk is on the right side of the law, and a case can certainly be made that Gillis's work is inhibited by the long shadows of copyright law. Changes in that law rebalancing the equation between the rights of creators and consumers will promote greater cultural participation and thereby serve a definite social purpose.

Some legal scholars, such as Robert Merges, do not believe that the impetus to promote this remix culture should lead to structural changes in copyright law. They argue that it would be unfair to the original creators of mass market content for remixers to "redistribute" their works and thereby interfere with their ability to appropriate the value of their creations. We cannot neglect the efforts of musicians, songwriters, novelists, and filmmakers who make this content. They have a right to control distribution, and, within limits, a right to control the fundamental meaning of those works. According to Merges, "The story of the original content creator should affect how

we think about remixing."[88] The solution is to structure the law so that both content creators and users are treated fairly and justly, but this does not mean diluting the rights original content creators deserve over their creative works.

Questions

1. Should copyright laws be altered to facilitate remixing and mashups (e.g., by broadening the terms of fair use, which currently permit the use of very small samples of music or movies)?
2. Should remixers be allowed to profit from their efforts?

Case Studies

A Parody of PETA

People for the Ethical Treatment of Animals (PETA) is a nonprofit organization dedicated to the promotion of animal rights. The group is opposed to eating meat, wearing fur and leather, and conducting research experiments on animals. In this case, the domain name **www.peta.org** was registered by Mr. Doughney to parody PETA and its views on animals. The webpage was entitled "People Eating Tasty Animals," and it included links to sites where leather goods or meat products were sold. The plaintiff filed suit under the auspices of the Anticyber squatting Protection Act (ACPA), alleging that the **peta.org** domain name was identical to or confusingly similar to the distinctive and famous PETA mark. Doughney and his lawyers contended that there was no infringement or dilution, and hence no violation of the ACPA, because his website was a parody.

A federal district court ruled in favor of PETA, finding Doughney liable for trademark infringement. The case was promptly appealed, but the U.S. Court of Appeals for

the Fourth Circuit affirmed the judgment of the district court. It agreed that the PETA mark was distinctive and that Doughney had no intellectual property right in **peta.org**. Moreover, according to the court, there was no record of any prior use of **peta.org**, and Doughney used the mark in a commercial manner. It also agreed that Doughney "clearly intended to confuse, mislead and divert internet users into accessing his website which contained information antithetical and therefore harmful to the goodwill represented by the PETA Mark."[89] Doughney himself "admitted that it was 'possible' that some Internet users would be confused when they activated '**peta.org**' and found the 'People Eating Tasty Animals' website."[90] The appeals court concluded that Doughney acted in bad faith; he made statements to the press that PETA should attempt to settle with him and "make him an offer."

A key issue triggered by this case is whether a good faith intention to criticize and parody a trademark owner such as PETA should constitute a valid reason for registering a domain name incorporating that trademark owner's trademark (**peta.org**). Or does that

domain name require some sort of appendage or distinguishing variation such as “**petasucks.com**” so that there will be no confusion?

Questions

1. Do you agree with the court’s decision in this case? If so, what about Mr. Doughney’s free speech rights?
2. In your view, why did the court reject Doughney’s parody defense?

Case Studies

Oracle vs. Google: The Fight over Java

The high-profile dispute between Oracle and Google has been described as the “most notable case in copyright,” and the “World Series of IP cases.”[91] The protracted conflict traces back to Oracle’s acquisition of Sun Microsystems after the demise of Sun’s hardware business. Oracle, founded in 1977, rose to prominence in Silicon Valley thanks to its flagship database business. Unlike Sun, Oracle has followed the path of Apple by favoring proprietary technologies over open source ones.

Sun had developed the programming language or platform called Java, hoping that it would become the standard language employed by programmers for website development and applications. In 1995, Sun introduced the Java platform, which allows a user to run the same Java application on many different kinds of computers. Java applications can be delivered over the internet to computers running different operating systems (for example, Windows, Macintosh, or Unix). Since its introduction in

1995 Java grew in popularity thanks to this portability or cross-platform functionality. Almost immediately, Netscape adopted Java for its Navigator browser.

The Java technology has several components that contribute to its superior functionality. It encompasses a programming language; a group of programs written in that language called the “Java class libraries” that expose their own Application Programming Interfaces (APIs); a compiler that translates the code written by a programmer into “bytecode”; and, finally, the Virtual Java Machine (JVM) that translates bytecode into instructions for the operating system. Applications that use the Java APIs will run on any systems with a Java Runtime Environment (JRE), that is, the Java class libraries and a JVM.

While the Java programming language is essentially free to use under the open source terms of a general public license, the Java platform or Java SE requires a license. Java SE allows the code written in the Java programming language to run on a variety of different operating systems using the Java Virtual Machine (JVM). Java SE also

includes the Java APIs. The APIs, which consist of standardized, prewritten "methods" or blocks of code to handle basic programming functions, work as software interfaces. They allow programs, websites, or apps to communicate with one another. For example, the APIs allow an operating system like Android to download a website or open and run a particular app. Java developers would be unable to create new programs for platforms like Android without relying on these software interfaces.[92]

The pivotal question in this case is whether these APIs or software interfaces are copyrightable. According to the U.S. copyright law, copyright protection does not extend to "any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such [original] work."[93] Do these restrictions apply to software interface or APIs which serve as the means of interoperability for information technologies, and have been often characterized as "methods of operation," because of their functional purpose? The Supreme Court sought to resolve a closely

related question in the *Lotus v. Borland* case but deadlocked in a 4–4 vote. At issue was copyright protection for the menu command hierarchy (e.g., a sequence of commands such as Paste–Cut– Copy). In the absence of a definitive Supreme Court Ruling the First and Sixth federal circuit courts ruled that copyright law excludes protection for all methods of operation, including those embedded into software interfaces. The first person to write a program cannot "lock up" basic or standard programming techniques and methods of operation such as a command hierarchy. The Third Circuit has taken the opposite position, ruling that a method of operation embodied in a software interface is copyrightable so long as it could have been written differently.[94]

Java and Google's Android Operating System

Google, the search engine giant, developed an open-source platform or operating system for mobile devices. The product was called Android, and it was released to the public in 2007. Many companies such as Samsung, Xiaomi, Nokia, and HTC use the Android operating system for their smartphones. Apple, on the other hand, uses its own

proprietary operating system (OS) known as the iMac. Although Google executives did not intend to directly monetize Android, it was designed to become a vehicle for promoting its search functionality and other applications. The company's goal was to produce and distribute "the world's first open source handset solution with built-in Google applications."[95]

Java was vital to the success of this open source project for a number of reasons. The company had to move fast because competitors were working on their own proprietary systems. Therefore it was not feasible to write all the code from scratch. Also, there was already an "existing pool" of developers and applications. Java therefore, meant "a safe sandbox for third party developers."[96]

There were extensive negotiations with Sun about the use of Java for Android, but Google found the company's licensing terms to be too restrictive. Negotiations broke down, but Google's commitment to Java was undeterred. Using the Java language was not a problem since it was an open source product that Sun had released to the public.

Google also planned to develop and code its own virtual machine (called “Davlik”). But copyright issues arose because the Android team wanted to use 37 Java API packages from the Java Standard Edition (SE). Each of the API packages uses two types of source code: declaration code and implementation code. The Android developers used the declaration code of the APIs, analogous to chapter headings and titles, but wrote their own implementation code. These declarations represent the “header line of code” that introduces the “methods” or blocks of code that perform functions such as mathematical calculations or the display of simple graphics. The Java API declarations inform developers how to access these prewritten methods that perform the tasks which are executed by the implementation code. One of the API packages implemented in Android was java.security, which provides the classes and interfaces for the product’s security framework and allows an app’s security commands to function.[97]

Despite its disapproval, Sun did not challenge Google and it did not file a copyright or patent infringement law suit. But

Oracle's acquisition of Sun in 2010 changed everything. Oracle CEO Larry Ellison regarded Java as "the single most important software asset we have ever acquired."[98] Moreover, Oracle was prepared to take legal action over Google's use of these 37 API libraries of coding blocks without a license, since it perceived this action as a blatant infringement of its copyright. The company sued Google for copyright infringement and sought $9 billion in damages. In its lawsuit, Oracle claimed that Google had illegally copied Java source code along with the structure and organization of Java class libraries to develop its Android OS.[99]

Legal History and Arguments

Specifically, Oracle alleged that Google directly copied 7,000 lines of declaring code and generally replicated without permission the structure, sequence, and organization of 37 Java API packages. Oracle conceded that the implementation code was different and the Davlik virtual machine was not an issue. The central question before the court would be whether these components of the Java platform were entitled to copyright protection. And if they were subject to such

protection did Google's use of this material constitute a form of fair use under current copyright law.[100] According to Oracle, while no single name was copyrightable, "Java's overall system of organized names – covering 37 packages, with over 600 classes, with over 6,000 methods – is a 'taxonomy' and, therefore, copyrightable."[101] In its defense Google insisted that Sun had freely licensed the Java programming language and encouraged the use of Java APIs by developers. Google also argued that it independently implemented the functions of the 37 API packages at issue and that its use of 7,000 lines of declaring code was a small part of Android's 15 million lines of source code. For example, a declaration might call for something to be displayed and the associated implementation code would display the output on the screen of a smartphone or other mobile device. The reuse of these Java software interface declarations in Android was necessary so that developers could program Android applications in the open Java language.[102]

The first trial took place in 2012 in the U.S. District Court for the Northern District of California. The jury was deadlocked on the

fair use issue. But Judge Alsop generally rejected Oracle's arguments. He ruled that Google's use of the Java APIs constituted fair use because an API is a "method of operation." He also ruled that the 37 API packages were not subject to copyright protection. The declaring code was not protectable since "names and short phrases cannot be copyrighted." As a result, the Court entered its final judgment in favor of Google.[103]

In 2013, Oracle appealed Judge Alsop's ruling to the U.S. Court of Appeals for the Federal Circuit. The case was now attracting widespread attention with major software companies siding with Oracle, but independent application developers siding with Google. Libertarian groups such as the Electronic Frontier Foundation (EFF) were also aligned with Google. In its legal brief laying out the rationale for its appeal, Oracle's attorneys employed a literary analogy to help convince the jurists of the validity of their claims:

> Ann Droid wants to publish a best seller. So she sits down with an advance copy of *Harry Potter and the Order of Phoenix* – the fifth book – and proceeds to transcribe. She verbatim copies the chapter titles – from **Chapter 1** (Dudley Demented) to Chapter 38 (The Second War Begins). She copies verbatim the topic sentences of each paragraph starting from the first (highly descriptive) one and continuing, in order, to the last, simple one ("Harry nodded"). She then paraphrases the rest of each paragraph. She rushes the competing version to press before the original under the title: Ann Droid's *Harry Potter 5.0*. The knockoff flies off the shelves.
>
> J.K. Rowling sues for copyright infringement. Ann's defenses: "But I wrote most of the words from scratch. Besides, this was fair use, because I copied only portions necessary to tap into the Harry Potter fan base."
>
> Obviously, the defenses would fail.

Thus, Oracle's approach was based on a comparison of the creativity in the design and coding of computer software with the copyrightable creativity of a literary work.[104]

But in their rebuttal Google's attorneys resorted to familiar arguments about the nature of software. They argued that software interfaces are not like literary or artistic works because they "perform

functions that are not entitled to copyright protection."[105]

In May 2014, the Federal Appeals Court hearing the case reversed the District Court's 2012 decision. It ruled that the structure, organization, and sequence of the APIs was copyrightable and remanded the case back to the district court for a retrial on the basis of whether Google's use of the material constituted fair use. According to the Court, "because Oracle exercised creativity in the selection and arrangement of the method declarations when it created the API packages and wrote the relevant declaring code, they contain protectable expression that is entitled to copyright protection."[106] In 2016, Judge Alsop conducted the retrial that dwelt on the issue of fair use of the copyrightable declaring code by Google. In closing arguments at the trial Google attorneys emphasized Android's "transformative purpose," reminding the Court that Android was not a substitute or direct copy of Java SE but an innovative software platform. Oracle's attorneys, on the other hand, relied on a simple moral theme: "You don't take other people's property without permission and use it for your own

benefit," and you don't take "shortcuts" at other people's expense and come up with the "fair use excuse."[107] The jury seemed unpersuaded by that moral argument. It found that this was a case of fair use and exonerated Google.

However, in March 2018, the Federal Circuit Court of Appeals overturned the verdict and ruled that Google's use of the APIs wasn't "fair." According to the Court of Appeals, "There is nothing fair about taking a copyrighted work verbatim and using it for the same purpose and function as the original in a competing platform."[108] But, despite this ruling, the extended battle between Google and Oracle has continued. In 2019, Google filed a petition with the U.S. Supreme Court asking its members to review the Circuit Court's decision.

Questions

1. Outline as clearly as possible the main facts of this case and explain the moral issues at stake.
2. Assume that you are an attorney representing Google (or Oracle). Prepare a two-page brief defending the position of your client.

3. If you were a Supreme Court Justice and the Court decided to hear this case, would you vote in favor of Oracle or Google? Explain your reasoning in one succinct paragraph.

REFERENCES

1. Julie Cohen, *Configuring the Networked Self* (New Haven, CT: Yale University Press, 2012), 223.
2. Larry Lessig, *Free Culture* (New York: Penguin Press, 2004), 12–13.
3. See Robert Merges, *Justifying Intellectual Property* (Cambridge, MA: Harvard University Press, 2011), 24–27.
4. Anthony M. Honore, "Ownership," in *Oxford Essays in Jurisprudence*, ed. Anthony Gordon Guest (Oxford: Oxford University Press, 1961), 108.
5. U.S. Constitution, Article I, § 8, clause 8.
6. 17 U.S.C. § 106.
7. Paul Goldstein, *Copyright's Highway* (New York: Hill & Wang, 1994), 20.
8. *Campbell v. Acuff-Rose*, 510 U.S. 569, 1994.
9. *Sony v. Universal*, 464 U.S. 417, 1984.
10. William Fisher, "Business Method Patents Online," accessed March 2000, **http://eon.law.harvard.edu/property00/patents**.
11. Henri Hanneman, *The Patentability of Computer Software* (Deventer, The

Netherlands: Kluwer Academic Publishers, 1985), 87.

12. Background material in this section was found in Joe Liu, “Overview of Trademark Law,” Berkman Center for Law and Technology, Harvard University.

13. John Locke, “Second Treatise of Government,” in *Locke: Two Treatises of Government*, ed. Peter Laslett (Cambridge: Cambridge University Press, 1988), § 27. See also David McGowan, “Copyright Non-Consequentialism,” 69 *Missouri Law Review* 1 (2004): 38–39.

14. Merges, *Justifying Intellectual Property*, 15, 35–36, 47. I am indebted to Merges’ analysis of Locke throughout this discussion.

15. Locke, “Second Treatise of Government,” § 27.

16. Jeremy Waldron, *The Right to Private Property* (Oxford: Oxford University Press, 1988), 215.

17. Adam Moore, “Intangible Property: Privacy, Power, and Information Control,” in *Information Ethics*, ed. Adam Moore (Seattle: University of Washington Press, 2005), 176–80.

18. *Mazer v. Stein,* 347 U.S. 201, 1954.

19. Georg Wilhelm Friedrich Hegel, *Philosophy of Right*, trans. T. Knox (New York: Oxford University Press, 1967), 40.

20. Justin Hughes, "The Philosophy of Intellectual Property," in *Intellectual Property*, ed. Adam Moore (Lanham, MD: Rowman & Littlefield, 1997), 107–77.

21. Ibid.

22. William Fisher, "Property and Contract on the Internet," *Chicago-Kent Law Review* 73, no. 4 (1998): 1203–56. See also Merges, *Justifying Intellectual Property*, 2–4.

23. *Washington Publishing Co. v. Pearson*, 306 U.S. 30, 1954.

24. Jane Ginsburg, "Copyright Legislation for the 'Digital Millennium,'" *Columbia-VLA Journal of Law and the Arts* 23 (1999): 137.

25. See Richard A. Spinello, "The DMCA, Copyright Law, and the Right to Link," *Journal of Information Ethics* 13, no. 2 (2004): 8–23.

26. Pamela Samuelson, "Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised," *Berkeley Technology Law Journal* 14 (1999): 519.

27. Thomas Stearns Eliot, “Tradition and the Individual Talent,” in *Selected Essays* (New York: Harcourt Brace, 1950), 4.

28. *United Christian Scientists v. Christian Science Board of Directors*, 829 F.2d 1152 (D.C. Cir. [1987]).

29. William Fisher, “Digital Music: Problems and Possibilities,” 2000, **http://www.law.harvard.edu/faculty/tfisher/Music.html**.

30. Plaintiff’s Brief, *A&M Records v. Napster*, *Inc.* 2000 WL 573136 (N.D. Cal. [2000]).

31. *Gershwin Publishing v. Columbia Artists Mgmt* 443 F 2d 1159, (2d Cir, [1971]).

32. United States Court of Appeals for the Ninth Circuit, *A&M Records et al. v. Napster*, 239 F.3d 1004 [2001].

33. *Harper & Row Publishers, Inc. v. Nation Enters*., 471 U.S., 539, 85 L. Ed. 2d 588 [1985].

34. Stephanie Greene, “Reconciling Napster with the Sony Decision and Recent Amendments to Copyright Law,” *American Business Law Journal* 39 (2001): 57.

35. *A&M Records, Inc. v. Napster*, 239 F. 3d 1004 (9th Cir. [2001]).

36. Ibid.

37. *Arista Records v. Lime Group* 715 F. Supp 2d 481 (2010).
38. Erich Schwartzel, "U.S. Lays Out Case against Megaupload," *The Wall Street Journal*, December 21, 2013, B1, B4.
39. Christine Korsgaard, *Creating the Kingdom of Ends* (Cambridge: Cambridge University Press, 1996), 98.
40. For a more thorough treatment of this case see "Note on the DeCSS Trial," in *Readings in Cyberethics*, 2nd ed., eds. Richard Spinello and Herman Tavani (Sudbury, MA: Jones and Bartlett Publishers, 2004), 264–68.
41. *Universal City Studios v. Remeirdes et al*., 111 F. Supp.2d 294 (S.D.N.Y. [2000]).
42. Amy Harmon, "Free Speech Rights for Computer Code," *The New York Times*, July 31, 2000, C1.
43. *Lexmark International, Inc. v. Static Control Components, Inc.* 387 F. 3d 522 (6th cir. 2004).
44. *Alice Corporation Ltd v. CLS Bank* 573 v. 416 (2014). See also by Ashby Jones, "Hard Questions on Software," *The Wall Street Journal*, March 31, 2014, B4.

45. Richard Stallman, “GNU Manifesto,” 2015, http://www.gnu.org/gnu/manifesto.en.html .

46. European Commission, “Study into the Use of Open Source Software in the Public Sector,” (2001, Part 3, Interchange of Data between Administrations, at 16).

47. Rupert M. Scheule, Rafael Capurro, and Thomas Hausmanninger, eds., *Vernetz Gespalten: Der Digital Divide in Ethischer Perspektive* (München: Wilhelm Fink Verlag, 2004).

48. Eric Raymond, *The Cathedral and the Bazaar* (Sebastopol, CA: O’Reilly Media, 2001), reprinted with permission.

49. Eric Raymond, “Homesteading the Noosphere,” 2000, http://www.catb.org/esr/writings/homesteading/homesteading.

50. Yochai Benkler, “Coase’s Penguin or Linux and the Nature of the Firm,” *Yale Law Journal* 112 (2002): 369.

51. Mark Stefik, “Trusted Systems,” *Scientific American*, March 1997, 46.

52. Raymond Ku, “The Creative Destruction of Copyright,” *University of Chicago Law Review* (2002): 69.

53. Cory Doctorow, *Information Doesn't Want to Be Free* (San Francisco, CA: McSweeney, 2014), 126–27.

54. *State Street Bank and Trust Co. v. Signature Financial Group, Inc.,* 149 F. 3d 1368 [1998].

55. Ibid.

56. Ibid.

57. Christopher Lewis, "What Is a Cyberpatent's Value to Emerging e-Business," December 1999.

58. Complaint, ***Priceline.com**, Inc. v. Microsoft Corporation and Expedia, Inc.* (U.S. Dist Ct. CN [1999]).

59. Jess Barvin, Mylene Mangalindan, and Don Clark, "eBay Ruling Changes Dynamic in Patent Infringement Cases," *The Wall Street Journal*, May 16, 2006, B1. See also *eBay v. MercExchange,* L.L.C. (2006) 547 U.S. 388.

60. Brent Kendall, "Door Open on Method Patents," *The Wall Street Journal*, June 29, 2010. A5. See also *Bilski v. Kappus* 130 U.S. 1238 (2010).

61. Paul Elias, "Apple, Samsung Lawsuit Heads to Court for Showdown," *Associated Press*, July 30, 2012.

62. Apple Opening Brief, *Apple, Inc. v. Samsung Electronics Co*. 01846 N.Dist. CA (2012).

63. Samsung Opening Brief, *Apple, Inc. v. Samsung Electronics Co*. 01846 N.Dist. CA (2012).

64. Jessica Vascellano, "Samsung Case Is a Proxy for Google," *The Wall Street Journal*, July 30, 2012, B1, B5.

65. Ibid.

66. See Phillip DeWitt-Elmer, "*Apple v. Samsung*: The Patent Trial of the Century," *Tech Fortune*, **CNN.com**, July 30, 2012.

67. Ibid.

68. *Apple, Inc. v. Samsung Electronics* 580 U.S. 137 (2016). See also Brent Kendall, "Supreme Court Hears Samsung, Apple Patent Suit," *Wall Street Journal*, October 12, 2016, B3.

69. *Sporty's Farm L.L.C. v. Sportman's Mkt., Inc.* 202 F.3d 489 (2d Cir. [2000]).

70. *Panavision International v. Toeppen* 141 F.3d 1316 (9th Cir. [1998]).

71. See Kat Henderson and Richard Spinello, "Cybersquatting: Rights and Conflicts," The American Philosophical Association, *Newsletter of Law and Philosophy* (Spring 2005): 16–22.

72. Ibid.

73. Courtney Macavinta, “Scientologists in Trademark Disputes,” CNET **News.com**, January 29, 1998.

74. “Uniform Domain Name Dispute Resolution Policy [UDRP],” 1999, **http://www.icann.org**.

75. Julia Angwin, “Are Domain Panels the Hanging Judges of Cyberspace Court,” *The Wall Street Journal*, August 20, 2001, B1.

76. Anticybersquatting Consumer Protection Act (1999). 15 U.S.C. § 1125.

77. Ryan Owens. “Domain Name Resolution after *Sallen v. Corinthians Licenciamentos* & ***Barcelona.com**, Inc. v. Excelentisimo Ayuntameiento de Barcelona*,” *Berkeley Technology Law Journal* 18 (2003): 257.

78. *Utah Lighthouse Ministry v. FAIR* 527 F.3d 1045 (U.S. Dist. 2008).

79. Peter Baldwin, *The Copyright Wars* (Princeton, NJ: Princeton University Press, 2014), 368. See Baldwin’s full account of Google’s project: 359–69.

80. George Priest, “Apple Should Win Its E-Book Appeal,” *The Wall Street Journal*, December 15, 2014, A13.

81. Chris Sagers, *United States v. Apple: Competition in America* (Cambridge, MA:

Harvard University Press, 2019), 188-200. See also L. Gordon Crovitz, “The Antitrust Book Boomerang,” *The Wall Street Journal*, June 2, 2014, A13.

82. Joe Palazzolo, “Apple Loses Its Court Appeal on E-Books,” *Wall Street Journal*, July 1, 2015, B3. See also Joe Palazzolo, “Apple Heads to Court over E-Books,” *The Wall Street Journal*, December 15, 2014, B1, B7 and Sagers, *United States v. Apple,* 1-4, 200-201.

83. Sagers, *United States v. Apple,* 4-5, 251-2, 263. See also Crovitz, “The Antitrust Book Boomerang,” A13.

84. Esther Dyson, “Intellectual Property on the Net,” in *Release 1.0* (New York: Random House, 1994).

85. Jessica Litman, “Readers’ Copyright,” 208 *Journal of the Copyright Society of the USA* 325 (2011).

86. Larry Lessig, *Remix: Making Art and Commerce Thrive in the Hybrid Economy* (New York: Penguin, 2008).

87. Litman, “Readers’ Copyright,” 352.

88. Robert Merges, “Copyright, Creativity, and Catalogs,” 40 *U.C. Davis Law Review* 1259 (2007).

89. *People for the Ethical Treatment of Animals v. Michael T. Doughney* 113 F. Supp. 2d (E.D. Va [2000]).

90. Ibid.

91. Jeffrey Neuberger, "Federal Circuit Again Reverses California Court in Oracle-Google Copyright Dispute," Proskauer New Media and Technology Law Blog, March 30, 2018; **https://newmedialaw.proskauer.com/2018/03/30/federal-circuit-again-reverses-california-court-in-oracle-google-copyright-dispute**.

92. Aaron Ward, "Google v. Oracle: Silicon Valley Braces for 'Lawsuit of the Decades,'" *JPLT*, Harvard Law School, March 13, 2019.

93. Copyright Act of 1976, 17 U.S.C. § 102 (b).

94. *Lotus Development Corp. v. Borland International Inc.* 49 F. 3d 807 (1st Cir. 1995). "The Lotus menu command hierarchy is an un-copyrightable 'method of operation' [that]. . . provides the means by which users control and operate Lotus 1-2-3" (at 813). See also *Apple Computer v. Franklin Computer Corp* 714 F. 2d 1240 (3rd Cir. 1983) and Petition for Writ of Certeriorari, *Google LLC, Petitioner v. Oracle America*, January 2019, 12–13.

95. Google Product Strategy, Trial Exh. 1, *Oracle America, Inc. v. Google Inc*., 872 F. Supp 2d 974 (N.D. Cal 2012), 4.

96. Ibid., 8.

97. Ward, "Google v. Oracle."

98. Patrick Thibodeau, "Oracle Buying Sun in $7.4 Billion Deal," *Computerworld*, April 20, 2009, 1, 14. See also Jay Greene and Brent Kendall, "Oracle Defeats Google in Court," *Wall Street Journal*, March 28, 2018, B1–2.

99. *Oracle America Inc. vs. Google Inc.* 730 F.3d 1339 (2014).

100. *Oracle America, Inc. v. Google Inc*. (2012), 998.

101. Peter Mennel, "Rise of the API Copyright Dead? An Updated Epitaph for Copyright Protection of Network and Functional Features of Computer Software," 31 *Harvard Journal of Law and Technology* 305 (Spring 2018).

102. *Oracle America, Inc. v. Google Inc*. (2012). See also Petititon for Writ of Certeriorari, 27.

103. *Oracle America, Inc. v. Google Inc*. (2012), 983.

104. Opening Brief and Addendum of Plaintiff-Appellant, *Oracle America Inc. v. Google Inc*. No. 2013-1021, (Fed Cir. 2013), 1022. See

also Mennel, “Rise of the API Copyright Dead?,” 384–85.

105. *Sony Computer Entertainment v. Connectix Corp* 203 F. 2d (9th Cir.), cert. denied, 531 U.S. 871 (2000), 602. See also Mennel, “Rise of the API Copyright Dead?,” 386.

106. *Oracle America Inc. vs. Google Inc.* (2014), 1387. See also Mennel, “Rise of the API Copyright Dead?,” 406.

107. Greene and Kendall, “Oracle Defeats Google in Court,” B1.

108. Ibid.

ADDITIONAL RESOURCES

Alderman, John. *Sonic Boom: Napster, MP3 and the New Pioneers of Music*. Cambridge, MA: Perseus Books, 2001.

Baldwin, Peter. *The Copyright Wars*. Princeton, NJ: Princeton University Press, 2014.

Bettig, Ronald. *Copyrighting Culture*. Boulder, CO: Westview Press, 1996.

Boyle, James. *The Public Domain*. New Haven, CT: Yale University Press, 2009.

Doctorow, Cory. *Information Doesn't Want to Be Free*. San Francisco, CA: McSweeney, 2014.

Drahos, Peter. *A Philosophy of Intellectual Property*. Aldershot, UK: Dartmouth Pub., 1996.

Feller, Joseph, ed. *Perspectives on Free and Open Software*. Cambridge, MA: MIT Press, 2005.

Gantz, John, and Jack B. Rochester. *Pirates of the Digital Millennium: How the Intellectual Property Wars Damage Our Personal Freedoms, Our Jobs, and the World Economy*. Upper Saddle River, NJ: Financial Times Prentice-Hall, 2005.

Goldstein, Paul. *Copyright's Highway*. New York: Hill & Wang, 1994.

Helprin, Mark. *Digital Barbarism*. New York: Harper, 2009.

Henderson, Kat, and Richard Spinello. "Cybersquatting: Rights and Conflicts." The American Philosophical Association, *Newsletter of Law and Philosophy* (Spring 2005): 16–22.

Lessig, Larry. *Free Culture*. New York: Penguin Press, 2004.

Lessig, Larry. *Remix: Making Art and Commerce Thrive in the Hybrid Economy*. New York: Penguin Press, 2008.

Littman, Jessica. *Digital Copyright*. New York: Prometheus Books, 2001.

Merges, Robert. *Justifying Intellectual Property*. Cambridge, MA: Harvard University Press, 2011.

Moore, Adam, ed. *Intellectual Property: Moral, Legal and Intellectual Dilemmas*. Lanham, MD: Rowman & Littlefield, 1997.

Netanel, Neil. *Copyright's Paradox*. New York: Oxford University Press, 2008.

Raymond, Eric. "The Cathedral and the Bazaar." 1998, **http://www.unterstein.net/su/docs/CathBaz.pdf**.

Sagers, Chris. *United States v. Apple: Competition in America*. Cambridge, MA: Harvard University Press, 2019,

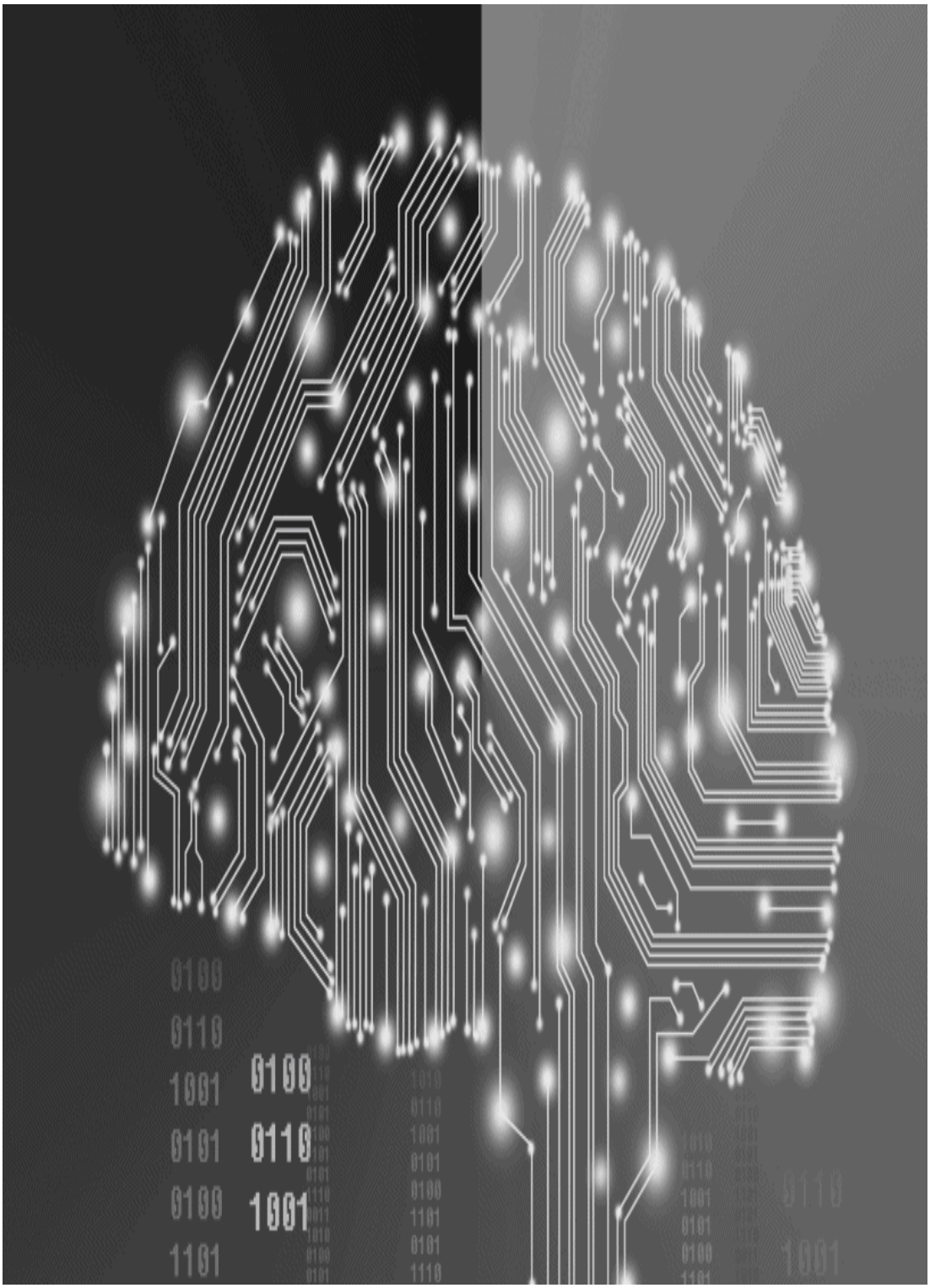
Spinello, Richard. “The DMCA, Copyright Law, and the Right to Link.” *Journal of Information Ethics* 13, no. 2 (2004): 8–23.

Spinello, Richard, and Maria Bottis. *A Defense of Intellectual Property Rights*. Northampton, MA: Elgar, 2009.

Spinello, Richard, and Herman Tavani. *Intellectual Property Rights in a Networked World: Theory and Practice*. New Brunswick, NJ: Idea Group Publishing, 2005.

Stallman, Richard. “GNU Manifesto.” 1985, **http://www.gnu.org/gnu/manifesto.html**.

Weber, Steven. *The Success of Open Source*. Cambridge, MA: Harvard University Press, 2004.



CHAPTER 5

Privacy Rights in the Age of Surveillance

The digital infrastructure has created a more open and porous society, where privacy seems to grow scarcer with each innovation. Automated information flows allow companies to acquire vast amounts of predictive, behavioral data about their customers. Some of these extraction and monitoring technologies are quite simple. Beacons and digital cookies of different stripes enable an unprecedented level of surreptitious internet surveillance. Merchants are eager to collect data about our web activities and buying habits in order to deliver targeted ads that persuade us to purchase their goods.

The public seems to be ambivalent and even nonchalant about privacy issues until their collective consciousness is jarred by some startling new revelation. On occasion, some organization discovers that it has transgressed a certain threshold, and it is forced to withdraw a plan that simply goes too far. For example, Google was forced to apologize when it deployed special software code that tricked Apple's Safari browser into letting Google monitor the online activities of iPhone users. In similar fashion, Facebook altered its policy after a 2019 *Wall Street Journal* report revealed that popular health and fitness apps were sharing personal information with Facebook that included a person's weight or menstrual cycles.

In addition, as a result of sophisticated surveillance and monitoring technologies, the networked workplace has become a virtual panopticon, where workers' movements and interactions are more visible than ever before to their managers. GPS technologies can be especially intrusive. Hence, the employee's right to privacy now appears to be in greater peril than ever.

The preservation of privacy on social network or search engine platforms has been particularly tenuous. According to Shoshana Zuboff, digital reality has mutated into "surveillance capitalism," where digital connectivity is primarily a means for commercial ends. Google was one of the pioneers in leading this transformation. Google has always depended on advertising to monetize its search engine capabilities. Every time a user does a Google search the system is designed to present targeted ads. Those ads were derived not only from keywords and the user's search terms but also from "user profile information," comprised of data items collected and compiled by Google. Relying on these data, which include previous searches, websites visited, psychographics, and browsing activities, enhances the efficiency and precision for advertisers. Zuboff explains that Google's sophisticated automated architecture "operates as a one-way mirror irrespective of a person's awareness, knowledge, and consent."[1]

What are the ramifications of living in this world dedicated to the extraction and exploitation of our personal information? What are reasonable expectations for some sort of privacy protection as users conduct a Google search or shop at websites with voracious appetites for their data? Are children at an even greater risk for invasions of privacy because of their addiction to Facebook and YouTube? What

is the appropriate scope of privacy protection in the workplace? Finally, do privacy rights include a “right to be forgotten”?

These are the main questions to be reviewed in this chapter. But first we must explain why the right to privacy is of such fundamental importance from a legal as well as moral perspective. This will help us to appreciate why its incremental but persistent erosion represents a subtle assault on human dignity.

A Definition and Theory of Privacy

Privacy is not a simple concept that can be easily defined. In addition, theories of privacy often confuse the *concept* of privacy with the normative justification for a *right* to privacy. Perhaps the most basic and suggestive definition is implied in a seminal *Harvard Law Review* article written by Samuel Warren and Louis Brandeis in 1890. These authors differentiated the right to privacy from other legal rights and conceived privacy in terms of "being let alone."[2]

The broad definition embedded in Warren and Brandeis's discussion on privacy rights is a good starting point because it underscores that non-intrusion is an important condition of privacy. This concept of privacy is obviously inadequate, however, because "being let alone" is rather vague and imprecise. We might come across a group of stranded fishermen on a deserted island and decide to leave them alone, but we can hardly describe their situation in terms of "privacy."

Ruth Gavison has advocated a version of the so-called seclusion theory, which defines privacy as the limitation of others' access to an individual with three key elements: secrecy, anonymity, and solitude. Anonymity refers to the protection from

undesired attention; solitude is the lack of physical proximity to others; and secrecy (or confidentiality) involves limiting the dissemination of knowledge about oneself. Gavison's theory suggests that privacy is best understood as a condition of restricted access. Privacy is lost when someone observes a person or otherwise intrudes upon her in a private space where there is an expectation of being left alone.[3]

Both the Gavison and Warren/Brandeis theories of privacy deal primarily with the issue of physical privacy or "autonomy privacy," the ability to conduct one's activities without the observation or intrusion of others. Thanks to the rise of cybertechnology, however, more recent privacy theories have focused greater attention on information privacy, which concerns the protection of personal information. When one surveys the vast terrain of literature on information privacy, two generic privacy theories stand out: the control theory and the restricted access theory. Gavison's approach is often cited as an example of the latter, in which privacy amounts to restricting access to information about oneself in certain contexts. By comparison, the control theory, which is advocated by philosophers like Charles Fried, suggests that privacy is contingent on possessing control over information about oneself.[4] Even the U.S.

Supreme Court has opined that personal privacy can be defined as a condition of “control over information concerning his or her person.”[5]

Philosophers Jim Moor and Herman Tavani have synthesized these two theories and accurately describe information privacy in terms of “restricted access/limited control.”[6] They recognize that our information must sometimes be shared with others; thus the proper use of information must fall somewhere between the spectrum of total privacy and complete disclosure. The *restricted access* dimension of this model indicates that the condition of privacy exists where there is a capacity to shield personal data from some parties while sharing with others on a need-to-know basis. Information should be shared only if it is warranted by the situation or context. According to this perspective, an individual has privacy “in a situation with regard to others if and only if in that situation the individual is normatively protected from intrusion, interference, and information access by others.”[7] A “situation” can be described in terms of a relationship, an activity of some sort, or any “state of affairs” where restricted access is expected and justified. For example, a bank should share information about a customer seeking a mortgage with third parties (such as a credit bureau) only when necessary to complete

this transaction. Providing such information to data brokers for marketing purposes would be an unjustified infringement of this customer's privacy rights.

Moor and Tavani also make a critical distinction between situations that are naturally private (such as living like a hermit in the mountains of Montana) and normatively defined private situations (such as the doctor–patient relationship). In a situation where one is naturally protected from access by others, one has natural privacy. In a normatively private situation, ethical norms and legal requirements create a protective zone of privacy because the situation requires such protection. If those principles are ignored, there is a violation or unjust infringement of privacy rights. Natural privacy can be lost, but when this occurs there is no violation of rights. Thus, if you are sitting in a secluded place in a state forest and someone discovers you, you have lost your privacy, but you couldn't reasonably claim that your privacy rights have somehow been violated.[8]

Individuals also need *limited control* over their personal data to ensure restricted access to it. Control can take the form of mechanisms such as informed consent that can meditate online transactions and data exchanges. In situations where a user provides his or her personal

information to a merchant, social media platform, or other professional party, the user will be informed when that information will be shared with a third party and have the capacity to limit the sharing of that information. Thus, the restricted access/limited control theory signifies that one cannot possess information privacy without restrictions on information flows about oneself and without some measure of control over those information flows.

Now that we understand what privacy *is* (a condition or state of limited accessibility), we can briefly consider normative justifications for a right to privacy. Philosophers have made many attempts to ground or justify this right, but the most convincing approaches regard the right to privacy as an instrumental good, which supports other basic human goods such as friendship, security, and freedom. Without the support of privacy, it is exceedingly difficult to cultivate close friendships, sustain a marriage, or enjoy an adequate level of security.

As we have observed in **Chapter 1**, one of the intrinsic goods constitutive of our well-being is bodily life, which includes the "component aspects of its fullness: health, vigor, and safety."[9] Without privacy, we are at risk for threats to our safety and security. If a person's financial data fall into the

wrong hands, that individual can be subject to identity theft and perhaps robbed of her life savings. In extreme cases, a person's life or safety can be at stake because of an invasion of privacy. Even when certain types of sensitive information, such as a person's medical data, are subject by law to restrictions against sharing with others, it is still possible to release that data in a de-identified or anonymous form. And when combined with other publicly available information the data subject can often be re-identified.[10]

A primary moral foundation for the value of privacy is its role as a condition of freedom (or autonomy), which is another critically important instrumental good. A shield of privacy is essential in most societies if one is to freely pursue his or her projects or cultivate intimate social relationships. According to James Reiman, without privacy there are two ways in which our freedom can be diminished.[11]

First, there is the risk of an *extrinsic loss of freedom*, because the lack of privacy often makes individuals vulnerable to having their behavior controlled by others. The unwarranted collection of a person's sensitive information without her awareness and consent can be a potent weapon in the hands of those in positions of authority. Such information might be used to deprive

individuals of certain rewards and opportunities, such as job promotions or transfers, or it might preclude eligibility for insurance and other important necessities. This kind of restriction thwarts our autonomy, our basic capacity for making choices, and directing our lives without outside interference.

Second, there is the risk of *an intrinsic loss of freedom*. It is common knowledge that most people will behave differently when they are being watched or monitored by others. In these circumstances, it is normal to feel more inhibited and tentative about one's plans and activities. There is also an urge to conform with the observer's expectations. As Richard Wassestrom puts it, without privacy life is often "less spontaneous and more measured."[12]

In summary, without the benefit of privacy protection, we are not only more inhibited but also more vulnerable to manipulation and control by others. In this digital era the adverse effects of privacy erosion can be quite subtle and difficult to discern. There are ways in which the extraction and collection of our personal data by companies like Google or Facebook shape our future behavior by the persuasive personal ads and other information they feed us based on that data.

What’s at stake, therefore, is sovereignty over one’s own life and personal experience.[13]

Personal Information on the Internet

Some naïve internet users are still astonished to learn about the plethora of personal data that is now available online. Consider the following scenario. Suppose that you live in a prosperous, leafy suburb of Milwaukee and that you are quite curious about your new eccentric neighbor. Something about her demeanor is rather unsettling and unusual. The internet has many so-called "people search" sites where someone can hunt around for information about another person. In this case you might start off by using the Zaba Search website. You type the woman's name in the simple search box and Zaba gives you personal information such as an address, phone number, and date of birth. Zaba also includes links to other services that provide more information for a small fee.[14] A quick search on Google brings you to the woman's LinkedIn page, where you learn some new details about her job and educational background. You then go to the Milwaukee City Tax Assessment Online database, key in the address, and within seconds you find out the assessed value of her property, her current property tax, and the fact that she has a partial

personal exemption because she is a surviving spouse.

You have spent about 15 minutes on the internet and you have just begun scratching the surface of this woman's background. You could continue and probably build a pretty thorough profile of this woman by using some of the other websites listed on Zaba search. But where does one draw the line in the search for another individual's personal data? Has anything immoral happened here in this incident of "cybersnooping"? Does it make any difference if we make no revelations to others or take no actions based on our findings? Is there anything wrong with the search engines that facilitate this process? Should this type of data be subject to some sort of regulation to limit online stalking and similar abuses?

The question we must first consider is whether information residing on the internet should be so "public" and hence easily accessible. Most of the data that have become fodder for search engines existed in a public or pseudo public format (such as a phone book and court records) and has now become digitized. According to Beth Givens, "Courts and government agencies at all levels—local, state, and federal—are increasingly making public records available on websites."[15] The trend of posting court documents on the internet is

especially unsettling because those documents sometimes contain highly sensitive data.

On one hand, it is easy to see the benefits in having this information more accessible, especially for media investigations that may further the public interest. Converting information into an electronic format and providing a better mechanism to search those data seems to be perfectly acceptable. On the other hand, personal data are being made available in these online databases that are accessible to search engines without our knowledge and consent. Further, there is more going on here than a mere conversion of data from hardcopy to digital format. The internet makes these data globally and instantaneously accessible. One probably would not pore through documents stored in city hall for hours to find out about his neighbor, but if it takes just 15 minutes on the internet, there is more of a temptation to snoop around. Court documents were always public, but few individuals would take the time to physically check through these documents. Also, what makes these data more of a threat is the possibility for recombination of disparate and hitherto unconnected data elements. Businesses could build or augment customer databases using these publicly available data, such as court records, which could easily be searched with

software hubs. Our hypothetical example illustrates that with little effort a fairly thorough profile of someone could be constructed.

Of course, people voluntarily expose many details about their lives, especially through interactive social media. They often leave a trail of writings and photos that make their lives quite transparent. In addition, news stories about people are readily and easily available online, accessible through a simple search on Google. Once newspapers and other print media digitized their archives, even old information became available “forever” in the infosphere. Reports of scandalous, embarrassing behavior are only a click away. In Europe, this development has given rise to claims that there must be a digital “right to be forgotten.” This right, which would force search engines to remove particular search results, significantly expands the scope of privacy rights, and its moral validity is the subject of some lively debate.

An outright ban (or detailed restrictions) on digitized public information (such as court documents) is unrealistic, but so is a laissez-faire approach. One could argue that for security purposes there are certain data elements that should never be in a public, online database, and this includes social security numbers, which are a link to a wealth of other sensitive information.

These databases should also exclude sensitive unique identities, such as mothers' maiden name information, which is used for identification verification at banks and other financial institutions. The ethical justification is that the potential for harm increases exponentially when such items are made so readily available.

Consumer Privacy on the Internet

Privacy-Invasive Technologies

Prior to the Information Age the transactions that occurred between vendors and consumers were private affairs, nobody's business but the two parties involved. They were also quickly forgotten. The local baker knew you by name but probably couldn't remember what sort of breads and pastries you purchased last month. This has changed rather dramatically in the information economy because automated information systems can remember everything for an indefinite period of time. When we use a shopping card at our local supermarket, a data warehouse stores the details of our purchases, and sometimes these data are shared with food producers and others for targeted marketing campaigns. Thanks to networking technologies, any of this information can be easily mobilized and monetized.

Some corporations, such as Metromail, function exclusively as data brokers or information service providers. They specialize in aggregating and maintaining myriad data about consumers. Metromail's National Consumer Database includes detailed information on 103 million people in the United States. Metromail is especially proficient in tracking important transitions in people's lives. For example, if someone has moved to a new house, his or her name will be provided to junk mailers or

other vendors for 25 cents a name. These individuals are obviously prospects for new home furnishings and appliances, cable service, and so forth.

A similar company, Acxiom Corp., searches through public records and other online and offline data in order to build “dossiers” on consumers. It records the make and model of a family’s cars, what their house is worth, and so forth. It sells these personal data to marketers who use this information to make telephone or online pitches for their products.[16] This collection, aggregation, and analysis of information has come to be known as “big data.” Big data is a new paradigm, a way of thinking about knowledge through data and through “finely observed patterns . . . drawn inductively from massive datasets.”[17]

User data that are extracted and aggregated by digital companies and data brokers come from multiple sources. Many apps available for smartphones and other devices also collect data, which are often made available to third parties. For example, almost half of mobile apps that collect health and fitness information sell that information to advertisers. These apps have also shared sensitive personal information with Facebook by using software Facebook had provided to app developers. Very few of these companies have

privacy policies that outline how collected data will be shared with advertisers.[18]

As we have previously discussed, platforms like Google, Yahoo, and Facebook have refined their data extraction architectures to collect vast amounts of relevant consumer information. Google collects data from its search engine for the purpose of personalized advertising, and Google-owned YouTube collects information on what viewers watch. The internet portal Yahoo, now operated by Verizon Communications' Oath unit, analyzes Yahoo mail inboxes and the data they contain to search for clues about what products or services users may find of interest. This email scanning has become an effective method for tailoring ads to its user base. For example, Yahoo's algorithms might classify someone as an "investor" who can be targeted for finance-related advertisements.[19]

Web browsing habits and online commercial purchases are also fair game for merchants and data brokers. When a user visits a website, tiny tracking files monitor what he or she does in order to send marketing pitches for products and services. This is usually done by means of cookies, small data files that are written and stored on the user's hard disk drive by a website when the user visits that site with a browser. They

contain information such as passwords, lists of pages within the website that have been visited, and the dates when those pages were last examined. When the user revisits the website that stored the cookie, the user's computer system quietly sends the cookie back with all of its relevant information. Cookie functionality does not require the consumer's identity because the cookie relies primarily on a unique identifier. But a website can correlate anonymous cookie data with identifiable personal information, if, for example, the user has registered or made a purchase at that website.

Cookies represent a modest means of monitoring a user's movements when they visit a particular website. If a customer visits an online bookstore, a cookie can reveal whether she browses through sports books or is more apt to look at books on wine and gourmet foods. If a user comes to this store merely to window-shop in cyberspace, cookies can provide the retailer with valuable information that could be the basis of a targeted promotion for that person's next visit. For Yahoo, once its intelligent algorithms establish a link between certain emails and consumer preferences, a cookie is placed on the user's computer that allows advertisers to target their ads

to this person when they visit a certain website or conduct a search.

The most controversial manifestation of this technology is the “third-party” cookie. These are cookies placed across a network of related sites so that users’ movements can be tracked not just within a certain site but within any site that is part of this network. Online ad agencies like DoubleClick (now owned by Google) rely on a common cookie that allows it to deliver custom ads any time a customer enters a DoubleClick-affiliated site. It also allows DoubleClick to monitor clickstream data across this network.

Tracking tools are not confined to cookies. Beacons are small pieces of software code installed on a user’s computer that can track a web surfer’s location and online activities. Beacons are often installed by companies like Lotame Solutions, which track web surfers’ activities in order to create databases of consumer profiles that can be sold to advertisers. Both beacons and third-party cookies can track users from site to site, which allows the company that installed these tiny tracking tools on a user’s computer to build a database of online activities. Not only can this information be sold to advertisers, it can also be sold on a data exchange to data brokers who can combine it with offline data.

As we have indicated, the underlying objective behind all this data collection and surveillance is targeted marketing and personalized advertising. Companies extract and aggregate these behavioral data to acquire predictive knowledge for the purposed of ad targeting. It's far more effective to send your ad for a brokerage service to someone who is already an investor or stock trader. More precise marketing techniques eliminate some of the risk and uncertainty in the process of generating new customers. As Borgmann has observed, "the distinctive discourse of modernity is one of prediction and control."[20]

For example, let's say that Mary Merlot is a wine connoisseur. She often does Google searches to gather information and reviews about premium wines. Google will use this information to develop predictive products aimed at sending her targeted ads as she browses the web. She likes to purchase wine online from **www.winesandspirits.com**. On her first visit to the website, she purchases several bottles of Cabernet Sauvignon and spends some time looking at some French wines, such as Pouilly-Fuisse. Thanks to the purchase she makes, the website collects her name, address, phone numbers, and email address, along with her American Express card number. It also monitors

the wines she looks at but does not purchase and acquires information about her browser, IP address, and so forth. Some of this is stored on the cookie deposited on her hard drive when she exits the website. The next time she enters the website, that cookie is retrieved and she receives customized promotions based on her profile and her search history—a banner ad for a new French restaurant in her city, a recommendation to check out the latest imports from France, and a discount if she buys two or more cases of this wine.

Since Mary is a Facebook user, the social media company will also be tracking her online movements. Facebook's web tracking is done with a special cookie architecture that collects data on users' browsing even when they are not logged into Facebook. The cookie would have been placed in Mary's web browser when she visited the **Facebook.com** website. It informs Facebook whenever Mary's browser accesses a web page with an active social media plug-in, such as the ubiquitous "like" button. Since the wineandspirits site has an active "like" button the cookie will report her purchases to Facebook.[21]

Although Mary Merlot may appreciate the personalized ads along with the discounts offered by advertisers, she may have some valid concerns about what could happen to all of these data. Will

her favorite online wine vendor sell these data to third parties for additional marketing campaigns? How will Facebook employ data about her purchasing habits? And how will Google use the predictive knowledge about her it has cultivated from her search history and other sources? Who decides what happens with all this information about Mary and the aspects of her lifestyle she has revealed? And will Mary have a voice in that decision? Probably not. These knowledge and power asymmetries are unsettling and represent a loss of control for Mary and the millions of other users who behave just as she does.

Policy Considerations

How can Mary Merlot's information be protected? Can she ever retrieve some semblance of control over all of this personal information and have a voice in how that information is to be utilized? Should there be tougher laws to guard against data extraction and collection without the consumer's permission? Law, of course, is not the only solution. Recall Lessig's framework: there are other modalities of regulation besides law, including code (or technology), norms, and the marketplace. These modalities are not mutually exclusive, so the answer might well be arriving at the right mix of constraints.

If we choose the legal solution, a comprehensive law protecting consumer privacy would most likely embody two simple values: notice and choice. Companies and organizations would be required to inform consumers about how their data are to be used, and they would not use those data for any other purpose without the consumer's consent. There are two variations of this model. The first is the "opt-in" approach, whereby individuals must explicitly approve secondary (or even tertiary) uses of their personal information. For example, if someone provides credit data to a bank to apply for a loan, the bank cannot sell that data to a marketing company without permission.

The second is the “opt-out” approach, whereby individuals are notified that their personal data will be used for secondary purposes unless they disapprove and notify the vendor accordingly.

Yahoo provides an opt-out option for its email scanning. Users must visit the “ad interest manager” web page and click a button to opt out. A superior Yahoo policy or legal requirement would be a system that lets users deliberately opt-in to the email scanning “service.” Privacy experts argue that the law should force platforms like Facebook to give a user the option of objecting to the collection of his or her personal data for targeted advertising.

If the mechanism of informed consent, reinforced by legal sanctions, is to work properly, regulations would need to ensure that consumers have both knowledge and opportunity; that is, they must be made aware of any projected reuse of their data in a timely fashion and be given a reasonable opportunity to restrict it.

Laws can also be targeted to confine and regulate certain technologies. Given the prevalence of online surveillance, it could be argued that specific laws are needed to protect web browsing activities. Those laws might require that users be informed when a beacon or other tracking tool is

being installed on their computers so that they can immediately be given the opportunity to “opt out.” Laws might also mandate privacy policies that clearly spell out how a consumer’s data will be used.

In purely economic terms, the loss of privacy is a market failure. It is a negative externality analogous to various forms of environmental degradation. For example, the sale or exchange of Mary’s data between two parties imposes a cost on Mary: a loss of her personal privacy. The cost is not borne by the two parties who engage in the transaction but is instead borne involuntarily by Mary, the data subject. But can the market fix this failure? The invisible hand of market forces sometimes compels companies to “get it right” in social terms, but is this likely to happen with privacy rights? Given its endless privacy disputes and consumer backlash, will social media companies like Facebook build a more privacy-focused platform? The problem is that a significant shift to privacy would imperil its steady revenue stream. Most of Facebook’s profits come from targeted ads that are made possible by the open sharing of user information along with the company’s predictive models. The more data extracted, the more added value for advertisers. There is little market incentive to give priority to

privacy unless the company can find some way to monetize these efforts.[22]

It seems highly unlikely, therefore, that free market mechanisms and consumer demands can reverse the trend of privacy erosion on any significant scale. The big payoffs and marketing benefits of trading in the commodity of information are too great to rely on free market forces to bring predatory information collection practices under control. There will probably be no voluntary retreat from the economic imperatives of “surveillance capitalism,” which is driven by digital giants like Google and Facebook.

The third broad approach involves reliance on industry norms and self-regulation. Those norms are often expressed in industry codes of conduct, which member firms are expected to follow. The assumption is that organizations that collect and disseminate personal data will impose constraints upon themselves to avoid infringing upon their customers’ privacy rights. Companies could decide to regulate themselves for several reasons. They may seek to preempt government regulations, which they fear could be more onerous than their own self-imposed constraints. Or they may have purer motives and be convinced that they must act with ethical probity because privacy standards deserve their respect. But given the data-hungry

business models of companies like Google, Facebook, and Yahoo, this type of ethical conversion is an unlikely scenario.

Finally, we must not overlook the role consumers can play in safeguarding their own privacy rights with the help of technology. Browsers such as Internet Explorer or Chrome allow users to view and delete cookies installed on their computer systems. Users can also tweak their browser settings to limit the installation of cookies. In addition, users can install “plug-ins” to monitor tracking activities. Code, therefore, can be part of the solution, as long as users are willing to assume some responsibility to limit their online exposure.

Moral Considerations

How might we assess Mary Merlot's plight from a moral standpoint? Is there anything truly immoral in collecting these data and selling them without her permission to generate extra revenues? Given the importance of privacy as a condition for security in an information-intensive society, a potent case can be made that social media organizations and other corporations that infringe on privacy rights are acting immorally. They are engaging in actions that create the risk of harm for people. When personal information is extracted, shared, and recombined, a more thorough profile is created, and this creates the risk of manipulation by other private parties or organizations. One of the big problems that can occur through electronic profiling is that people can be judged out of context. The fact that Mary Merlot buys a sizable amount of wine online may lead some who examine her profile to jump to the conclusion that she has a drinking problem, when, in reality, she entertains with some frequency.

In addition, the moral problem is compounded by the asymmetries of knowledge and power. These companies know a lot about us but our access to that knowledge is limited. As Zuboff points out, this information is *about* us but it is not *for* us—it is developed and manipulated in the shadows for the

benefit of others who will use it for commercial gains. For example, Facebook users cannot be sure what information the company has extracted, and how that information will be used. Even if we had such knowledge it is still difficult to assess the potential harms. Could we be charged higher prices by some online merchants like Amazon because they have accurately calculated our price sensitivities? Could our online identity discourage banks from giving us an auto loan or a mortgage? What other kinds of discriminatory behavior could we be subject to? Thus, the lack of online privacy opens the door for impairments to our well-being that the extractors of information like Facebook are not even aware of. There is a palpable lack of fairness and justice in this arrangement because it ultimately fails to give users what is due to them: privacy protection that prevents harm such as discrimination.[23]

As we have seen, according to some theories, privacy has been described in terms of secrecy, restricting access to the person and to her decision-making process so that she can carry out her life-plan and build relationships with others without the threat of unwarranted attention or embarrassment. According to William O. Douglas, “Privacy involves the choice of the individual to disclose or to reveal what he believes, what he

thinks, what he possesses." But too many companies ignore every person's right to decide what he or she will disclose or keep secret. Consider Facebook's Beacon program, which disclosed users' purchases to their network of friends without their permission. One user described how his purchase of a diamond ring for his girlfriend was published online to all his friends (including his fiancé to be) without his knowledge or consent. The surprise of the engagement was ruined and what was meant to be a memorable and special event was destroyed. The lack of privacy not only undermines a person's sovereignty over what she wants to reveal about herself but also disrupts personal relationships.[24]

Thus, from both a natural law or Kantian perspective we can assess the salience of privacy rights because of the significant risk of harm that occurs when those rights are disregarded or marginalized. If privacy is a necessary condition for security, which is an aspect of the intrinsic good of life and health, there must be a right to privacy and a correlative duty to safeguard that right. Similarly, important relationships depend on preserving a "sanctuary" for ourselves that allows us to shape those relationships according to our own plans and preferences. When that right is eroded, there is grave risk of damage to some

intrinsic human goods. This moral duty is also consistent with Kant's second formulation of the categorical imperative: "Act so that you treat humanity, whether in your own person or in that of another, as an end and never only as a means." For Kant, this principle is "the supreme limiting condition in the pursuit of all means."[25] The exploitation of sensitive personal data for economic gain in a way that infringes on someone's privacy and security is inconsistent with treating the other as an end.

Of course, what constitutes the wrongful infringement of someone's privacy rights is not always altogether clear. But at the core of a privacy policy manifesting respect for this basic right are the principles of *notice* and *choice.* Companies that extract and process data should inform users about how their information will be used and obtain their explicit consent, so they have real options. There should also be better oversight to ensure that when data are shared with third parties (such as app developers) they are used in accordance with company policies. On the other hand, policy choices that consistently put users at risk are immoral because those choices are contrary to the good of human persons.

The United States and the European Union: Divergent Paths to Privacy Protection

Now that we have considered the general avenues for dealing with privacy—the use of law, industry norms, reliance on the marketplace—it is instructive to compare the different strategies followed by the United States and Europe in their quests to provide privacy rights for their citizens. The United States has relied on a philosophy of light regulation with no comprehensive privacy legislation. The goal is to implement limited privacy protection that is compatible with economic growth. Instead of comprehensive laws, there are targeted regulations that protect privacy rights in certain sectors such as health care. These sectoral statutes are enacted when sensitive information is at stake or the data subjects are too vulnerable. In such situations it is too risky to put faith in the self-correcting mechanisms of the marketplace.

By contrast, in the European Union (EU), privacy is treated as a basic human right deserving the full protection of the law, so broad, cross-sectoral legislation has been developed. The purpose is to solidify the user's right to exercise control over the extraction and use of their data. In this section we

first consider privacy legislation in the United States. Several laws have been triggered by networked information technologies, but in most cases consumer laws developed before the rise of e-commerce are now applicable to internet transactions.

Privacy Legislation in the United States

In the 1960s, the legal right to privacy, recognized decades earlier by Warren and Brandeis, had become more formalized thanks to several landmark Supreme Court cases such as *Griswold v. Connecticut*. In this pivotal case the Supreme Court ruled that a Connecticut law barring the dissemination of birth control information violated the right to marital privacy. The majority opinion also stated that each individual was entitled to "zones" of privacy created by First, Third, Fourth, Fifth, and Ninth Amendments to the Constitution. The justices agreed that privacy was a right "so rooted in the traditions and conscience of our people as to be ranked as fundamental" (*Griswold v. Connecticut*, 1965).

Shortly after the Griswold decision, Congress began to enact selective legislation to protect that privacy. It is difficult to discern a pattern or coherent plan in this legislation because the catalyst for a particular law was sometimes a public event that captured attention. In this context, we cannot review every piece of privacy legislation, but we do cite enough examples to provide a reasonable overview.

In 1970, Congress passed the Fair Credit Reporting Act (FCRA), which regulated and restricted disclosures of credit and financial

information by credit bureaus. The FCRA sets standards for the legitimate use of credit reports and delineates a consumer's rights in disputing those reports. The Federal Trade Commission (FTC) is responsible for enforcing this act. In general, according to the FCRA, a consumer's credit report should be released or provided to a third party only in response to a court order, in response to a written request from the consumer who is the subject of the report, or in response to responsible third parties who intend to use the information. Credit information can also be given to those third parties who have a "legitimate business need" for the information; the meaning of this ambiguous phrase has been further clarified in recent years. As credit report information becomes more accessible online, the FCRA should offer consumers some protection by these limits on disclosure.

The FCRA was followed up by the Right to Financial Privacy Act in 1978, which required a search warrant before banks could divulge the financial data of their customers to federal agencies. Federal investigators must submit formal written requests to examine a subject's banking records, and that subject must be given notice of the request so that he or she can

challenge it. The FCRA offers similar protection for online banking records and related data.

In the 1980s, Congress continued to pass legislation intended to better protect the privacy rights of U.S. citizens. In 1984 it passed the Cable Communications Policy Act, which prohibited cable television companies from collecting or disseminating data about the viewing habits of their customers. A related piece of legislation was the Video Privacy Protection Act of 1988, which bars rental video stores from disclosing a list of videos watched by their customers. This act was passed as reaction to public outrage after journalists were able to retrieve Robert Bork's video rental records during his contentious (and unsuccessful) Supreme Court confirmation hearings. Some have argued that Congress may have overreached when it passed the Video Privacy Act. But there are valid reasons behind safeguarding this sort of information. As Rosen argues, "people are reluctant to have their reading and viewing habits exposed because we correctly fear that when isolated bits of personal information are confused with genuine knowledge, they may create an inaccurate picture of the full range of our interests and complicated personalities."[26]

In 1994, Congress was prompted to protect motor vehicle records, and so it passed the Driver's

Privacy Protection Act. This piece of legislation prohibits the release or sale of personal information that is part of the state's motor vehicle record (social security number, name, age, address, height, and so forth) unless drivers are provided an opportunity to opt out. Prior to the enactment of this legislation, the sale of these data to third-party marketers, a lucrative business for many states, would usually occur without permission or notification. The catalyst for the passage of this act was the murder of actress Rebecca Schaeffer by a crazed fan who obtained her address from the California Department of Motor Vehicles.

In 1998, Congress passed the Children's Online Privacy Protection Act (COPPA), which forbids websites from collecting personal information from children under age 13 without parental consent. This legislation was in response to growing complaints from parents. Enforcement of COPPA, however, has not been so easy. Many child-oriented websites just meet the letter of the law by merely posting a disclosure that the site is not for children or they believe a child when they enter the age or click the OK button when it asks if the user is at least 13 years old. Despite these implementation problems, the law is having some salutary effects. According to Wasserman, "At the

very least, the law has compelled some sites to rethink the way they communicate with kids."[27]

And, in 1999, Congress passed the Gramm–Leach–Bliley bill, also known as the Financial Services Modernization Act. The main purpose of this deregulatory legislation was to make it easier for banks to merge with companies selling securities and insurance. The act also contained a key provision requiring financial services companies to disclose their information privacy policies in writing to their clients once a year. They must also provide their customers with an opt-out form that enables consumers to forbid the selling or sharing of their financial information. The burden is on the customer to return the form. So far, as one might expect, the opt-out forms are being returned at a surprisingly slow rate. Critics contend that the privacy notices are too confusing (some are several pages long and enshrouded in legal terminology) and that an opt-in system, where privacy is the default, would have been a better solution.[28] Some companies have gone beyond the law and adopted the opt-in approach. In response to this legislation FleetBoston developed a new privacy policy stating that "the company won't share nonpublic customer data with nonaffiliated third parties for marketing purposes unless the customer authorizes it to do

so."[29] The company has deliberately adopted this proactive privacy policy to gain the loyalty and respect of its customers.

Finally, in April 2001, new rules went into effect to protect medical privacy. Those rules were mandated by the Health Insurance Portability and Accountability Act (HIPAA), and they prohibit healthcare providers from using and disclosing patient information without the patient's consent. This means, for example, that hospitals can no longer sell the names of pregnant women to manufacturers of products such as baby formula. Patients now have the right to access, examine, and copy the information in their medical records. The restrictions also limit the disclosure of health information to the "minimum necessary" for a specific purpose (such as paying bills). This provision is designed to end the practice of releasing a patient's whole record when only several specific pieces of information are needed. And new criminal and civil sanctions have been established if medical data are improperly used or disclosed.

What becomes evident as one examines this legislation is that the attempt to protect personal privacy in the United States through legal measures has been highly reactive and unsystematic. As a result, what we have is an *ad*

hoc and fragmented approach rather than a coherent body of federal privacy legislation predicated on a discrete set of privacy principles.

The current legislative philosophy reflects a commitment to a dichotomy of public and private information that reserves legal protection for certain spheres of a person's "private" life. It ignores contextual issues that can play a role in the erosion of privacy.[30] The United States has so far avoided comprehensive prescriptive privacy legislation. Policy makers have apparently assumed that responsibility for privacy protection belongs primarily with the private sector and not with the government. The aim is to rely on corporate self-regulation and public pressure, but when companies fall short the FTC intervenes.

Privacy Protection in the European Union

The situation is quite different in Europe, however. For some time, European countries like Sweden and Germany have adopted a much more proactive approach to the protection of privacy rights than countries like the United States. Part of the reason behind this different philosophy is Western Europe's conceptualization of privacy as a matter of "data protection," and its view that privacy is rooted in basic human rights. There has also been a long-standing assumption that the state must have a major role in protecting personal information.[31] Unlike Americans, Europeans have not become preoccupied with interminable debates about justification of privacy as a normative concept.

Data protection legislation in some European countries was formulated as far back as the early 1970s. The data protection law of the German state of Hesse was the first such law in the world. Several years later, in 1973, Sweden passed its Data Protection Act, which was designed to prevent "undue encroachment on personal privacy." The purpose of these early laws was to control the process of data processing, particularly the processing of the copious information required by the emerging social welfare bureaucracies. According to Mayer-Schonberger, European

legislatures in the early 1970s saw the need to enact “functional data protection norms focusing on processing and emphasizing licensing and registration procedures aimed at controlling *ex ante* the use of the computer.”[32]

During the 1980s, data processing became much more decentralized. As a consequence, there were no longer just a few massive central databases, but a variety of databases on mainframe and minicomputer systems dispersed throughout Europe. This gave rise to a second generation of “data protection” laws where “existing individual rights were reinforced, linked to constitutional provisions, broadened, and extended.”[33] The focus shifted to the individual, who was given the right to have some say over the process of data collection and transfer. Subsequent legislation has strengthened and reinforced those rights.

In addition, enforcement of privacy legislation has not been taken lightly. European countries such as Germany, the Netherlands, Italy, and Sweden have established government agencies dedicated to the objective of privacy protection. In Sweden, for example, the Data Inspection Board issues licenses to keepers of commercial databases containing consumer information and carefully

monitors any matching or recombining of data from one database system to another.

In October 1995, acting on behalf of all of its member countries, the EU Parliament adopted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. The goal was to harmonize the different rules and regulations that had been developed by the member states. It is known simply as the *European Union Directive on Privacy*. The directive imposed an obligation on each member of the EU to enact legislation that implements these privacy norms. The primary objective was clearly articulated in Article 1: “to protect the fundamental rights and freedom of natural persons, and in particular the right to privacy with respect to the *processing of personal data*” (emphasis added). The directive concentrates on the processing of data or the flow of information between organizations; there is less attention paid to how data are collected and stored.

Article 6 delineates several important principles regarding that processing: “Member states shall provide that personal data must be (a) processed fairly and lawfully; (b) collected for specified, explicit, and legitimate purposes and not processed in a way incompatible with those

purposes . . . (c) adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date. . . .” With Article 6 the directive mandates a certain level of data quality, ensuring that data are adequate, relevant, precise, and accurate.

Also important for understanding the core principles of this directive is Article 7, which seeks to explicate the “criteria for making data processing legitimate.” Data may be processed when the data subject has provided his or her consent, the processing is necessary for the performance of a contract between the organization and the data subject, the processing is necessary “in order to protect the vital interests of the data,” or for the “performance of a task carried out in the public interest.” There are special restrictions for data of a sensitive nature (such as information concerning one’s ethnic background or religious affiliation). The directive also gives the data subject the right to notice about the processing of his or her personal data, along with the right to access that data and correct mistakes. Finally, the directive stipulates that EU citizens have the right to a national privacy agency to enforce all of these rules and protections.[34]

In 2018, the General Data Protection Regulation (GDPR) went into effect and replaced the EU's Data Protection Directive. The GDPR is now the fundamental law that protects the personal data of all EU citizens. Companies that have been in compliance with the original Directive must ensure that they are compliant with the stricter requirements of the GDPR. Articles 17 and 18 of the GDPR give the data subject more control over their information that is extracted and processed automatically. Companies can only collect and store the minimum amount of user data needed to provide a specific service. The GDRP also gives users the right to obtain a copy of the records the company has compiled about them. For social media companies like Facebook, these records would include any categories, descriptions, or "behavior scores" that were assigned to them.[35]

According to the GDPR, all digital companies, including Facebook, Google, and Yahoo, must use clear and straightforward language to explain what consumer data they are collecting and how they will use those data. In addition, users have a right to portability so they can easily transfer personal data between service providers and a "right of erasure." The latter right means that consumers can direct companies to erase their personal data (under certain conditions). Finally, articles 31 and

32 pertain to data breaches. Companies must notify authorities within 72 hours after discovery of a data breach and notify data subjects as quickly as possible. The marketplace is still waiting to see how the GDPR will be interpreted by the European judicial system. It remains to be seen, for example, whether Google's real-time bidding for online ads based on user search history and behavior is a violation of the law.[36]

A Prescription for Privacy?

It should be evident by now that the problem of privacy is quite complex. Privacy is difficult to define and there are endless paradoxes that can confuse regulators. People are indignant when they hear about privacy breaches but do very little to protect their own privacy, even when the tools are available to do so. They have general concerns about the erosion of privacy but rarely worry about what happens to the information they provide to online vendors or in social networking venues. People don't like to be tracked on the web, but they have grown accustomed to targeted advertising based on their physical location, web-browsing history, app usage, and other personal information. Of course, if beacons are banned and the digital cookie "crumbles," that personalization goes away, along with some free services on popular websites.

There are many tools available to protect privacy and so code may seem a promising approach. However, there is an emerging consensus that code and self-regulation are inadequate to deal with this intractable problem. Evidence of this is the long history of privacy transgressions by corporations and the most recent behavior of

companies like Google and Facebook, which arguably engage in transgressive practices in order to monetize and manipulate user information. Digital information is the currency of the new economy and there is too much market incentive to commoditize information, even when privacy may be compromised. Also, the individual user is no match for the extraction architectures perfected by the likes of digital titans like Facebook.

As we have discussed, despite privacy's paradoxes, the Europeans have opted for a blunt solution that relies on a comprehensive legal framework to safeguard privacy. This "omnibus" approach is probably well suited for the culture and political tradition of Europe. The idea of the benevolent state enforcing corporate social responsibility has had considerable appeal in most European countries for quite some time. The United States, on the other hand, has opted for sectoral-specific statutes that protect sensitive information such as medical data. In contrast to the constitutions of most European states, there is no right to information privacy in the U.S. Constitution. Hence, privacy legislation is enacted incrementally, creating specific zones of privacy in the areas of health care, financial information, and so on.

Although there is much to be admired with the European approach, the drawback is the financial burdens that accompany an elaborate regulatory regime. Economists like Ronald Coase have long been skeptical of relying too heavily on government regulations due to the magnitude of the costs necessary to regulate so many externalities like privacy erosion. Both the original Directive and the new GDPR require an expensive bureaucratic infrastructure for their enforcement. Government intervention is not always welfare enhancing, and sometimes the intervention does more harm than good, especially if self-interested policy makers are captured by industry interests. Not everyone shares this pessimism about the efficacy of government intervention, but it is essential to bear in mind the limitations of relying on the state to guarantee our privacy rights, especially when the state itself can so easily violate those rights.

Moreover, some legal solutions are ineffectual because they are typically predicated on dichotomizing public and private information. In the U.S. system some networked spaces, such as medical records, are off limits, while others, like the user information on a Facebook page, are not protected by specific privacy laws. Hence it is not unlawful to harvest those data, link them to data

captured by tracking a user's comings and goings on the internet, and sell the whole package to data brokers seeking to deliver targeted ads.

As Helen Nissenbaum has pointed out, the effort to distinguish public from private information based on that information's sensitivity has serious drawbacks. It is increasingly difficult to determine what constitutes "sensitive" information in an age when information processing systems are so pervasive and possess such potent aggregative capabilities. In addition, there is a tendency to presume that information provided to businesses, especially ones in the IT and information industries, is "up for grabs" and available for collection and disclosure to third parties. However, these practices, which are forbidden in sectors like health care or education, may not align with the privacy expectations and needs of consumers.[37]

According to Nissenbaum, for several reasons there must be far more attention paid to context. First, although a piece of data may be benign in isolation and hence apparently not worthy of legal protection, that same piece of data could become revealing if combined and aggregated with other bits of data. Users need more contextual information about how their data will be used and disseminated if they are to have any hope of preventing potentially harmful data aggregations.

Second, rather than adopt rules developed for specific sectors (such as financial institutions), a superior approach concentrates on preventing improper information flows that violate "context-specific informational norms." Informational norms are determined by the actors involved (i.e., the subjects, senders, and recipients of information), the information type, and the transmission principles that specify constraints on the information flows. For Nissenbaum, to respect privacy is to respect "contextual integrity," that is, informational norms that support transcendent ethical and social values as well as context-specific purposes and values. Thus, these informational norms, rather than standards set according to specific sectors, should become the foundation of policy and practice.[38] Similarly, Cohen advocates "just aggregation" principles that would preserve the "spatial disconnects" that separate one context from another.[39] It would not be easy for any legal system to incorporate the requirement of contextual integrity proposed by Nissenbaum. But real privacy is impossible without paying attention to peoples' reasonable privacy expectations and to the informational norms based on those expectations.

In conclusion, given the failure of self-regulation and the irrational behavior of many consumers,

comprehensive laws like the GDPR may be the only viable resolution to the privacy conundrum. Too many digital companies have consistently prioritized data extraction and processing from its user base over privacy protection. They have little market incentive or moral impulse to initiate any substantial changes or prevent abuses. Facebook, Google, and other corporations need to be regulated more tightly. The law, for example, should finally coerce Facebook to change policies, such as the one that requires Facebook subscribers to allow the social media giant to track their activities on other apps and websites. Perhaps, with the assistance of comprehensive laws, users can begin to regain control over their lives and recover the capability to decide how and what they will disclose to others.

Privacy in the Workplace

Privacy Rights at Risk

During the past three decades technology has significantly redefined the nature of work as corporations and employees rely more heavily on networked information technologies (IT) to process data and help control far-scattered operations. IT has enabled many corporations to redesign the flow of work and automate more routine processes. The internet has clearly played a major role in all of this by expediting interorganizational communication and information flows.

But there is a more ominous side to this digital transformation of the workplace. Technology has also facilitated greater control over employees and a heightened intrusiveness into their private lives. Some omniscient employers, for example, check the whereabouts of their employees through GPS tracking or maintain health surveillance databanks. They also regularly monitor an employee's incoming and outgoing email, voice mail, and web-surfing habits. There is a real danger that the workplace is becoming a panopticon where workers' activities and interactions are almost completely transparent to the corporate hierarchy.

The category of tools utilized to filter and monitor employee internet usage is known as Employee Internet Management (EIM) software. In the 1990s an employee could rely on some private space at

work (such as email), but now that privacy has evaporated. Some EIM products such as WorkExaminer or Cerebral Security are designed primarily for website control. They keep an eye on websites visited, applications used, and chat activities. Other software systems such as iMonitor provide a more integral solution. This software allows companies to monitor up to 1,000 computers from a central server. It monitors every keystroke, clipboard activities, document activities (moving, cutting, pasting, printing), email, websites visited, and online searches.[40]

Some company policies that push the limits of the law provoke questions about how far corporations can go in monitoring their employees. Every company can access what is on work devices in the workplace, but what about a computer (or mobile device) purchased by a company for work purposes but also used at an employee's home as a family computer. Should companies be able to remotely access and inspect these devices which will usually contain a great deal of personal information? A typical policy statement stipulates corporation X's right to read, access, or monitor all electronic documents stored or processed on X's computers, including documents and messages that don't directly relate to X's business. But what

are the limits of corporate cybersnooping on their workers?[41]

Employers claim that monitoring is essential to guard against the loss of trade secrets and to prevent abuses of their computer systems. Companies worry that employees will use this proprietary information to start a competing business or send it to unauthorized third parties for profit or revenge. They also contend that monitoring helps in performance evaluation. For example, customer service representatives who interact over the phone are monitored for accuracy and politeness.

Despite the occasional rebellion, there is little sign that this trend is about to reverse itself any time soon. Most employers have no problem with these practices and define workplace privacy rights so narrowly that there is ample room for the expansion of monitoring technologies. Some rights advocates, however, see routine monitoring as a perilous policy. Sewell and Barker, for example, argue that we cannot be indifferent about this matter but must adopt a “critical disposition towards workplace surveillance that can be used to engage with its ‘dangerous side.’”[42] They argue that, at the very least, questions should be posed in each context about the necessity and legitimacy of the surveillance, which should lead us to

“confront and challenge the basic reasoning behind its existence.”[43]

Comparing U.S. and European Policies

It is probably not surprising that the European legal systems differ from the U.S. system on the issue of workplace monitoring. In the United States, there are virtually no laws that expressly forbid workplace surveillance. The Fourth Amendment to the Constitution stipulates the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” But this right applies only to the government and not to private organizations, so it offers little protection in the workplace. In addition, the Electronic Communications Privacy Act (ECPA) of 1986 amended the federal wiretap law to protect cellular telephones, electronic mail, pagers, and electronic data transmissions from unauthorized wiretaps. But the ECPA makes an exception for private communications systems and it excludes telephones or devices “furnished to the subscriber or user by a provider of the . . . communication service in the ordinary course of its business.”[44] Thus the ECPA offers little protection for workers’ privacy rights.

On the other hand, the laws in many European countries, such as France and Italy, offer much more extensive protection. In Italy, the Italian Workers Statute “prohibits remote surveillance of

workers by video camera or other devices," unless agreed to by the union for the sake of a business necessity; even then, a worker has the right to challenge the surveillance.[45] In addition, the Italian courts have interpreted this law broadly, forbidding software installed exclusively for the purpose of monitoring and controlling a worker's performance.

Similarly, French law has been equally sympathetic to employee privacy rights. Consider Article 120-2 of France's Labor Code: "No one may place restrictions on the rights of persons and individual or collective liberties which are not justified by the nature of the task to be accomplished and proportional to the objective sought." The French courts have interpreted this broad statue in favor of employees. According to Rothstein, "courts have penalized employers for collecting or processing electronic data concerning employees without informing employees in advance, consulting with the works council or submitting a declaration to the CNIL [National Commission on Data Processing and Liberty]."[46]

Europe's human rights court has ruled that companies can monitor employee email, but only if they are notified in advance. The decision came from the European Court of Justice of the EU which explained that "it is not unreasonable for an employer to want to verify that the employees are

completing their professional tasks during working hours." However, the Court also concluded that it is insufficient for employers to have a general policy that permits employee monitoring. The policy will have to be more specific, detailing *why, how, and where* employees can be monitored and delineating how the information collected could be used. And employees must be duly informed of this detailed policy.[47]

What accounts for this discrepancy in how employee privacy is regarded in the United States and in Europe? According to Rothstein's analysis, the basis of this different treatment is continental Europe's emphasis on dignity. Whereas Americans talk about the value of privacy and the need to weigh that value against other concerns, most European countries stress the worker's dignity, which must not be unjustly compromised just because he or she is in the workplace. Dignity connotes intrinsic worth, and each person has dignity by virtue of his or her rationality and autonomy. When overly intrusive workplace surveillance invades the private sphere of an employee's life, there is an affront to that person's dignity (not merely the infringement of abstract privacy rights). This focus on the worker's dignity makes it easier to appreciate the potential perniciousness and threat to a worker's well-being

when she cannot keep certain information about herself private.

The Case for and against Monitoring

Before concluding this chapter, it would be instructive to review the ethical arguments for and against such extensive workplace monitoring. Do corporations have a moral prerogative to inspect email or to monitor the web traffic of their workers? Or should employees be able to communicate via email and visit websites without the fear that their activities will be observed by officious managers?

Although most organizations support the notion that their employees are entitled to some level of privacy protection, they have adopted policies that allow for extensive monitoring. The level of such monitoring varies. Most companies monitor internet usage and email messages; some monitor phone calls and periodically review an employee's computer files or documents. They also routinely monitor employer-provided mobile phones or devices. Monitoring apps record an employee's text messages, email communications, internet usage, contacts, and call logs.[48]

Email has been one of the prime targets for such monitoring for quite some time, because it has become such a vital communication tool for workers. Employees are usually notified that their email is not considered private and can be read at any time by their managers or other authorized company officials. The core argument justifying

this policy is simple: an email network, including its contents, is owned by the employer, and hence the employer has a right to inspect these messages whenever it is deemed necessary. Employers contend that they have the right to read incoming and outgoing email to make sure that employees are not using company property for private purposes or for transmitting corporate secrets. There is an apparent conflict between the rights to ownership and privacy, and the employer claims that property rights should take precedence.

Those who support monitoring point out that employers can be held liable for what their employees transmit over a corporate email system, either to those within the company or to external parties. If an employee uses that system to indulge in sexual harassment, the company might be held legally liable if it can be demonstrated that they are too tardy in taking corrective actions. Companies also point to recent federal legislation such as the Sarbanes–Oxley Act, which requires corporations to prevent the unauthorized release of material corporate data. Without filtering outbound messages, they argue, it would be difficult to ensure compliance. Hence the need for careful and routine monitoring.

Supporters also argue that the law is firmly on their side. The case of *Smyth v. Pillsbury Co.* has

established the most important precedent since this ruling was made in a federal court. In this case, Mr. Smyth filed a wrongful discharge suit against Pillsbury. He was terminated for inappropriate use of the company's email system. In one email message in which Smyth was expressing his disgust with some of his managers, Smyth said that he would "kill the backstabbing bastards." According to Smyth, Pillsbury had informed its employees that email communications were confidential. Pillsbury said that all employees were told that their email should not be considered "secure" and could be inspected by the company at any time. The U.S. District Court for the Eastern District of Pennsylvania ruled in Pillsbury's favor. The court stated that company email does not demand privacy protection because email by its very nature is a public form of communication and employees should therefore have no expectation of privacy in their email messages. The *Smyth* ruling has been reaffirmed in a number of more recent state cases such as *Falmouth Firefighters Union v. Town of Falmouth*. This Massachusetts court once again concluded that there is no expectation of privacy for email communications in the workplace.[49]

Despite these rulings, there are several convincing moral arguments supporting stronger workplace

privacy rights. We focus on one line of reasoning that seems especially pertinent. Jim Moor has argued that although privacy is not a core value (because one can envision cultures that flourish without privacy), privacy is an articulation of security in some cultures. And security is a core value; no person or culture can thrive without being secure. According to Moor, “As societies become larger and highly interactive, but less intimate, privacy becomes a natural expression of the need for security.”[50] Thus, a strong case can be put forth that privacy should be considered an indispensable instrumental good because of its link to security in an information-intensive environment.

The plausibility of this argument is confirmed when we consider the ramifications of privacy’s erosion in the workplace. Without a reasonable level of privacy, employees cannot be secure in their work environment. Genetic testing, constant surveillance by hidden cameras, GPS tracking, and so forth, are intrusive activities that could reduce an employee’s security, that is, the employee’s ability to protect herself from undue harm. These data, particularly when taken out of context, can lead to adverse judgments and the possibility of manipulation by one’s supervisor or others who might have objectives opposed to the

employee's welfare. Therefore, in order to remove the threat to an employee's security in the workplace, employers must only collect and use job-relevant information. Such information should be restricted to what will help employers protect themselves against theft and other employee abuses or will play a material role in evaluating employee job performance. On the other hand, the extraction and use of data irrelevant to the employer–employee relationship is a violation of an employee's privacy rights and cannot be morally justified.[51]

Even the European Court of Justice has acknowledged that most employers need to monitor email and other online activities for their protection. But companies should develop specific, detailed policies and employees should be informed of this policy to better protect their interests. U.S. companies should follow Europe's lead and inform employees why, how, and where their electronic communications will be monitored. Some data, such as employee personal email, even on a work device, should be off limits. What must be avoided is overly intrusive monitoring or surveillance that does not yield authentic job-relevant information. A presumption should be given to a *prima facie* or conditional right to workplace privacy, given that privacy is such an

important instrumental good. Companies should strive to use monitoring systems that avoid infringing on an employee’s privacy. When this is not possible the burden should fall on the employer to justify why a more invasive monitoring system is absolutely essential.

DISCUSSION QUESTIONS

1. Analyze the costs and benefits of a legal resolution to the privacy problem. Is the European model worth emulating in the United States?
2. What is your general assessment of those snippets of code called cookies or beacons that collect personal data about buying habits? What about Facebook's datr cookie? Do they help or hurt consumers?
3. Is it morally acceptable for an employer to inspect the contents of a computer paid for by the corporation but installed at an employee's home? How would you define the scope of workplace privacy rights?
4. Almost every major commercial website has a privacy policy. Visit one of these sites in order to read and evaluate that policy. Is the policy clear and comprehensible? Does it afford enough protection for that site's customers? For example, check out a site such as **http://privacy.yahoo.com/privacy/us**.

Case Studies

Privacy and the Right to Be Forgotten

Henri was a well-known shopkeeper and café owner in a small town on the outskirts of Paris. He was thrust into a vortex of controversy in the summer of 2007 when he was falsely accused of sexual harassment by a disgruntled clerk under his employment. Henri was completely exonerated, but links to old, damaging articles in the local newspaper remained accessible through Google. That newspaper was particularly aggressive in its initial coverage of the events and did not give Henri the benefit of the doubt, despite his protestations of innocence. Years later, people still brought up the incident to him or his family, often with an accusatory tone. Henri wanted this portion of his past, full of these false allegations and innuendos, to be expunged. Since most people came across this reporting through their search of Google.fr, he had asked Google for its help in suppressing the links to these old stories. Google was not interested in responding to

his repeated requests for its assistance in removing these links.

There are two attributes of internet data that cause problems for victims like Henri: internet data are both permanent and easily accessible. Web pages are rarely deleted, and sometimes those that are deleted are nevertheless preserved by caching services like Google Cache and the Internet Archive. At the same time, search engines like Google and Bing make all of those data exceptionally easy to access.[52]

It seemed that people like Henri would never be able to control incriminating information about their past circulating on the internet. However, in 2014 the European Union Court of Justice issued a surprising court order against Google. It demanded that the search engine company remove hyperlinks that connect search engine users to content that is “no longer necessary,” or “inadequate, irrelevant, or no longer relevant.” Exceptions are warranted if there is some “preponderance of public interest” at stake. Thus, if someone like Henri asks Google to remove these links to “irrelevant” and

outdated material, the search engine company must oblige this request.[53]

The European Court's decision was based on the "right to be forgotten," which was cited as a basic aspect of a person's overall privacy rights. The legal authority of this right to be forgotten is found in the Data Protection Directive adopted by the European Parliament in 1995. The Directive established a comprehensive privacy framework in the European Union, requiring that data "controllers" respect the privacy rights of all "data subjects."[54]

Advocates of this right claim that individuals should be able to insist on the removal of old, irrelevant material that infringes on their basic privacy rights. Skeptics of this new legal development, on the other hand, expressed their unease about the burdens placed on search engine companies like Google. There was also concern that the deletion of these links for private interests could lead to "counterfeit histories."[55] What about the public's right to know this information that is now filtered out thanks to an individual's complaints about irrelevancy?

The EU's decision establishes a new but more precarious boundary between privacy and free speech that clearly favors privacy. The decision is in keeping with Europe's tradition of giving equal weight to privacy and free speech rights. In the United States, however, priority is generally given to free speech rights, and so it is probably unlikely that a version of the "right to be forgotten" will be codified in U.S. law.

Google agreed to comply with the European Court's ruling but acknowledged the difficulties with implementation. Within a few months after the ruling, Google had received over 100,000 requests for the removal of links to "irrelevant" or "unnecessary information." The EU's order, however, applied only to European domains such as Google.fr or Google.co.uk—not to **Google.com** itself. Some privacy rights advocates claim that this doesn't go far enough and that the ruling should apply globally in order to fully protect the data rights of European citizens. There are other questions about how extensively to apply European privacy rules, such as whether or not publishers should be allowed to appeal

Google's decision to remove links to their content.[56]

Questions

1. Do you sympathize with the plight of someone like Henri? Do you agree that the right to be forgotten is an aspect of one's overall right to personal privacy?
2. Has the European Union recalibrated the balance between privacy and free speech too heavily in favor of privacy?
3. Has Google gone far enough to protect this right from being deprived?

Case Studies

Facebook’s “Unfriendly” Privacy Policies

Facebook CEO, Marc Zuckerberg, couldn’t quite believe all the attention he was getting. Facebook was on the verge of its initial public offering (IPO), and it seemed that the media couldn’t get enough of this Cinderella story. Zuckerberg had created a primitive version of the social media application in his Harvard dorm room. Thanks to its immediate popularity, he commercialized this product and founded Facebook, a pioneer in social networking. There were 1.4 billion active users on Facebook and the company’s revenue exceeded $12 billion. As Zuckerberg traveled around the country to promote the IPO, the press followed him everywhere. The Facebook IPO took place on May 18, 2012, making many of its brash and talented managers instant millionaires by the end of 2014. Since the IPO, Facebook’s user base has expanded to 2.7 billion. It has also grown by making strategic acquisitions including WhatsApp and Instagram.

Most people at the social network company welcomed the publicity and attention surrounding the IPO. But over the years Facebook has attracted negative publicity and unwelcome attention for its controversial privacy policies. Facebook has had to deal with several embarrassing missteps as it struggles to reconcile user privacy with an open network. The company's policies have been the object of scrutiny by the U.S. Federal Trade Commission, which has investigated a number of privacy-related complaints. Problems arise from Facebook's business model: collect voluminous information about the user base so that advertisers can target Facebook users with more precision.[57] This case reviews some of Facebook's most contentious privacy policies and disputes.

Facebook first caught the attention of privacy advocates in 2007, when it implemented a technology known as the "News Feed." This feature was designed to display in real time changes a person makes to her user profile on the home pages of all of her online friends. A Facebook user like Sally no longer had to visit the pages of all her friends to see updates since those updates were now

automatically shared in a stream of data appearing on Sally's homepage. To the surprise of the company, users initially balked at this innovation and Facebook had to abandon this default feature, but it has now become the "most valuable billboard on earth."[58]

In that same year, Facebook launched an ill-fated venture known as the Beacon program, a new way to "socially distribute information." Thanks to Beacon, advertisers and web merchants could track user purchases across the internet. A Facebook user's purchase on a website (such as Amazon) was disclosed to his or her network of friends as soon as the purchase was made. This information was conveyed without the user's knowledge or consent. The Facebook community protested the online tracking along with the immediate disclosure of these aspects of their personal history. As resistance mounted, Facebook abruptly ended the program.[59]

In 2010, Facebook once again shocked many of its users by suddenly changing its privacy settings. In its early years, Facebook shared most profile fields only with friends

and friends of friends. But the policy was modified so that information that was once private such as one's profile picture, name, gender, address, professional networks, and so forth, became publicly available by default to everyone online. As one observer noted, Facebook changed the defaults to more efficiently monetize customer information and because the company "appreciated its power."[60] Facebook's decision to make previously confidential information "publicly available" was reversed thanks to public protest, and users now have the capability to control access to most of their personal information.

Despite these and other problems, Zuckerberg insisted in 2010 that privacy was no longer a "social norm." There was an expectation that people wanted to be more open about their lives and activities. Zuckerberg and other Facebook executives remained convinced that the social media company's innovations were ahead of the convictions of its user base and not in opposition to them.[61]

In order to expand its revenues the corporation decided to open its platform to

outside developers. Programmers could build Facebook games, develop personality tests, or construct other apps. These programs were offered to users for free in exchange for information. For a few years the Facebook developer platform hosted several popular games including Farmville and Candy Crush. Facebook customers agreed to give these game developers access to their data in exchange for playing these games. However, there were no protections for the reuse of these data collected by the developers. Algorithms were extracting items such as users' messages and photographs. One game developer used Facebook data to construct unauthorized profiles of children on its own website. Facebook had allowed for the sharing of its customer data without a system to prevent any abuses.[62]

In 2009, Facebook introduced a remarkable innovation which it called the "Like" button. The famous plug-in was a matter of internal debate among Facebook executives for some time. But they gradually realized that this simple button could "transform the platform from a book into a blizzard of mirrors." The more things a user liked, the

more she revealed about herself, her preferences, interests, and aspirations. Facebook now knew what their users “liked” along with their friends and relationships. This data gold mine allowed advertisers to target those Facebook users with even greater precision.[63]

Facebook’s tracking of its users across the internet had begun in 2010 with the help of the Like button. At first, Facebook denied that it was tracking users as they surfed the web. But by 2014 internet tracking was an established corporate policy and part of the contract between Facebook and its users. Facebook collects data on its users’ internet browsing even when they are no longer logged into their Facebook accounts. This happens by means of a small piece of technology known as the “datr” cookie that Facebook deposits in each user’s web browser (once they log on to **Facebook.com**). The datr cookie informs Facebook whenever that browser visits a website with an active social plug-in, such as the “like” button. This tracking of website activities and purchases allows Facebook to build a more detailed profile of their users as the basis for more personal ads. Users are

informed of the tracking (in the dense terms-of-service agreement), but they do not have the option to opt out of this practice, which has riled European authorities. They claim that Facebook has unfairly leveraged its power to collect data on the activities of Facebook users on those third-party sites that use tools such as the “like” button.[64]

It remains to be seen whether Facebook can successfully fend off regulators in Europe and the United States and live up to the expectations of its investors, who expect the company to continue leveraging the commercial value of the information it collects. Facebook became a social media behemoth by collecting user data when there were few privacy restrictions. There are now stricter laws in Europe, and if similar laws minimizing data collection are enacted in other countries, Facebook may be able to crush would be competitors who want to challenge Facebook using the same business model that made Zuckerberg’s company so successful.[65]

Questions

1. Which of Facebook’s past or present privacy policies do you find to be the

most troubling? Which ones are not a “big deal” in your estimation?

2. Should social media sites like Facebook be subject to more regulations to ensure the preservation of privacy rights?
3. Do you agree with Zuckerberg’s claim that privacy isn’t an important social norm anymore?

Case Studies

The Monitoring of Social Media by Employers

Monitoring and electronic surveillance of employees in the workplace has a long and complex history. Workers have always felt uneasy about such intrusions but have had little legal recourse. Disputes quickly arose when companies began to systematically monitor email accounts of their workers. Workers objected, but several key court decisions such as Smyth v. Pillsbury have strongly affirmed a corporation's legal right to monitor virtually all of the digital activities of their employees.

The debate about employee monitoring has now shifted to social media. Social media has generally been more popular for personal matters rather than work-related ones, but it has a growing presence in the workplace. LinkedIn is a social network for professionals and is a popular workplace tool that provides an online contact book, curriculum vitae, and publishing platform for anyone in the labor market.[66] Facebook is trying to establish a presence in corporations, but some companies ban

Facebook because of its detrimental impact on worker productivity.

However, monitoring a person's personal Facebook page has become routine for some businesses. There is a wealth of information on these pages that makes a worker's life and activities highly transparent. Moreover, consultants predict that online monitoring of social media by employers will rise over the next decade. Their research also shows that younger people are more open to sharing their personal data with their employers, with 36% of younger workers saying they would be happy to do so.[67]

Social media offers a tantalizing opportunity for employers to gain some insight into the personal lives and preferences of their employees. It is also a way to detect potential problems and weed out unattractive job applicants. It is fairly common for employers and head hunters to check out a candidate's background and qualifications on social media. They are interested in seeing what a person's Facebook page reveals about his or her skills, personality, political leanings, recreational activities, and so forth. Job candidates who have been

indiscreet, who have posted inappropriate photos, or sent provocative tweets may find that good job opportunities are passing them by.

Some human resources (HR) specialists and consultants also contend that this monitoring of social media should continue even after a worker has been hired. Advocates of such monitoring point to many examples of employees posting inappropriate material, such as private or confidential information. Some hospital employees, for example, have been discovered discussing the sensitive details of a patient's medical history on their Facebook pages in direct violation of HIPAA. Others cite examples of how employees use Twitter or Facebook to put the company they work for in a bad light by making harmful and pejorative statements, often full of hyperbole. According to Nancy Flynn, "Strict monitoring allows employers to spot potential problems early [and] get the information offline as quickly as possible."[68]

These consultants, therefore, argue that companies should monitor the social media sites of both their prospective and current

employees. There are many benefits of such monitoring both for employers and for employees, such as a tradeoff of privacy for the guarantee of greater job security. Other HR professionals disagree with this policy, even if the trend among younger workers is to be more obliging. Cary Cooper, distinguished professor of organizational psychology and health at Lancaster University, regards this monitoring as "a plain case of trying to find out what employees are doing and thinking—clearly an intrusion into their private life. I see no HR justification for it whatsoever."[69]

Questions

1. Where do you stand on the issue of social media monitoring by employers? What should be the scope of such monitoring? Do you agree with Mr. Cooper's claim that there is no justification for this activity?
2. Do you agree with the research suggesting this monitoring will intensify in the future?

REFERENCES

1. Shoshana Zuboff, *The Age of Surveillance Capitalism* (New York: Hachette Book Group, 2019), 81; see also 7–9 and 79–80.
2. Louis Brandeis and Samuel Warren, “The Right to Privacy,” *Harvard Law Review* 4 (1890): 1890.
3. Ruth Gavison, “Privacy and the Limits of the Law,” *The Yale Law Journal* 89 (1984): 421.
4. Christine Borgman, “New Models of Privacy for the University,” in *Privacy in the Modern Age*, eds. Marc Rotenberg, Julia Horwitz, and Jeramie Scott (New York: New Press, 2015), 34–37. See also Charles Fried, “Privacy,” in *Philosophical Dimensions of Privacy*, ed. Ferdinand Schoeman (New York: Cambridge University Press, 1984).
5. *United States v. Reporters Comm*. 489 U.S. 749 (1989).
6. Herman Tavani and Jim Moor, “Privacy Protection, Control of Information, and Privacy-Enhancing Technologies,” *Computers and Society* 31 (2003): 6–11.
7. Jim Moor, “Toward a Theory of Privacy for the Information Age,” in *Readings in*

Cyberethics, 2nd ed., eds. Richard Spinello and Herman Tavani (Sudbury, MA: Jones and Bartlett Publishers, 2004), 407–17.

8. For a lucid and extended account of the Moor/Tavani model, see Herman Tavani, "Philosophical Theories of Privacy: Implications for an Adequate Online Privacy Policy," *Metaphilosophy* 38, no. 1 (2007): 1–22.

9. John Finnis, "Liberalism and Natural Law Theory," *Mercer Law Review* 45 (1994): 687.

10. Julie Cohen, "Between Truth and Power," in *Information, Freedom and Property*, ed. M. Hildebrandt (New York: Routledge, 2016), 62–63. See also Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review* 57, no. 6 (2010): 1701–77.

11. James Reiman, "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future," *Santa Clara Computer and High Technology Law Journal* 11 (1996): 27.

12. Richard Wassestrom, "Privacy: Some Arguments and Assumptions," in *Philosophical Dimensions of Privacy*, ed. Ferdinand Schoeman (New York: Cambridge University Press, 1984), 328.

13. Zuboff, *Age of Surveillance Capitalism*, 521.
14. See Michael Tobby, “How to Protect Your Personal Information,” *The Wall Street Journal*, January 29, 2007, R1, R3.
15. Beth Givens, “Public Records on the Internet: The Privacy Dilemma” (Paper presented at Computers, Freedom, and Privacy Conference, San Francisco, CA, April 19, 2002).
16. Kevin Delaney, “Firm Mines Offline Data,” *The Wall Street Journal*, October 17, 2007, B1.
17. Solon Barocas and Helen Wissenbaun, “Big Data’s End Run around Anonymity and Consent,” in *Privacy, Big Data, and the Public Good*, ed. Julia Lane (New York: Cambridge University Press, 2014), 46.
18. Sam Schechner, “Apps Stop Sharing Data with Facebook after Report,” *Wall Street Journal*, February 25, 2019, B1–2. See also Elizabeth Dwoskin, “Data Privacy,” *The Wall Street Journal*, April 20, 2015, R6.
19. Douglas MacMillan, Sarah Krouse, and Keach Hagey, “Yahoo, Bucking Industry, Scans Emails for Data to Sell,” *Wall Street Journal*, August 29, 2018, A1, A10.

20. Albert Borgmann, *Crossing the Postmodern Divide* (Chicago, IL: University of Chicago Press, 1992), 2.

21. Natalia Drozdiak, “Facebook Fined by French Watchdog,” *Wall Street Journal*, May 17, 2017, B4.

22. Jamie Condliffe, “Can Facebook Profit from Privacy,” *New York Times*, March 11, 2019, B3.

23. Eduardo Porter, “The Facebook Fallacy: Privacy Is Up to You,” *New York Times*, April 25, 2018, B1, B4. See also Zuboff, 187.

24. William O. Douglas, Dissenting Statement, *Warden v. Hyden* 387 U.S. 294 (1967). See also Zuboff, *Age of Surveillance Capitalism*, 47–48, 90 and Judith Wagner DeCew, *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca, NY: Cornell University Press, 1997), 64.

25. Immanuel Kant, *Grounding for the Metaphysic of Morals* (Indianapolis, IN: Hacket Publishing Company, 1981), 47.

26. Jeffrey Rosen, *The Unwanted Gaze* (New York: Random House, 2000), 166.

27. Elizabeth Wasserman, “Save the Children,” *The Industry Standard*, August 28, 2000, 110.

28. To *opt in* is to accept some condition such as the sale of one's personal data ahead of time.
29. Eileen Colkin, "Privacy Law Requires Hard Work," *InformationWeek*, August 20, 2001, 54.
30. Helen Nissenbaum, *Privacy in Context* (Stanford, CA: Stanford University Press, 2012), 115–21.
31. Richard Spinello and Herman Tavani, "Introduction to Chapter Four: Privacy in Cyberspace," in *Readings in Cyberethics*, 2nd ed., eds. Richard Spinello and Herman Tavani (Sudbury, MA: Jones and Bartlett Publishers, 2001), 339–48.
32. Victor Mayer-Schonberger, "Generational Development of Data Protection in Europe," in *Technology and Privacy: The New Landscape*, eds. Philip Agre and Marc Rotenberg (Cambridge, MA: The MIT Press, 1997), 219–42.
33. Ibid.
34. European Parliament and the Council of the European Union, 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *Official Journal of the European Union* L 281 (1995).

35. Julian DeGroot, “What Is the GDRP?” ***DigitalGuardian.Com***, May 15, 2019.

36. DeGroot, “What Is the GDRP?,” See also Natasha Singer, “Facebook Curbs Coming (Thanks to E.U.),” *New York Times*, April 9, 2018, B5 and Nick Kostov and Sam Schechner, “GDPR Is a Boon to Tech Giants,” *Wall Street Journal*, June 18, 2019, R8.

37. Helen Nissenbaum, *Privacy in Context* (Stanford, CA: Stanford University Press, 2012), 216. See also Helen Nissenbaum, “Respect for Privacy as a Benchmark for Privacy Online,” in *Privacy, Security and Accountability,* ed. Adam Moore (Lanham, MD: Rowman & Littlefield, 2016), 57.

38. Nissenbaum, “Respect for Privacy as a Benchmark for Privacy Online,” 46-50.

39. Julie Cohen, *Configuring the Networked Self* (New Haven, CT: Yale University Press, 2012), 252.

40. Brian Turner, “Best Employee Monitoring Systems of 2019,” *Techradar.pro*, May 4, 2019, **https://www.techradar.com/best/best-employee-monitoring-software**

41. Nicole Hong, “Lawsuit Tests Limits of Bosses’ Snooping,” *Wall Street Journal*, September

10, 2018, A3.

42. Graham Sewell and James Barker, “Neither Good nor Bad, but Dangerous: Surveillance as an Ethical Paradox,” *Ethics and Information Technology* 3, no. 3 (2001): 194.

43. Ibid.

44. Electronic Communications Privacy Act 18 U.S. C. §2511 (2)(a).

45. Lawrence Rothstein, “Privacy or Dignity?: Electronic Monitoring in the Workplace,” *New York Law School Journal of International and Comparative Law* 19 (2000): 379.

46. Ibid., 385.

47. Sewell Chan, “Europe Limits Access to Workers’ Email,” *New York Times*, September 6, 2017, B1, B3.

48. “Workplace Privacy and Employee Monitoring,” Privacy Rights Clearinghouse, May 25, 2019, **https://www.privacyrights.org/workplace-privacy-and-employee-monitoring**.

49. *Falmouth Firefighters Union v. Town of Falmouth* No. 09-517 (S.Ct. Ma, 2012). See also *Smyth v. Pillsbury Co.* 914 F. Supp 97 (E.D. Pa 1996).

50. Moor, “Theory of Privacy,” 29.

51. Joseph DesJardins and Ronald Duska, “Drug Testing in Employment,” in *Ethics at Work*, ed. William Shaw (New York: Oxford University Press, 2013), 100–111.
52. Michael Alistair Poon, “The Right to Be Forgotten: One Year Later,” *The Bolt*, (Stanford Law Review) April 5, 2015.
53. “Drawing the Line,” *The Economist*, October 4, 2014, 67–68.
54. Poon, “The Right to Be Forgotten: One Year Later.”
55. Mark Scott, “Google Touring Europe on ‘Right to Be Forgotten,’” *The New York Times*, September 10, 2014, B7.
56. Alistair Barr, “Google Panel: Limit Right to Be Forgotten,” *The Wall Street Journal*, February 7, 2015, B4.
57. Evan Osnos, “Ghost in the Machine,” *The New Yorker*, September 17, 2018, 34.
58. Victor Luckerson, “Here’s How Your Facebook News Feed Actually Works, *Time*, July 9, 2015, 26. See also Zuboff, *Age of Surveillance Capitalism*, 458–59.
59. Zuboff, *Age of Surveillance Capitalism*, 47–48 and 91–92.
60. Porter, “Facebook Fallacy,” B4.
61. Osnos, “Ghost in the Machine,” 39.

62. Sandy Parakilas, “Facebook Won’t Protect Your Privacy,” *New York Times*, November 20, 2017, A23. See also Osnos, “Ghost in the Machine,” 38.

63. Zuboff, *Age of Surveillance Capitalism*, 457.

64. Natash Singer and Sapna Maheshwari, “ Europe Asks: Is Facebook Vacuuming Up Too Much Data From Users,” *New York Times*, April 25, 2018, B4. See also Drozdiak, “Facebook Fined by French Watchdog,” and Zuboff, *Age of Surveillance Capitalism*, 161.

65. Mike Isaac, “After Zuckerberg’s Invitation to Regulate Facebook, A Closer Look,” *New York Times*, April 1, 2019, B3.

66. “Workers of the World, Log In,” *The Economist*, August 16, 2014, 51–53.

67. Helen Pidd, “Social Media Monitoring by Employers Predicted to Rise,” *The Guardian*, August 17, 2014, 6.

68. Nancy Flynn, “Keeping an Eye on Employees Helps Companies Protect Themselves,” *The Wall Street Journal*, May 12, 2014, R1.

69. Pidd, “Social Media Monitoring by Employers Predicted to Rise.”

ADDITIONAL RESOURCES

Agre, Philip, and Marc Rotenberg, eds. *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT Press, 1997.

Bennett, Colin. "Cookies, Web Bugs, Webcams, and Cue Cats: Patterns of Surveillance on the World Wide Web." *Ethics and Information Technology* 3, no. 3 (2001): 197–210.

Brin, William. *The Transparent Society*. Reading, MA: Addison-Wesley, 1998.

Capurro, Rafael. "Privacy: An Intercultural Perspective." *Ethics and Information Technology* 7, no. 1 (2005): 37–47.

Clark, Ross. *The Road to Big Brother*. New York: Encounter, 2009.

Cohen, Julie. *Configuring the Networked Self*. New Haven, CT: Yale University Press, 2012.

DeCew, Judith. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology.* Ithaca, NY: Cornell University Press, 1997.

Floridi, Luciano. "The Ontological Interpretation of Informational Privacy." *Ethics and Information Technology* 7, no. 4 (2005): 185–200.

Gavison, Ruth. “Privacy and the Limits of the Law.” *Yale Law Journal* 89 (1984): 421.

Kirkpatrick, David. *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*. New York: Simon & Schuster, 2011.

Landau, Susan. *Surveillance or Security.* Cambridge, MA: MIT Press, 2013.

Lane, Julia, ed. *Privacy, Big Data, and the Public Good*. New York: Cambridge University Press, 2014.

Moor, James. “Towards a Theory of Privacy in the Information Age.” *Computers and Society*, 27 no. 3 (1997) 27–32.

Nissenbaum, Helen. *Privacy in Context*. Stanford, CA: Stanford University Press, 2012.

Rotenberg, Marc, Julia Horwitz, and Jeramie Scott, eds. *Privacy in the Modern Age*. New York: New Press, 2015.

Rothstein, Lawrence. “Privacy or Dignity?: Electronic Monitoring in the Workplace,” *New York Law School Journal of International and Comparative Law* 19 (2000): 379.

Smith, Robert Ellis. *Ben Franklin’s Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*. Providence, RI: Sheridan Books, 2000.

Solove, Daniel. *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press, 2005.

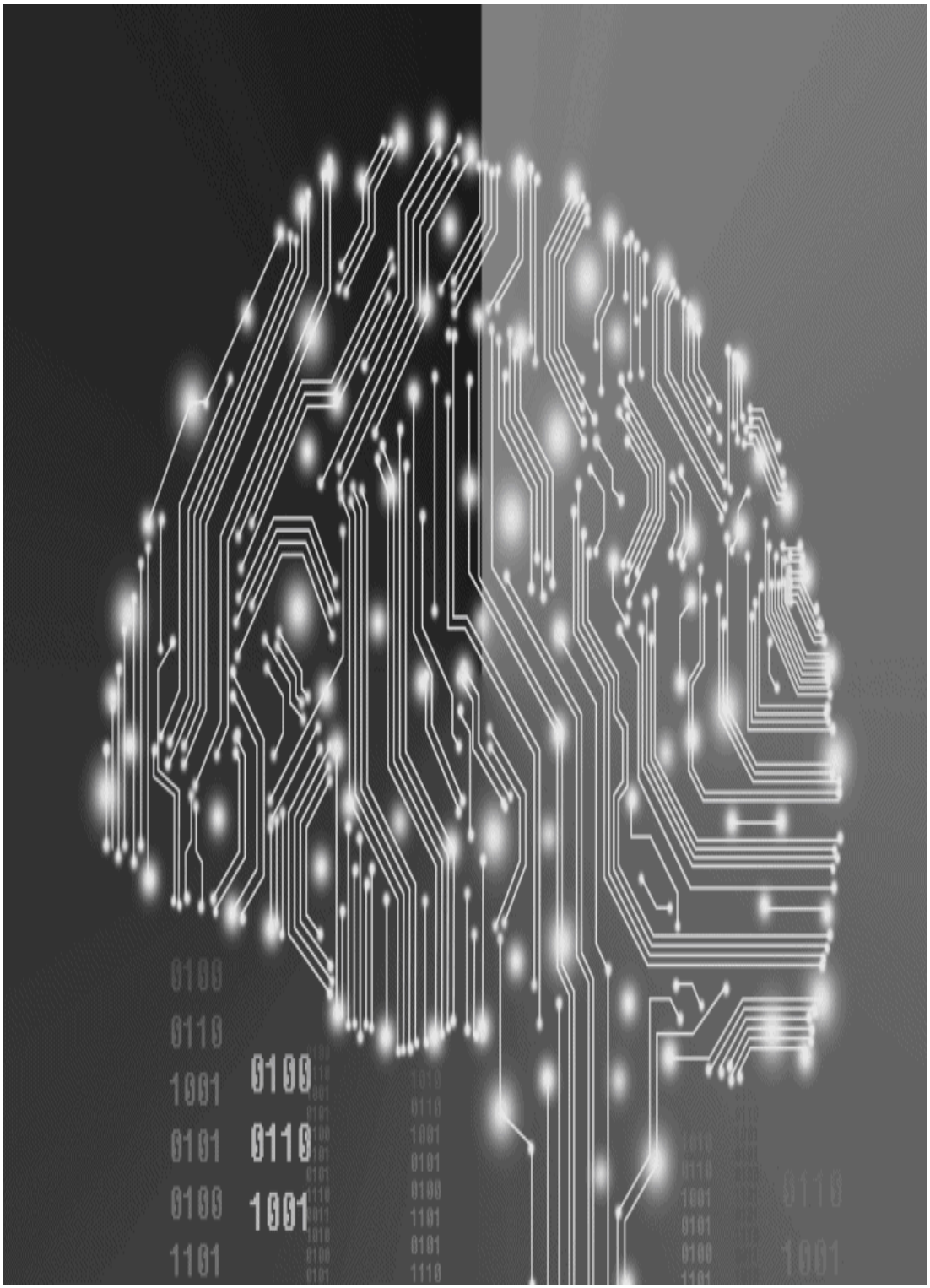
Solove, Daniel. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.

Spinello, Richard. “E-Mail and Panoptic Power in the Workplace.” In *Perspectives on Business Ethics*, edited by Laura Hartman, 236–257. New York: McGraw-Hill, 2002.

Tavani, Herman. “Philosophical Theories of Privacy.” *Metaphilosophy* 38, no. 1 (2007): 1–22.

Westin, Alan. *Privacy and Freedom*. New York: Atheneum, 1967.

Zuboff, Shoshana. *The Age of Surveillance Capitalism*. New York: Hachette Book Group, 2019.



CHAPTER 6

Securing the Digital Infrastructure

Vulnerabilities of Networked Technologies

The attack on Sony Pictures Entertainment could have been a plot for one of its movies. A hacker group known as Guardians of Peace (or #Gop) breached Sony's poorly protected computer system. The hackers leaked internal Sony documents, along with the social security numbers of 47,000 current and former employees. They also posted controversial and embarrassing emails among Sony executives. The hackers even distributed pirated copies of several upcoming movies. What was the reason for this damaging intrusion? The group was protesting the release of *The Interview*, a satirical film that mocked North Korea's leader Kim Jong-un. The #Gop demanded that Sony stop showing this "movie of terrorism" or face "dire future consequences."[1]

The Sony attack has not been the only high-profile data breach where corporate networks have been penetrated. Major breaches have occurred at Target, Home Depot, Uber, Equifax, Facebook, and Marriott International. The Marriott breach for its Starwood properties, one of the largest in history, exposed the personal data of up to 500 million guests. The consumer data stolen or compromised included passport numbers, travel

information details, and credit card numbers. Passport information could be of considerable value for spy agencies who wish to compile dossiers on corporate executives and government officials.[2]

Despite the use of firewalls, security scanners, intrusion prevention and detection products, and sophisticated encryption, corporate and government websites have been a major target for hackers. Individual users are also at risk. Aside from the theft of data (such as credit card information), a common menace is online identity theft or phishing. In a ***phishing*** *attack* emails are sent to users that appear to come from a bank or an online retailer. The emails look authentic, often complete with accurate-looking logos, and they direct users to a website where they are asked to enter sensitive information such as passwords, bank account numbers, or credit card information. The information is used to pilfer money from those accounts or to create bogus credit cards. *Spear phishing* occurs when phishers pursue a specific person. They might identify a person of interest on a social network, who becomes targeted for identity theft. Phishing has also spread out beyond email to text messages, WhatsApp chats, and search engines.[3]

Thanks to its open architecture, the internet is particularly susceptible to various forms of malware or malicious software. A virus, for example, is a self-replicating program usually hidden away in another host program or file that can disrupt a computer system. The biggest fear is that terrorists will use malware to interfere with vital services controlled by computer technology. For example, a disgruntled employee reconfigured the computerized control system at a water treatment plant in Australia, which caused the release of 200,000 gallons of sewage into parks and rivers.[4]

Worms are also malicious pieces of code, which differ from viruses because they can run independently. They can travel automatically from one computer to another across network connections. The famous Stuxnet worm was aimed at undermining Iran's nuclear research program. One other popular form of "malware" is the *Trojan horse*, used to insert corrupt information into a program. There has been a rise in the use of backdoor Trojan horses that are sent covertly through email. According to one description, "You run the program and that opens a door, which people on the outside can use to steal your passwords, destroy files, and so on."[5]

One of the first cases that brought the public's attention to the internet's vulnerability was the "Internet Worm" developed by Robert Morris, a student at Cornell University. In November 1988, Morris released this worm, a concise, self-replicating C program, from Cornell's host computer system so it would quickly spread to other systems on the internet. This worm's progress was facilitated by a fatal security hole in the UNIX operating system software of the infected machines. Once these computers were invaded, the program reproduced itself incessantly, consuming large volumes of memory. It did not modify system files or destroy any information, but the performance of systems infected by the worm deteriorated rapidly, causing many of them to crash. The Computer Systems Research Group at Berkeley developed a program to destroy the worm and prevent its recurrence. The final toll: 2,500 computers infected in some way and a clean-up cost of over $1 million.

Fortunately, incidents on this scale are not an everyday occurrence, but in the many years since this event occurred, there has been insufficient progress made in securing the electronic frontier. In addition, many more connected devices are being added to the global network as the Internet of Things (IoT) magnifies its reach. These

products, such as home appliances, will expand the “attack surface” or the means through which hackers can exploit computer systems. A vulnerability in one device can affect all other products networked with it.[6]

Yet organizations, which now realize the crucial importance of cybersecurity, also discover that implementing strong security measures is a complex challenge. The fundamental problem is familiar: the internet’s underlying architecture is radically open, designed to share information, not to keep it from others. It is possible to develop an adequate level of security with an acceptable degree of risk, but this requires an investment of time and money that many government agencies and private corporations have been reluctant to make.

Computer system security is a massive topic, and we cannot possibly do it justice here. In this chapter, we focus on several issues that are related to the main themes of this text. We first examine the topic of cybercrime: how it is defined, what sorts of activities can be categorized as a cybercrime, and whether or not antipiracy technologies are an appropriate antidote. We then review the interrelated issues of trespass, hackers, and hacktivism.

The next topic concentrates on the most effective security measures that should be adopted to protect electronic commerce and online communications against unauthorized access and other abuses. This discussion includes some treatment of digital certificates and other protocols that are designed to safeguard the integrity of information being transmitted to and from websites.

Finally, we devote some attention to the matter of encryption and the public policy debate it has reignited in the United States. One way to achieve tight information security is by encrypting communications. This makes the data undecipherable to anyone who does not have a key to the encrypted data. But the U.S. government has always sought some leverage over this technology because it has the potential to become a dangerous weapon in the hands of criminals and terrorists. The issue has been given new life thanks to the use of strong encryption architectures on iPhones and other mobile devices.

Our purpose here is not to provide an exhaustive account of the internet’s security deficiencies or a primer about proper preventive security measures. Rather, it is to explore several ethical dimensions of this important problem, illustrate how the critical

goal of information security can sometimes collide with other worthy objectives (such as the preservation of privacy rights), and ponder how these competing objectives can be effectively balanced.

Cybercrime

It is no secret that the internet has become a breeding ground for certain forms of cybercrime; there are unfortunately many criminals lurking in the virtual world of cyberspace. Cybercrime is rather nebulous, so some clarification of its precise meaning is essential. We define *cybercrime* as a special category of criminal acts that are typically executed through the utilization of computer and network technologies. Cybercrime then includes three basic categories: (1) software piracy, (2) computer sabotage, and (3) electronic break-ins.[7] What all of these crimes have in common is that they require the use of a computer, which is the target and/or the tool of the crime. Obviously these crimes can be committed with an isolated, unconnected computer system, but the locus of most of these crimes today is the network; connectivity enables creative variations of rogue activities like piracy and sabotage.

Software piracy involves the unauthorized duplication of proprietary software and the distribution or making available of those copies over the network. The unauthorized copying and distribution of proprietary operating system software, applications software programs, or MP3

files fall under this category. The No Electronic Theft Act of 1997 forbids the willful infringement of a copyright for purposes of commercial advantage or for some financial gain. This and other laws protecting copyrighted material are often flouted by those who subscribe to the philosophy that "content on the Internet wants to be free." The copying of music and video software files has become rampant. What the music industry sometimes regards as piracy, websites like Napster saw as fair use, as discussed in **Chapter 4**. Despite the demise of Napster, other music-sharing software such as LimeWire have emerged to take its place. Some notorious websites such as Megaupload, run by "Mr. Dotcom," encourage users to share pirated content. In its defense, Megaupload claimed, "We're not pirates—we only provide 'shipping services' to pirates."[8]

Computer sabotage implies interference with computer systems, such as the disruption of operations by means of malware in the form of a virus, worm, logic bomb, or Trojan horse that infects a computer system. According to Tavani, computer sabotage also involves using computer technology to "destroy data resident in a computer or damage a computer system's resources."[9] Malware is usually spread through websites to which unwary users are directed through email

messages or links posted on social networking sites. The purpose is usually not to destroy data but to steal passwords and other data so that computers can be commandeered by hackers. These machines linked to others around the world create a “botnet,” which can be used to transmit spam, spread more malware, or initiate a denial-of-service (DoS) attack. A study conducted by the *Economist* found that in a 24-hour period there were over 100 million infected machines throughout the world.[10]

The DoS attack, usually enabled through malware, assaults a website with mock requests from multiple computers until the server crashes and service is disrupted. Thanks to a botnet, the software to send the mock requests can be easily and surreptitiously implanted in computers all over the world. When signaled, those personal computers (PCs) spring into action and begin bombarding a chosen website with requests unbeknownst to the PC’s owner. There have been a number of high-profile attacks on websites such as Yahoo and eBay, and there is evidence that the DoS remains a strong weapon in the hacker’s arsenal.

Malware is not always used merely as a means to gain backdoor entrance to a computer system for DoS attacks. One of the most alarming and

potentially destructive worms in recent memory was Stuxnet, which infected a number of industrial control systems throughout the world. Stuxnet infects PCs through the USB drive and then seeks Siemens software controlling industrial components. If that software is not found, it searches every computer in the local area network connecting PCs and other computer systems. Once Stuxnet locates the Siemens software, it reprograms the logic controls and sends new instructions to industrial machines. Stuxnet has shown up in many countries, including China and India, though the primary target is Iran, leading many to conclude that its primary purpose was to disrupt Iran's nuclear facilities.[11]

Another form of sabotage that has grown in popularity is ***ransomware***. By means of ransomware cybercriminals encrypt a victim's computer files and hold them for ransom. Ransomware usually originates with an email message that contains an attachment or link to a website that surreptitiously installs the software. The software encrypts files on a user's computer, usually targeting Microsoft Word documents. It then transmits a message indicating where to send the payment—when the payment is received, the files are decrypted. Thus, ransomware is a combination of two types of malware: the worm

designed to spread from one computer to another and the encrypting software that is delivered by that worm. One of the biggest ransomware attacks was perpetrated through a piece of malicious software known as WannaCry. This program spread across the internet, initially in Britain and Spain, and affected 230,000 computers within 48 hours. The main targets of this brazen cyberattack were big companies and government agencies. It attacked machines running Microsoft Windows that did not have up-to-date security patches.[12]

Should organizations make these ransomware payments? This disputed ethical question is not easy to resolve. Making ransom payments will probably embolden the culprits and lead to more ransomware attacks in the future. Hence it may be difficult to justify payments on utilitarian grounds. Also relevant is the agent behind the ransom demand and likely purpose for which the money will be used. It would be morally unreasonable to make ransom payments that one knows are earmarked for violent or terrorist causes. On the other hand, both private and public sector organizations have a duty to ensure the integrity and utility of their data and to avoid any disruption of vital services that might occur if that data is locked by outsiders.

The final category, electronic break-ins and unauthorized access, raises some complex issues and is covered later in this chapter. There are clear-cut cases of unwanted intrusion, and the most serious form is cyber espionage. In one provocative incident, computer spies hacked into the Pentagon's $300 billion Joint Strike Fighter project to glean some details about this new weapon. The spies were able to download relevant data about this jet fighter, though they couldn't access the most sensitive material.[13]

Not included in this strict definition of cybercrime are crimes that are facilitated through the use of computer and network technologies. These crimes do not require computer technology; that is, the use of a computer to commit the crime is not necessary, but it may aid the commission of that crime. In most cases these crimes were going on long before the arrival of networked technologies. One might include in this category stalking, theft (including fraud, swindling, or embezzlement), and the illicit distribution of proprietary information (such as trade secrets). However, computer and network technology often make some of these crimes easier to commit. Therefore, activities such as data theft or phishing, which are greatly facilitated by cyber technology, constitute a

secondary form of cybercrime. We might also refer to them as computer-related crimes.

For example, the scam known as *phishing* would not fall into the category of direct cybercrime, as we have defined it. Someone who wishes to perpetrate a fraud could get bank account numbers by rummaging through trash cans outside the local bank as well as from a fake website where users are asked to divulge their account numbers. People have always been duped into handing over vital financial information to scammers, but digital technology facilitates these schemes and makes them possible on a larger scale.

Antipiracy Architectures

There are various technological tools and mechanisms to protect networked systems and proprietary data. Digital rights architectures (DRMs), for example, make sure content is secured by encryption or other controls, and they contain instructions outlining which uses to permit. Embedded in iTunes is a DRM (called FairPlay), which limits the distribution of iTunes music to authorized devices. Apple's success with iTunes has restored confidence that digital content can be successfully distributed through traditional market mechanisms. It is instructive to revisit the topic of DRMs in light of the discussion in this chapter on the crime of piracy.

Laws have been ineffectual in combating software piracy, and many users have few qualms about bootlegging music and videos in a digital format. The entertainment and content industries have become increasingly frustrated with the constant pilfering of digital music and videos. As a result, they have turned to computer manufacturers and software developers for code that is more efficient in stopping piracy. In their view, Silicon Valley has not done enough to address the piracy problem. In testimony before Congress, the CEO of Disney

even accused companies such as Apple, Dell, and Microsoft of failing to develop secure systems because piracy actually helped them sell more computers. He cited Apple's slogan "Rip, Mix, Burn," as a signal to consumers that a Macintosh computer facilitates theft.

The main antipiracy strategy of the entertainment industry has been the incorporation of a copy-protection mechanism not only into PCs but also into DVD players and other digital media devices. The industry also puts pressure on major digital platforms to block access to website domains that host infringing content. The entertainment and content industries have been pushing for stricter laws, hoping that they will more effectively prevent privacy. Those laws could support the code that ensures the tight enclosure of content and provides technical protection against copying.

But new antipiracy laws may not be necessary, since these trusted systems are quite proficient. Also, direct exclusion of infringing content has become normative among major internet players. Companies like Twitter and YouTube that host user-provided content rely on automated filtering technology to restrict the posting of any infringing content. Google has announced that it will remove entirely from search results websites that ignore multiple takedown notices. Critics of these

developments worry about the consequences of copyright law being enforced by private actors, especially given the opacity of Google's algorithms. These programs are undoubtedly more effective than the law they imitate, but they accomplish by private and nontransparent means what Congress and the content industries have been unable to do.[14]

Arguably, from a moral perspective, the use of antipiracy architectures such as DRM and takedown algorithms is not objectionable. On the other hand, prudence dictates that these systems should be modeled as much as possible on current copyright law. If consumer rights and interests along with broader values recognized in the law like fair use and first sale are not ignored, it may be possible to achieve security through code without causing collateral damage. But overly aggressive copyright enforcement effected by private parties could easily work to the detriment of social welfare by threatening fundamental rights of speech and privacy and impeding scientific and cultural progress.[15]

Trespass, Hackers, and Hacktivism

Those who break into computer systems to steal data or plant worms are typically referred to as hackers. Initially, the word “hacker” had a fairly benign connotation. A hacker was someone who simply disregarded the rules, along with online property boundaries. Recreational hackers thrived on breaking into supposedly “secure” systems to demonstrate their superior skills. According to Dorothy Denning, the hacker ethic is predicated on a basic principle: “Access to computers—and anything which might teach you something about the way the world works—should be unlimited and total.”[16]

These pesky “white hat” hackers continue to break into systems for fun and curiosity or to expose a system’s vulnerabilities. But many hackers these days are malicious. They hack into vulnerable systems to deface a website or to steal sensitive data for monetary gains. There are also hackers who combine hacking and political activism, the so-called “hacktivist.” Before we consider hacktivism, let us briefly discuss the problems of recreational hacking and electronic trespass.[17]

Many people do not see an exact parallel between trespassing on a computer system and physical

trespass. They regard the former as more abstract, rationalizing that networked computer system resources are something to be “borrowed” and returned with no harm done. Is unauthorized access the same as physical trespass despite the fact that the internet’s architecture is such an open and unstructured environment?

The 1986 Computer Fraud and Abuse Act (CFAA), which was last amended in late 1996, is the primary legal vehicle for dealing with trespass. The provisions of this act protect the confidentiality of proprietary information and make it a crime to “knowingly access a computer without or in excess of authority to obtain classified information.” The statute also makes it a crime to access any “protected computer” without authorization and, as a result of such access, to defraud victims of property or to recklessly cause damage. Thanks to the 1996 amendment, protected computers include those used by the government, financial institutions, or any business engaged in interstate or international commerce, or anyone involved in interstate communications. The category of “protected computer,” therefore, includes virtually any computer connected to the internet. According to the CFAA, trespass is a federal crime if one does so to pilfer classified information, to perpetrate fraud, or to cause damage (e.g., to

destroy files or disable an operating system).[18] It is also a federal crime to cause the transmission of a program or piece of code (such as a virus) that intentionally causes damage to a protected computer. In addition, the CFAA "prohibits unauthorized access that causes damage regardless of whether the damage was 'recklessly caused.'"[19]

All U.S. states, with the exception of Vermont, have also enacted their own computer crime statutes that in some cases go well beyond the scope of the CFAA. Specifically, most state laws make unauthorized use of computers a crime even if the motive is just curiosity and one is merely snooping around. There are harsher penalties for computer trespass where the entry has occurred to commit another crime such as the theft of material.

Some have argued that law enforcement officials should not be taking such a hard line against purely recreational hacking, that is, incidents of trespassing that do not involve damage to property or theft of data. There have been numerous arguments put forth to defend break-ins by hackers, especially when there is no deliberate destruction of property. Among these arguments we find the following: break-ins actually serve a valuable purpose because they uncover security

flaws that would otherwise go unnoticed and the intruder is probably only utilizing idle resources so there is really no cost for the victim. There is also what Eugene Spafford calls the student hacker argument: “Some trespassers claim that they are doing no harm and changing nothing—they are simply learning about how computer systems operate.”[20] Still others might say that a little digital graffiti inscribed on a website by a hacker is merely a prank and should be treated accordingly.

On the surface, it might appear that some of these arguments are defensible and that there is little or no harm to most forms of electronic intrusion. If, for example, a hacker is able to penetrate a secure environment and search through a few programs but does no damage, where is the harm? This might be analogous to walking through someone’s property while leaving everything perfectly intact. Thus, one could argue that unauthorized access that leaves the environment undisturbed is only a minor ethical transgression and not worth much of a fuss. And digital graffiti are not much worse; it can be cleaned up more easily than the graffiti that comes from spray paint.

The strongest restraints on this deviant behavior are code and the law or some fusion of the two. There are numerous technologies designed to deter hackers, along with laws like the CFAA that

prescribe strict punishment for electronic trespassing. On the other hand, social norms are ambivalent, since there is still some cultural acceptance of hacking in cyberspace. Society sends mixed signals about hackers who are seen as rogues and villains but also as modern-day Robin Hoods and adventurers, who deserve some credit for their skill and ingenuity.

This ambivalence dissipates, however, when ethical norms are applied to hacking. To begin with, it is generally recognized that it is simply wrong to trespass even if no direct damage is caused. When one trespasses, one violates respect for property rights, which is an important ethical and social value. Property rights buttress the moral good of autonomy because they allow individuals to control what they own, which is essential for their commercial and personal well-being. Breaking into a private corporate headquarters after hours just to look around the lobby is still trespassing, even if one does not pilfer any files or cause any damage. There is no basis to treat a hacker who breaks into a secured computer site only to look around any differently. Individuals should not go where they do not belong, either in real space or in cyberspace. This is a fundamental rule of law and basic tenet of morality.

Furthermore, the hacker may intrude into a system and not intend to do any harm, but he or she may inadvertently cause damage to a file or software program. The more complex the system, the more likely the occurrence of accidental damage. In addition, unauthorized use of a computer system wastes the victim's valuable computer resources, which does amount to a more tangible form of theft. Moreover, even if there is no malicious intent or destruction of webpages, a trespasser's activities can still be disruptive and costly. Any unwarranted intrusion must be inspected by system administrators, who must spend time verifying and checking their network systems and software to make sure that no damage has been done. Thus, as Spafford and others have illustrated, most of the arguments that justify the actions of nonmalicious hackers are weak and difficult to defend.

Finally, is unauthorized access or hacking *ever* morally permissible? We must obviously conclude that malicious breaches where the intruder intends to cause harm or steal data for profit are morally wrong. But what about situations where the intruder's intentions appear to be noble? Sometimes the motive behind hacking is strictly political—an action taken as a protest or to advocate for social change. An attack or

unauthorized intrusion on a government website might be regarded as a form of civil disobedience. In these cases, digital intrusion, its defenders say, is not different from a physical “sit-in” or protest on government property that may be demanded by exigent political circumstances. This phenomenon has become known as hacktivism, which is defined as “the (sometimes) clandestine use of computer hacking to help advance political causes.”[21] The term can be traced to Cult of the Dead Cow, a hacker group located in Lubbock Texas. This group argued that access to online information was a basic right, and their early hacking efforts involved several dubious projects to combat internet censorship.[22]

Hacktivists argue that it is morally acceptable to intrude on corporate or government networks to protest unjust laws or harmful policies. In their view, a DoS attack directed at the World Trade Organization’s (WTO) website for its alleged support of dangerous globalization policies would be a valid form of online protest. There is no destruction of property, nor any real lasting damage to the WTO site. Hacktivists not only invade websites as a protest, but also develop software systems that allow users to flout certain restrictions on online activities.

The merits and legitimate parameters of hacktivism are surely debatable, but in some cases it appears to be a morally valid means of resisting government censorship or oppression. For example, a Chinese hacker named Bill Xia developed Freegate, a rogue software program that connects companies in China to U.S. servers so Chinese citizens can look at content forbidden by the Chinese government. Xia calls this software the “red pill,” a reference to the drug in the movie *Matrix* that catapults captives of a totalitarian government into reality. In this context, Xia is helping Chinese citizens circumvent a presumptively unjust censorship regime, so his actions are arguably a noble form of civil disobedience.[23]

Other cases, however, are far more controversial. WikiLeaks, headed by Julian Assange, purports to be a place where whistleblowers can disclose and disseminate information that usually exposes wrongdoing or questionable activities. WikiLeaks algorithms safeguard the origin of that information so it is not traceable. When WikiLeaks published tens of thousands of secret U.S. military and foreign policy documents, some businesses, including Visa and PayPal, cut their ties with this self-described “media organization.” Assange, who is described as an “antiestablishment computer

hacker," got quick support from hacker groups such as Anonymous, which targeted PayPal and slowed down payment processing on its website. No real damage was done, but PayPal got the message, thanks to this "digital protest." But, is it morally permissible to punish these companies for their convictions and to cause some harm to the innocent third parties inconvenienced by this type of slow down? The situation is complicated by the fact that WikiLeaks' actions are morally questionable.[24]

Security Measures in Cyberspace

It is obvious from the number of massive data breaches and repeated security failures that many public and private organizations have been far too lax about digital security. Security experts claim that the reason for this is a lack of real liability and little sense of urgency. Some experts opine that it would take the equivalent of a “cyber-Pearl Harbor,” an attack that caused physical destruction and even some loss of life, to awaken countries to the vulnerabilities of networked computer systems.[25]

But what can be done to guard against these various threats, to safeguard the internet and make it a more secure environment? A sound security scheme should begin with protecting the perimeter, usually by means of a firewall.

The firewall is the first line of defense because it should prevent intruders from gaining access into the internal network. A firewall consists of hardware and/or software that is positioned between an organization’s internal network and the internet. Its goal is to insulate an organization’s private network from intrusions by trapping any external threat, such as a virus, before it can penetrate and damage an information system. The

simplest form of firewall is the packet filter, which relies on a piece of hardware known as a router to filter packets between the internal network and an outside connection such as the internet. It operates by examining the source address of each individual packet along with its destination address within the firewall. If something is suspicious or the source address is considered to be untrustworthy or dubious, it can refuse the packet's entry. According to Garfinkel and Spafford, "Ideally, firewalls are configured so that all connections to an internal network go through relatively few well-monitored locations."[26] The goal of the firewall is to allow legitimate interactions between computers inside and outside the organization while turning away unauthorized and potentially harmful interactions.

In the wake of costly DoS attacks, some companies began implementing specialized firewalls to handle DoS filtering. According to Yasin, "router-based filtering has emerged as one method of stemming DoS attacks, since most routers can filter incoming and outgoing packets."[27] But these firewalls are much more expensive than general-purpose firewalls, and they also tend to degrade performance.

Of course, a firewall is not always effective, and in those cases where a breach has occurred, an

intrusion prevention and detection system can be quite helpful. This software monitors the entire network to look for signs of an intrusion in process and it takes steps to stop the intrusion. In addition, these intrusion detection programs will indicate the details of a data breach that has already taken place so that remedial steps can be taken. Advanced systems also identify the precise location of security holes so they can be promptly repaired through security patches or other means.

Antivirus software is another critical element of any sound security architecture. This software is programmed to scan a computer system for malicious code and deletes that code once it has been found. This software works pretty well against known viruses, but new viruses evolve all the time and this requires the constant updating of antivirus programs. Even the more conservative estimates claim that there are about 300 new viruses introduced each month. For example, antivirus programs now screen for macro viruses, but they must be continually updated to detect new variations of these viruses.

Filtering systems can also be a helpful security mechanism. Software such as MIME sweeper can scan incoming mail for spam or for viruses while searching outgoing mail for sensitive corporate data that should not leave the confines of the

organization. This software may enhance security, but it also diminishes employee privacy, and the tradeoff needs to be carefully weighed.

A more complicated problem is securing information in motion, data travelling over this open network. The optimal way to secure these data is through ***encryption***, encoding the transmitted information so it can be read only by an authorized recipient with a proper key that decodes the information. Through the use of encryption, information can be protected against interception and tampering. Data encryption has its roots in the ancient science of *cryptography,* the use of ciphers or algorithms that allow someone to speak and to be understood through secret code. When a message is encrypted, it is translated from its original form or plain text into an encoded, unintelligible form called *cipher text*. *Decryption,* which is usually accomplished with a key, is the process of translating cipher text back into plain text.

The first encryption systems were symmetric; that is, the same key is used to encrypt and decrypt the data. This is sometimes referred to as a *single-key encryption* system. In a simple encoding pattern, the numbers 1 through 26 might represent the letters of the alphabet (1 = A, 2 = B, 3 = C, and so forth) so that the message 7–18–5–5–20–9–14–7–

19 means “greetings.” The key is the decoding pattern. For this method of encryption to work properly, both parties, the sender and receiver of the data, must have access to this key. The same key that scrambles the message is the one used to descramble it. The key itself then must be communicated and maintained in a secure fashion or it could be intercepted by a third party and fall into the wrong hands. Another disadvantage of private key cryptography is that if the key gets lost it will be impossible to decrypt the messages encrypted with this key.

Private or symmetric key encryption has been in widespread use since the 1960s. For many years, the most popular algorithm was the Data Encryption Standard (DES), which the federal government adopted as its standard in 1977. The DES was originally created by IBM researchers, but it was modified and fortified by the National Security Agency (NSA). In 2003, the Advanced Encryption Standard (AES) was approved by the U.S. government as a successor to DES. The AES is currently its default encryption algorithm for protecting classified information. The government’s endorsement of this technology has led to its extensive utilization in the private sector. AES has been implemented for many hardware

and software applications including Apple's iPhone.

Encryption keys are composed of bits of data that can have a value of 1 or 0. DES keys were originally 56 bits long, so there were 2^{56} possible values. In 1998 the Electronic Frontier Foundation demonstrated that it could break a DES key in about 2 days using a $200,000 computer system. Hence, to ensure full confidentiality, private and public sector organizations have turned to strong encryption, that is, at least 128-bit (2^{128} possible values) or greater algorithm, which is virtually unbreakable. 256-bit encryption is now the norm for most commercial applications.

The other popular encryption technique is ***public key encryption*** or the dual key system, considered to be one of the most critical innovations of this short network age. Data transmissions are even more secure using this method; even if one key is intercepted or stolen, it is impossible to derive the other key. With public key encryption, each party gets a pair of keys, one public and one private. The public key, which is usually kept in a directory or is posted on a website, is used to encrypt a message, and a secretive private key is used to decrypt the message. Messages encrypted with this public key can be decrypted only with the private key that is

known only to the recipient of the message. Public key cryptography also provides a secure means of authenticating the sender of an electronic communication. The sender signs the message with his or her private key and the recipient uses the sender's public key to unlock that signature. The two most popular public key systems are RSA (Rivets–Shamir–Adleman) and PGP (Pretty Good Privacy).

The obvious advantage of public key cryptography is greater security. The sender and receiver of the message do not have to exchange a secret private key before they begin to communicate. The bottom line, according to Michael Baum, "is that public-key encryption creates trusted commerce for all parties doing business."[28]

In practice, the Secure Sockets Layer (SSL) protocol is most often used in e-commerce transactions. SSL is used to encrypt data sent between web browsers and web servers. Thanks to SSL, data such as a credit card number can be exchanged through a secure conduit that prevents would-be intruders from seeing or tampering with those data. SSL also authenticates the server so that users know that they are at the website they intended to visit.

Why the need for protocols such as SSL? Consider what transpires in a typical online transaction. If someone decides to buy a book from an online bookstore, the person must electronically submit a credit card number along with some personal information to complete this transaction. There is a danger that the credit card number or password will be “sniffed” by hackers. *Sniffers* are automated programs used to seek out security lapses and intercept vulnerable communications traveling over a network. To avoid this, SSL relies on encryption so that data traveling between the customer’s web browser and the online bookstore cannot be sniffed out or monitored while it is in transit. SSL also supports digital identification so that each party can verify the other’s identity. This helps prevent *impersonation*—criminals using phony identities to purchase goods.

Online transactions can also be made more secure if identification of both parties is authenticated. *Authentication* is the process whereby a security system establishes the validity of an identification. In this way, if George sends a message to Nancy, Nancy can be sure that the message is really from George and not from an impostor. The best way to verify identity is through the use of *digital signatures,* which is made

possible by public key encryption. In this case a private key is used to sign one's signature to some message or piece of data and a public key is used to verify a signature after it has been sent. Assume that Nancy is sending an important request to her lawyer, George, regarding a transfer of funds. Nancy signs the request with her private key and then encrypts the signed message with George's public key that she finds on his website. When George receives this encrypted request, he applies his private key to descramble that message. He then uses Nancy's public key to authenticate that the message is really from Nancy; with that public key, he unlocks a signature that could only have come from her. As Levy observes, "this nonrepudiation feature is the electronic equivalent of a notary public seal."[29]

CyberSecurity as a Moral Obligation

There are, of course, many reasons why companies should be motivated to implement state-of-the-art security techniques to ensure information integrity and system reliability. There are certainly market pressures at work that encourage corporations to fix insecure computer networks. Customers will punish vendors who have a cavalier attitude about their personal data or who fail to practice commonsense digital hygiene. Government fines and class action lawsuits initiated by victims often ensue after a major data breach. Sound security mechanisms, on the other hand, will bolster consumer confidence that a corporation's online domain is a safe place to do business.

More importantly, there is a moral imperative to ensure that the level of cybersecurity is adequate. When customers make purchases online with their credit cards, engage in searches, or share information on a Facebook page, they are placing their trust in the hands of these digital and social media companies which collect and store all of this data. If those organizations are careless or lack proper security consciousness, the end result could be calamitous for their customers, who might

easily become victims of credit card fraud, identity theft, or other forms of mischief once their personal data are exposed and misappropriated. Hence, there is a moral duty to take reasonable precautions and to implement feasible security measures that will provide for the integrity of online transactions and prevent the risk of harm to unsuspecting consumers. As a correlative to the right to privacy there is not only the duty to avoid depriving people of that right but also the duty in relevant circumstances to prevent that right from being deprived by others. That latter duty certainly applies to custodians of personal data and digital platforms like Facebook, Google, or Apple, which must be constantly vigilant about preventing damaging data breaches. For example, companies must be proactive about investing in security measures such as advanced intrusion detection software. And they must be particularly diligent about updating their software with security patches once a vulnerability is detected.

Custodians of data also have an obligation to promptly notify users whenever there is a serious data breach. While Europe's General Data Protection Regulation (GDPR) mandates swift data breach notification, there are no comparable laws in the United States. But given the harm that can result from unauthorized access to their

personal data, users must be informed and given the opportunity to take steps to protect themselves as soon as possible. This knowledge is owed to all stakeholders who might be adversely affected by a data breach. To withhold or conceal data breach information without compelling and morally justified reasons is to engage in a form of deception.

In summary, unwarranted tardiness in disclosing data breaches along with half-hearted measures to secure user data represent serious forms of moral negligence. This indifference to the valid claims of stakeholders cannot meet the standards of morality nor ultimately satisfy market demands.

The Encryption Controversy: A Public Policy Perspective

As we have seen, the optimal means of securing information in transit is through the use of encryption. This technology enables users to send and receive sensitive data over a nonsecure network like the internet. However, the government has been apprehensive about the use and export of strong encryption systems (e.g., 128-bit keys), and in the past it has attempted to regulate exports by demanding “backdoor access,” that is, some form of control over all public and private keys. Government officials worried that international terrorists or bands of criminals would get their hands on a strong encryption system to which law enforcement authorities did not have the key. There were no restrictions on the domestic uses of strong encryption, and after a decade of squabbling, the export restrictions on encryption systems were greatly relaxed. But it is instructive to consider how encryption policy has evolved. The U.S. federal government’s previous plans and proposals provide historical perspective for the current controversies emerging from the availability of unbreakable encryption in consumer products and mobile devices.[30]

The Clipper Chip

The Clipper system was originally designed by the NSA as an encryption device for the telephone, but the plan was to quickly extend its use for computer data and communications. The ***Clipper chip*** was a specialized computer chip, with an encoded algorithm known as Skipjack, which would give law enforcement authorities access to all encrypted data communications. It was introduced in 1993 as a voluntary plan, but the government indicated that it would only purchase Clipper phones, and these phones would not interoperate with non-Clipper phones. The government's goal was to have this encryption chip become the industry standard for encryption.

The Clipper chip was a key escrow system with a backdoor key that was to be split between two government agencies. Each agency would hold half of a binary decryption key that could be used to decode encrypted communications. With a proper court order, law enforcement authorities could access these two halves so that this key could be used to eavesdrop on conversations of criminal suspects.

The technology behind Clipper was complicated but worked as follows: when two individuals using phones (or computers) equipped with these Clipper chip encryption devices activated the

encryption functionality, a symmetrical key, known as a *session key*, was generated. That session key encoded the sounds of the speaker as he or she left one end of the phone and decoded those sounds at the other end. The phone also automatically transmitted a packet of information called a law enforcement access field (LEAF). The LEAF included an encrypted version of the session key and a unique chip identifier. The Federal Bureau of Investigation (FBI) would have a universal family key that would give it access to the LEAF. Whenever the FBI (or other authorized law enforcement agency) was granted a legal warrant to wiretap, it could then extract from the LEAF the unique chip identifier. Once the FBI had this identifier, it could request the two portions of the unique key from the respective government agencies holding them in escrow; each agency would look up the unique identifier provided by the FBI and provide its portion of the key corresponding to that number. The FBI would combine the two halves of the key, thereby enabling it to decode the session key and to listen in on the encrypted communication.[31]

The National Security Agency (NSA) and other law enforcement authorities saw Clipper as an ideal solution that balanced the conflicting goals of privacy and public safety. According to an FBI

white paper on the issue, this encryption chip provided “extra privacy protection but one that can be read by U.S. government officials when authorized by law. . . . This ‘key escrow’ system would protect U.S. citizens and companies from invasion of their privacy by hackers, competitors, and foreign governments. At the same time, it would allow law enforcement to conduct wiretaps in precisely the same circumstances as are currently permitted under the law.”[32]

The Clipper chip proposal, however, was not met with the same enthusiasm outside of the federal government. It engendered enormous criticism and touched off a spirited and sometimes divisive debate. Security experts were quick to point out its many technical flaws: the Skipjack algorithm was classified and the scrambling was done by circuits hardwired on a tamper-proof computer chip rather than by software. This made it more difficult to change or upgrade this technology in the future. It also had the effect of making products with these devices more expensive because tailor-made chips were costly.

But most of the criticism was based on ideology and not on the absence of sound technology. Many believed that key escrow plans like Clipper chip were flawed because they relied on “trusted” third parties, namely, the escrow agents holding

the keys. According to this logic, the more parties involved in a cryptography scheme, the weaker it is. Civil libertarians saw this “scheme” as a massive assault on privacy rights that raised the specter of government officials routinely prying into the affairs of private citizens. According to the American Civil Liberties Union (ACLU), the Clipper chip plan was “the equivalent of the government requiring all homebuilders to embed microphones in the walls of homes and apartments.”[33] John Perry Barlow’s moral polemic against the Clipper chip sounded like a call to arms:

> Clipper is a last ditch attempt by the United States, the last great power from the old Industrial Era, to establish imperial control over cyberspace. If they win, the most liberating development in the history of humankind could become, instead, the surveillance system which will monitor our grandchildren’s morality. We can be better ancestors than that.[34]

The Clipper had some enthusiastic supporters, who feared what might happen if wiretapping became impossible thanks to hard-to-crack encryption technologies without any “backdoor” entry. They appreciated the government’s legitimate goal to prevent the spread of uncrackable encryption code. According to Stewart Baker, the strident and exaggerated opposition to Clipper reflected a “wide . . . streak of romantic

high-tech anarchism that crops up throughout the computer world."[35]

To be sure, there was some merit to these arguments. The exploitation of encryption by terrorists or computer-literate criminals is a valid public safety issue that cannot be dismissed. Barlow and his colleagues, however, also had a legitimate claim about the potential intrusiveness of the Clipper chip. In its efforts to balance national security needs and privacy, this technology might have given too much weight to national security by creating a system where the risks to privacy invasions were unacceptably high.

Key Management Infrastructure and Policy Reversal

In the wake of criticisms of Clipper, the government issued a new encryption plan. It was called *key management infrastructure* (KMI) and it authorized a government infrastructure with key recovery services. KMI was based on the premise that there must be a duly authorized certificate for all public keys. This would be achieved by registering the keys with a key escrow agent and having them digitally signed by certification authorities (CAs). These CAs would function as "digital notary's public," who would verify the identity of the individual associated with a given key.

Under this plan, encryption products with keys of any length could be exported as long as they included a sound key escrow (which the government now preferred to call *key recovery*) plan. The plan had to show how trusted third parties or escrow agents would hold the decryption key and be prepared to turn it over to federal authorities if presented with a warrant. This proposal too met with sharp opposition from privacy advocates and software firms, because the U.S. government would not abandon the requirement of key recovery.

In summary, the KMI proposal included the following policy guidelines, which were adopted in the fall of 1996:

> Jurisdiction over cryptography exports was shifted from the State Department to the Commerce Department.
>
> Companies could apply for approval to export encryption products using 56-bit DES immediately with the proviso that they must present their plans to implement key recovery in 56-bit products within a 2-year period.
>
> Finally, high-end or strong encryption products (such as 128-bit DES) could be exported but only if they included key recovery.

The shift of control for encryption products to the Commerce Department was seen as quite significant because this action signaled that the government no longer regarded encryption products as weapons to be managed by the State Department. Nonetheless, in his executive order authorizing this change, President Clinton reiterated the need for firm government control over this technology because of the threat to national security and America's foreign policy interests.

But, in January 2000, the Clinton administration finally reversed its long-standing policy on tight export controls. It issued a set of new encryption regulations that represented a fundamental

change in U.S. policy. In the U.S. government's view, these revised principles would help balance competing interests between electronic commerce and national security. The specific policy changes included the following: encryption commodities and software of any key length could now be exported to any nongovernment end user in any country (except the seven countries that supported terrorism). The new policy did not allow the export of strong encryption products to government end users without a license.

What about current U.S. encryption policy? That policy is not focused on export bans as it was in the past. Moreover, research has demonstrated that encryption architectures do not vary much from country to country. Comparable levels of strong data protection are available from different products in different countries. U.S. policy is now shaped by the government's direct participation in standard-setting organizations that direct the development of encryption software. The NSA also makes recommendations to government agencies to guide their adoption decisions. In 2015 it highlighted certain encryption algorithms that might be vulnerable to a new breed of supercomputers. The NSA advocated for the use of a new algorithm called Dual_EC_DRBG until significant weaknesses were discovered. U.S.

policy will also depend to some extent on the consequences of the recent proliferation of stronger encryption algorithms in messaging applications and mobile devices. It's certainly conceivable that the United States might exercise more control over encryption technologies if they are implicated in future terrorist attacks.[36]

New Encryption Disputes and Challenges

Since the terrorist attack in New York on September 11, 2001, law enforcement agencies in the United States have been pre-occupied with terrorism and the prevention of future attacks by groups like ISIS or Al Qaeda. Subsequent terrorist attacks of smaller scale in Paris, Sri Lanka, San Bernardino, and elsewhere have also concentrated renewed attention on encryption and surveillance. Following these attacks some countries began to feel pressure to allow law enforcement agencies more access to encrypted communications.

The debate in the United States about the use of strong encryption was revived by the decision of Apple to use 256-bit end-to-end and device encryption code as the default on their iPhones. Device encryption locks all the data on the smartphone and prevents the data from being read by anyone without a key. The decryption key is tied to the password and stored only on the phone. Apple has no copy of that key nor does it retain a master key. End-to-end encryption means that messages and other communications are encrypted with an unbreakable key so they can only be read by the original sender and intended

recipient. Other companies such as Google and Facebook have adopted these encryption technologies as well. WhatsApp, a messaging app owned by Facebook, uses 256-bit end-to-end encryption. Thus, all of the data on smartphones running Android or iMac will be unavailable to law enforcement officials even if they have a search warrant. There is no “backdoor” access to this encrypted data, which includes photos, messages, email, contacts, and call history.[37]

The FBI, along with other law enforcement agencies, reacted angrily to this latest chapter in the crypto wars. Some critics fault Apple for a lack of sensitivity to the national security element of the debate over this strong encryption architecture. Supporters, on the other hand, have argued that Apple is not designing systems that thwart law enforcement from executing a valid warrant. Rather, Apple is seeking to construct a secure system that prevents hackers and other bad actors from accessing data on a user’s iPhone. Given the revelations of Edward Snowden about the scope of U.S. government surveillance (such as the NSA’s access of user data found at several U.S. high-tech companies), Apple perceived a need to assure that their devices were secure from such prying.

This renewed encryption debate exposes once again the intractable tensions between privacy and security. Apple is committed to giving their users absolute privacy. But legal authorities sense a real threat to national security at the hands of these unbreakable encryption systems with no backdoor access. Ethicists have acknowledged the challenge of “going dark” and the competing security and privacy claims. Some argue that privacy rights are limited and therefore security interests can justify infringements of privacy rights under certain conditions. On the other hand, Adam Moore defends the position that in general “*privacy* for citizens. . .[is] more important than the security enhancing practices deployed or desired by government.”[38]

Finally, the United States and other governments have new reasons to be worried about encryption. The danger comes from hyper powerful, quantum computing systems that harness the quantum properties of atoms to solve intricate computer problems. These computers, which are still in the development stage, will be able to decrypt information that is now indecipherable. A quantum computer that intercepts information transmitted using current encryption standards (e.g., 256-bit key) could decrypt that data in hours and perhaps even in minutes. As a result, new encryption

algorithms that resist quantum computing will be necessary once these computers come online. Government agencies like the NSA must take the lead in developing a standard for quantum-safe encryption.[39]

Encryption Code, Privacy, and Free Speech

The heated encryption debate is closely interconnected with several of the other major themes discussed in this text—specifically, privacy and free speech. The encryption controversy is yet another example of how technology or code affects and controls behavior. The purpose of encryption code is to help guarantee privacy and information security. This code gives individuals the power to scramble up their communication in a way that makes it quite difficult for law enforcement authorities or anyone else to decrypt it. Once again, however, the radically decentralized network technology is empowering the individual in a way that threatens the interests of sovereign states. The United States has retreated from its impulse to regulate encryption, but there is no guarantee that it will not modify its encryption policy in the future.

Michael Godwin and other experts concur with the general reasoning behind the adoption of strong encryption: cryptography is central to free speech on an insecure medium such as the internet because it allows us to "speak with the assurance of confidentiality."[40] Without encryption, users cannot speak or share information with a high level

of confidence. It is important for people to feel that they can reveal “secrets” and express themselves freely without fear that the government agencies or other eavesdroppers may be listening. Encryption code has been regarded by libertarians as a way to promote the value of free speech in cyberspace. Hence their general support for the use of strong encryption code in devices like the iPhone and programs such as WhatsApp.

Arguably, allowing government to have backdoor access to encryption programs puts privacy rights in jeopardy as it opens up the possibility for general government surveillance. Once a person’s encryption key is uncovered, all of the individuals who electronically communicate with that person also become the subjects of government surveillance. A warrant is required before such surveillance begins, but, as Kang points out, “electronic eavesdropping cannot be regulated by a warrant precisely because of its dragnet quality.”[41] Moreover, if the FBI and other federal agencies get their wish about backdoor access and some type of master key, how could agents guarantee that this key would be safe from security breaches? And how could they assure the public that only authorized law enforcement officials would get access to that key?

Nonetheless, despite these questions, we must also acknowledge that the debate about encryption restrictions and national security has sometimes been a bit one-sided, especially in Silicon Valley. The government has the vast responsibility of enforcing the laws and ensuring civil order and stability. Law enforcement agencies are understandably threatened when terrorists or criminals use strong encryption to communicate. As the nation's national security strategy is revised in the light of recent terrorist events, there is growing sympathy for giving the government more discretion to monitor suspicious activities in order to prevent future attacks. However, any plans to enhance security must be implemented in a way that reflects the new realities of a more dangerous world while remaining sensitive to the centrality of individual liberties such as privacy and free expression for all users of modern technologies.

DISCUSSION QUESTIONS

1. Do you agree that hacktivism is a morally valid form of civil disobedience?
2. Is it morally permissible for a country like the United States or Israel to use a worm like Stuxnet to disrupt the development of nuclear weapons in countries like Iran or North Korea?
3. Where do you stand on the controversial encryption issue? Should governments like the United States be allowed to have an escrowed key or backdoor access to all encrypted communications? Is unfettered encryption a good thing for cyberspace?

Case Studies

The Lulz Sec Hackers

A New York City public housing project hardly looked like a place where someone could disrupt the activities of government agencies or corporations around the world. Yet in the midst of that obscure neighborhood, the Federal Bureau of Investigation showed up one morning to place under arrest a masterful hacker, Hector Xavier Monsegur, known in hacking circles as “Sabu.” Months after his arrest in 2011, Sabu became an informant, exposing the inner workings and structure of the hacker group known as “Lulz Sec,” which means laughable security. Federal prosecutors described Sabu as an “influential” member of the Lulz Sec organization.[42]

Lulz Sec is a splinter faction of “Anonymous,” a disparate group of hackers or hacktivists comprised primarily of young men ranging in age from their late teens to early 30s. In 2008, Anonymous initiated a DoS attack against the Church of

Scientology because of its obsessive efforts to keep its online data secret. Because Anonymous members believe strongly in the old internet value of free-flowing information, the group was sympathetic to WikiLeaks and its founder Julian Assange after he released thousands of confidential documents about U.S. military security. Anonymous hacked the websites of businesses that terminated their relations with WikiLeaks after this incident occurred. Among these companies were MasterCard, Visa, and PayPal (owned by eBay). Lulz Sec also hacked into the computers of the Public Broadcasting Service (PBS) after it aired an unsympathetic *Frontline* exposition about WikiLeaks. And in the spring of 2011, Lulz Sec disabled the Central Intelligence Agency's website for a short time—though, according to the Agency, no classified data were compromised.[43]

In addition to disabling websites and denying online service, Lulz Sec also filches computer files. After hacking into the computers of Sony Pictures, it stole the personal information of about 100,000 customers. It also seized the personal data

of 200,000 users of the video game *Brink*, which is a product of Bethesda Software.[44]

Lulz Sec has justified its highly publicized attacks as a vivid means of exposing security holes in the computer systems of government agencies and corporations. They have aimed to show that the strong security safeguards proclaimed by corporations and government agencies are no more than a fleeting illusion. However, group members also admit they do this for the fun of it. “This is the Internet,” one of them said, “where we screw each other over for a jolt of satisfaction.”[45]

While law enforcement officials point to its pernicious effects, hacktivism has supporters who consider this activity to be a valid form of online protest and even civil disobedience. Although not necessarily endorsing all the tactics of groups like Anonymous, hacktivist apologists applaud their creativity and ingenuity. They see value in protesting the treatment of organizations like WikiLeaks. Others regard hacktivists as providing an invaluable service by exposing security deficiencies so they can be properly repaired. Support for hacktivism sometimes

comes from unlikely places. Father Antonio Spadaro, writing for *Civiltà Cattolica*, a publication sponsored by the Vatican, approvingly characterized the hacker philosophy as “playful but committed, encouraging creativity and sharing, and opposing models of control, competition and private property.”[46]

On the other hand, hacktivism is not typical of civil disobedience, which involves peacefully protesting unjust laws while willing to suffer the consequences of one’s actions. Hackers are anonymous, elude law enforcement officials, and often cause damage to systems that they infect with worms and viruses. The favorite tactic of “doxing,” finding embarrassing personal information about someone and disclosing it online, has the potential to be extremely damaging. It’s one thing to protest the actions of a government agency or corporation, but it’s quite another thing to pick on one or two executives and expose the personal details of their lives. This tactic could inadvertently bring harm not only to them but to their families and associates, innocent third parties who have nothing to do

with the behavior under assault by the hackers.

The Lulz Sec group has dispersed for now, but hacktivism will surely live on and continue to be a source of interest and controversy.

Questions

1. How do you assess the various activities of Lulz Sec? Do you agree with their actions in support of WikiLeaks, such as DoS attacks?
2. Under what conditions is hacktivism morally permissible?

Case Studies

The New Crypto Wars: The Dispute over Apple's iPhone

Encryption technology in the United States has a long and involved history that has often pitted Silicon Valley against the federal government in Washington, D.C. In the latest chapter of this history Apple found itself entangled in an intense controversy centered on its very popular iPhone. At issue was the employment of hyper-strong device encryption that tightly locked the data stored on the iPhone. In the aftermath of a terrorist attack in 2015 in San Bernardino the FBI and Apple squared off in a public battle over encryption.

The San Bernardino shooting was another tragic incident where innocent people were senselessly killed at the hands of terrorists. Armed with an assault rifle, Mr. Syed Farook, a county health inspector, killed 14 people and wounded 22 others. Farook was assisted in the lethal attack by his wife. The couple was killed a short time later in a shootout with police.

One piece of crucial evidence was one of the assailant's iPhones. Since that phone ran the iOS 9 operating system, it was protected by unbreakable encryption, and its contents could not be accessed by the FBI as part of its investigation into these horrific shootings. Apple could not comply with the FBI's request, backed by a federal warrant, for access to the phone since the company did not retain the master key to this data. The FBI then requested that Apple create new software that would simply overcome the phone's built-in hyper security. The FBI did not ask Apple to construct a master key. Rather, it sought an alternative operating system software for this one phone that would allow them to break into this locked device. Among other things, this software would disable a feature that erases data stored on the phone after 10 unsuccessful password attempts. But Apple refused because it was concerned that such software, which bluntly overrode the iOS 9, could be stolen or somehow fall into the wrong hands.[47]

One year earlier, in the fall of 2014, the company had announced that this new encryption architecture would be built into

the iOS 8, the iPhone's operating system, along with all subsequent versions of that operating system (OS). The 256-bit AES algorithm would prevent anyone other than the iPhone user from accessing the data stored on that phone. Hence all the important data on a user's smartphone—photos, messages, contacts, reminders, call history—are now locked up with unbreakable encryption by default. Decryption is seamlessly linked to the user's password. Only the user would be able to access the iPhone's contents, unless his or her passcode has been compromised. Apple indicated that it would not retain a master key to unlock the contents of any user's phone or provide any sort of "backdoor access" to these data. Without the user's password and cooperation, law enforcement officials would have no means of accessing any information locked on the smartphone.[48]

Similarly, Facebook has introduced a 256-bit end-to-end encryption technology for its WhatsApp text messaging service to secure messages in transit from one smartphone or mobile device to another. WhatsApp has adopted the open-source software Text Secure, which scrambles messages with a

cryptographic key that only the user can access and never leaves his or her device. The result is unbreakable encryption for hundreds of millions of phones and tablets that have WhatsApp installed. Moreover, Facebook, following the precedent set by Apple, will not store a master key to unscramble these data.[49]

Law enforcement officials in the United States, including the Federal Bureau of Investigation (FBI), have expressed great dismay over this further evolution of the crypto wars. The FBI wants Apple and Google (the maker of the Android OS for smartphones) to design a smartphone system so that police and federal authorities (with a court order) can access information stored on that phone without any compromise in security. Former FBI Director James Comey insisted that the FBI needs access to suspects' iPhones and WhatsApp messages. Also, according to Comey, encrypted smartphone apps help terrorist organizations recruit and allow "bad people. . .to communicate with impunity." Full disk encryption, he argued, materially limits law enforcement's capacity to efficiently investigate crimes and terrorist acts.[50]

Companies like Apple, however, have ignored these government warnings, arguing that the protection of user privacy is of paramount importance. They are strongly opposed to building any version of an encryption backdoor. Apple CEO, Tim Cook, remains convinced that strong encryption without backdoor access is the only suitable way to protect the privacy of Apple's customers: "I don't know a way to protect people without encryption. . . .[and] you can't have a backdoor that's only for the good guys."[51]

Civil libertarians have generally applauded Apple's decision. According to *Wired*, "Apple has come to the right place. It's a basic axiom of information security that 'data at rest' should be encrypted. Apple should be lauded for reaching that state with the iPhone." Google's decision to follow suit by incorporating this full device encryption architecture in the Android operating system also pleased civil libertarians who have long called for strong crypto to protect user privacy. On the other hand, the *Washington Post* has argued for a "secure golden key" that would enable police to decrypt a smartphone with a warrant. Others citing

national security arguments contend that this "Clipper chip" approach is both suitable and necessary.[52]

In the midst of this debate, one thing is certain: the dispute about unbreakable encryption has been revived with a new fury and a renewed intensity. A pivotal question is whether it would be possible to develop some type of emergency access system for consumer devices with strong encryption that did not pose privacy and information security risks.

Questions

1. If you were Apple CEO Tim Cook would you have cooperated with the FBI after the San Bernardino shootings? How might you feel if you were a relative of someone killed in the San Bernardino attack?
2. Outline in as much detail as possible the costs and benefits of Apple's decision to encrypt the data locked on an iPhone without a backdoor key.
3. Evaluate Apple's policy from a moral point of view. Is the company right to prioritize privacy over security?

Case Studies

The Equifax Data Breach

Equifax, along with Experian and TransUnion, is one of the “Big Three” credit reporting agencies in the United States. All three companies offer credit monitoring services as their core business. There are many regulations and restrictions governing the collection and use of credit data, but these companies have enjoyed stable sales and profits for many years. Equifax is based in Atlanta and its long history traces back to 1913. It employs over 10,400 employees worldwide and maintains data on 820 million consumers.

All three agencies exchange data with banks and other financial companies that extend credit. They develop “credit scores” for how well a consumer has handled his or her credit and debt obligations. This score and the accompanying credit report detailing a person’s credit history are then sold to banks, credit unions, retail credit card issuers, auto lenders, mortgage lenders, and others who rely on this information when they make loans, issue credit cards, or offer consumers mortgages and home equity

loans. It is also used by banks to check this information before issuing bank credit cards such as Visa or MasterCard. Equifax, Experian, and TransUnion have most likely compiled credit histories for nearly every adult U.S. citizen.[53]

In early September 2017, Equifax announced that hackers had gained illicit access to the personal information of 143 million people. The data included social security numbers, birth dates, phone numbers, email addresses, driving license numbers, and, in some cases, credit card numbers. The total number expanded to 148 million by March 2018. The pilfering of social security numbers was particularly worrisome since that number in the wrong hands creates opportunities for identity theft and other types of fraud.

The Equifax data breach is one of the three worst data breaches in U.S. history along with Yahoo and Marriott. The Marriott data hack of 2018 affected 500 million users. In September 2016, Yahoo revealed a serious data security breach that had occurred 2 years earlier when 500,000 million records were compromised. Several months later, in

December, 2016, Yahoo informed its users of another newly discovered data breach. That breach occurred in 2013 and affected more than 1 billion Yahoo users. However, despite the magnitude of the Yahoo and Marriott breaches, the Equifax data breach is considered more damaging because social security numbers and birth dates were involved. As one security expert observed, "This data is the key to everyone's files and interactions with financial services, government, and health care."[54]

After the announcement was made, the credit reporting agency was heavily criticized for waiting until September 7 to reveal this data breach to the public. The breach actually took place in March 2017 and went undetected for almost 3 months. It was discovered in late July, but the company decided to withhold this information from the public until it was able to verify the scope of the breach. Thus, Equifax's public announcement did not happen until 6 weeks after the company had learned about the incident and 4 months after the hackers had penetrated the Equifax network.

Cause of the Data Breach

Not long before the data hack announcement, the CEO of Equifax, Rick Smith, reaffirmed his company's commitment to cybersecurity. In answer to a question at a mid-August breakfast meeting Smith said that protecting consumer data was a "huge priority" for the company.[55] However, according to several cyber risk analysis companies, weaknesses and flaws were obvious in the Equifax network well before this dangerous data breach had occurred. The company had long been considered an attractive target for identity thieves because of its defective cybersecurity practices.[56]

But exactly what went wrong at Equifax? The breach was enabled by a security flaw in a program called Apache Struts, a widely used web application development software product. Through that software bug, hackers gained access to the software underlying the Equifax online dispute portal and from there accessed the internal company databases. Hackers were able to send data to a server that was equipped to take advantage of the software flaw. It was "the digital equivalent of popping open a side window to sneak into a building."[57]

Apache issued a patch for the problem as soon as it was discovered. The U.S. Security Readiness Team, which is part of the Department of Homeland Security, sent out a public alert on March 8, 2017 about the software flaw. On March 9, Equifax's Global Threats and Vulnerability Management (GTVM) team released an internal notice declaring the urgent need to install the patch for any Apache Struts applications. The GTVM alerted its programmers and developers that the patch should be installed as soon as possible and no later than 48 hours from receipt of its March 9 memo.

However, Equifax did not patch the Apache Struts software flaw until August, 4 months later and well after the fatal intrusion occurred. There were two problems. First, Equifax's chief developer for the online dispute portal, which used the hacked Apache application, was not on the GTVM memo distribution list. Second, in response to the alert about the Apache Struts problem, Equifax scanned its network to identify the vulnerable versions of this program. But the scanning tool did not perform a thorough search at every level of the network and did not identify the vulnerable version of the

Apache Struts application that was used for the online dispute portal. Part of the problem was the company's failure to maintain a comprehensive and up-to-date information technology (IT) inventory. Without that inventory, the scanning tools could not be properly directed to find all the instances of the Apache Struts vulnerability.[58]

In contrast to Equifax, both of its rivals, TransUnion and Experian, received the same alert from Homeland Security and the same patch from Apache Struts. Both companies patched vulnerable versions of the software within days of receiving the patch and neither suffered a data breach because of this security flaw.

The 2015 Security Audit

Critics of Equifax have said that its IT and security capabilities have not kept pace with its lofty ambitions. CEO Smith had transformed Equifax from a credit reporting agency into a data giant by purchasing other companies with databases that tracked information about consumers' employment history, salaries, and so forth. Equifax was becoming a "global data-analytics company." But Smith and his executive team

concentrated more on data collection and processing and not so much on securing that data.[59]

As a result, Equifax lagged behind basic security maintenance, despite the fact that the data of credit firms tends to attract many opportunistic hackers. Security ratings companies sounded the alarm but no one at Equifax seemed to be listening. In April 2017, the cyber risk analysis firm, Cyence, rated the likelihood of a dangerous data breach at Equifax during the next 12 months at 50%. Also, according to Cyence, in their peer group of 23 companies the credit reporting agency was second to last. Security Scorecard ranked Equifax “in the middle of the pack” among financial services companies. The reason for the low score was the use of older software and tardiness in installing patches. And Fair Isaac Corp gave Equifax a 550 FICO score on a scale that ranges from 300 to 850. The score takes into account hardware, network security, and web services.[60]

Equifax appeared to be blindsided by the breach and allegations of its weak security infrastructure that followed its announcement

to many dismayed consumers who found out that their personal information may have been stolen. But the company had ample warning that its security system was vulnerable and in need of improvement.

In 2015, an internal security audit was conducted to review the state of cybersecurity and the company's current policies. The audit exposed salient cybersecurity flaws and deficiencies in the Equifax network. The report concluded "current patch and configuration management controls are not adequately designed to ensure Equifax systems are securely configured and patched in a timely manner."[61] The audit called attention to Equifax's failure to confirm the successful implementation of patches. According to the audit, "most Equifax systems are not patched in a timely manner." The audit report also underscored a large number of vulnerabilities in the company's IT systems. The report cited 1,000 vulnerabilities on externally facing systems and 7,500 on internal systems spread across 22,000 host servers. Despite these findings, there were no follow-up audits subsequent to the disappointing 2015 report.[62]

Epilogue

After the breach and the consumer backlash it generated, there were predictions that regulators would impose strict new rules on the credit-reporting industry. But no new regulations have been implemented in the United States. There are still no federal laws mandating notification of data breaches within a certain time frame. Equifax had to endure only minimal adverse consequences, but it has budgeted an additional $200 million for IT security. The Consumer Financial Protection Bureau, the agency responsible for the protection and security of consumer data, initiated no punitive actions against Equifax. The Federal Trade Commission also refrained from taking any enforcement action against this credit-reporting company.[63]

Questions

1. Discuss the moral issues in this case and whether or not Equifax's actions constitute a moral failing.
2. Should companies like Equifax be compelled to announce data breaches to the public within a certain time frame (e.g., 72 hours after discovery)? What would be the downside of legalizing such a requirement?

3. In your opinion, why was security so lax at Equifax and how can this laxity be remedied?

REFERENCES

1. Brooks Barnes, “Sony Breach Now Wider,” *The New York Times*, December 3, 2014, B1–2. See also “Horror Movie,” *The Economist*, December 13, 2014, 65.
2. Aisha Al-Muslim and Dustin Volz, “Marriott Hit by Data Breach,” *Wall Street Journal*, December 1, 2018, A1–2.
3. Geoffrey Fowler, “Phishing: You’re Still at Risk,” *Wall Street Journal*, February 23, 2017, B4.
4. Siobhan Gorman, “Electricity Grid in U.S. Penetrated by Spies,” *The Wall Street Journal*, April 8, 2009, A1–2.
5. Gary Anthes, “Malware’s Destructive Appetite Grows,” *Computerworld*, April 1, 2002, 46.
6. David O’Brien et al., “Privacy and Cybersecurity,” Research Briefing, Berkman Klein Center, Harvard University, September 2016.
7. This definition is derived from Tavani’s definition of computer crime. See Herman Tavani, “Defining the Boundaries of Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace,” in *Readings in*

Cyberethics, eds. Richard Spinello and Herman Tavani (Sudbury, MA: Jones and Bartlett Publishers, 2001), 451–62.

8. "Dotcom Bust," *The Economist*, January 28, 2012, 66.
9. Tavani, "Defining the Boundaries of Computer Crime."
10. "War in the Fifth Domain," *The Economist*, July 3, 2010, 25–27.
11. Joseph Mann, "Computer Worm Triggers Worldwide Alarm," *Financial Times*, September 24, 2010, 3.
12. "Electronic Bandits," *Economist*, May 20, 2017, 69–70. See also Stu Woo and Robert MacMillan, "Hack Probe Zeroes in on How Virus Invaded Networks," *Wall Street Journal*, May 16, 2017, A1, A6.
13. Siobhan Gourman, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *The Wall Street Journal*, April 21, 2009, A1–2.
14. Julie Cohen, "Between Truth and Power," in *Information, Freedom and Property*, ed. Mirielle Hildebrandt (New York: Routledge, 2016), 61–62.
15. Ibid., 67.

16. Dorothy Denning, “Concerning Hackers Who Break into Computer Systems,” in *High Noon on the Electronic Frontier*, ed. Peter Ludlow (Cambridge, MA: MIT Press, 1996), 141.

17. Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (Oxford: Oxford University Press, 2014), 295.

18. *The Computer Fraud and Abuse Act*, U.S.C. Section 1030 (a), (1)–(9).

19. Eric Blackwell, “Computer Crimes,” *American Criminal Law Review* 38 (2001): 481.

20. Eugene Spafford, “Are Computer Hacker Break-Ins Ethical?” *Journal of Systems Software* (January 1992): 45.

21. Mark Mannion and Abby Goodrum, “The Hacktivist Ethic,” in *Readings in Cyberethics*, 2nd ed., eds. Richard Spinello and Herman Tavani (Sudbury, MA: Jones and Bartlett Publishers, 2004), 526.

22. Singer and Friedman, *Cybersecurity and Cyberwar*, 77.

23. Geoffrey Fowler, “Chinese Censors of Internet Face Hacktivists in U.S.,” *The Wall Street Journal*, February 13, 2006, A1, A9.

24. Joseph Mann, “A Digital Deluge,” *Financial Times*, July 31, 2010, 5.

25. Nicole Perlroth, “Hacked vs. Hackers: Game On,” *The New York Times*, December 3, 2014, F1, F7.
26. Simson Garfinkel (with Gene Spafford), *Web Security and Commerce* (Cambridge, UK: O’Reilly & Associates, 1997), 21.
27. Rutrell Yasin, “The Cost of Security,” *InternetWeek*, February 21, 2000, 12.
28. Quoted in Laura DiDio, “Internet Boosts Cryptography,” *Computerworld*, March 16, 1998, 32.
29. Steven Levy, *CRYPO* (New York: Viking, 2001), 73.
30. Ryan Budish, Herbert Burkert, and Urs Gasser, “Encryption Policy and Its International Impacts” (Hoover Institution, Aegis Series Paper No. 1804, May, 2018).
31. See Levy, *CRYPO*, 232–33.
32. Quoted in Levy, 240–41.
33. See Dan Froomkin, “Deciphering Encryption,” *The Washington Post*, May 8, 1998, A4.
34. John Perry Barlow, “Jackboots on the Infobahn,” *Wired*, April, 1994, 87.
35. Stewart Baker, “Don’t Worry Be Happy: Why Clipper Is Good For You,” *Wired*, June 1994.
36. Budish, Burkert, and Gasser, “Encryption Policy and Its International Impacts.”

37. Matt Olsen, Bruce Schneier, and Jonathan Zittrain, “Don’t Panic: Making Progress in the Going Dark Debate,” Berkman Center Policy Paper. Cambridge: Berkman Center for Internet and Society, 2016.

38. Adam Moore, “Why Privacy and Accountability Trump Security,” in *Privacy, Security, and Accountability*, ed. Adam Moore (London: Rowman & Littlefield, 2016), 179–80.

39. Christopher Mims, “The Race to Save Encryption,” *Wall Street Journal*,” June 5, 2019, R1–2.

40. Mike Godwin, *Cyber Rights* (New York: Random House, 1998), 156.

41. Teddy Kang, “Cryptography,” Berkman Klein Center, Harvard University, 2002, **http://eon.law.harvard.edu/privacy/Encryption%20Description.html**.

42. Chad Bray and Reed Albergotti, “Hackers Arrested as One Turns Witness,” *The Wall Street Journal*, March 7, 2012, A1–2.

43. Cassell Bryan-Low and Ann Gorman, “Inside the Anonymous Army of ‘Hacktivist’ Attackers,” *The Wall Street Journal*, June 23, 2011, A1, A14.

44. Ibid.

45. Ibid.

46. Philip Willan, “Vatican Publication Rehabilitates Hackers,” *TechWorld*, April 6, 2011.

47. James Nicas and Robert McMillan, “Newer Phones Aren’t Easy to Crack,” *The Wall Street Journal*, February 18, 2016, A6.

48. Kevin Poulson, “Apple’s iPhone Is a Godsend, Even If Cops Hate It,” *Wired*, October 8, 2014. See also Devlin Barrett and Danny Yardon, “Apple, Others Encrypt Phones, Fueling Government Standoff,” *The Wall Street Journal*, November 19, 2014, A1, A10.

49. Andy Greenberg, “WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users,” ***Wired.com***, November 18, 2014.

50. Danny Yardon, “Tech Firms Hit Back at FBI on Encryption,” *Wall Street Journal*, July 8, 2015, B1.

51. Danny Yardon, “Attacks Fan Encryption Debate,” *The Wall Street Journal*, November 20, 2016, B1, B6.

52. Greenberg, “WhatsApp Just Switched,” and Editorial Board, “Compromise Needed on

Smartphone Encryption," *The Washington Post*, October 3, 2014.

53. "The Equifax Data Breach," *The Economist*, September 16, 2017, 69–70.

54. Anna Maria Andriotis, Robert MacMillan, and Christina Rexrode, "Equifax Comes under Attack for Data Breach," *Wall Street Journal*, September 9, 2017, B1–2.

55. Anna Maria Andriotis and Michael Rapoport, "Hack Upends Equifax CEO," *Wall Street Journal*, September 23, 2017, B1–2.

56. Anna Maria Andriotis, Michael Rapoport, and Robert MacMillan, "'We've Been Breached' Inside the Equifax Hack," *Wall Street Journal*, September 18, 2017, A1, A11.

57. Ibid., A11.

58. "How Equifax Neglected Cybersecurity and Suffered a Devastating Data Breach," Staff Report, Permanent Subcommittee on Investigations, United States Senate, May 2018, 7–9.

59. Andriotis and Rapoport, "Hack Upends Equifax CEO," B2.

60. Anna Maria Andriotis and Robert MacMillan, "Equifax Showed Signs of Trouble," *Wall Street Journal*, September 27, 2017, A1.

61. "How Equifax Neglected Cybersecurity," 7.

62. Ibid., 21–28.

63. Glenn Fleishman, “Equifax Data Breach, One Year Later: Obvious Errors and No Real Changes,” *Fortune*, September 8, 2018.

ADDITIONAL RESOURCES

Barlow, John Perry. “Jackboots on the Infobahn.” *Wired*, April, 1994, 87–88.

Bidgoli, Hossein, ed. *Handbook of Information Security*. 3 volumes. New York: Wiley, 2005.

Denning, Dorothy and Peter Denning. *Internet Besieged*. Reading, MA: Addison-Wesley, 1998.

Diffie, Whitfield. “The First Ten Years of Public Key Cryptography.” *Proceedings of the IEEE* 76, no. 5 (1998): 560–77.

Himma, Kenneth, ed. *Readings on Internet Security: Hacking, Counterhacking, and Other Moral Issues*. Sudbury, MA: Jones and Bartlett Publishers, 2006.

Hoffman, Lance. *Rogue Programs: Viruses, Worms, and Trojan Horses*. New York: Van Nostrand Reinhold, 1990.

Huschle, Brian. “Cyber Disobedience: When Is Hacktivism Civil Disobedience?” *International Journal of Applied Philosophy* 16, no. 1 (2002): 69–84.

Levy, Steven. *CRYPTO.* New York: Viking, 2001.

Levy, Steven. *Hackers*. New York: Dell Publishing, 1984.

Manjikian, Mary. *Cybersecurity Ethics*. New York: Routledge, 2018.

Mannion, Mark, and Abby Goodrum. “Terrorism or Civil Disobedience. Toward a Hacktivist Ethic.” *Computers and Society* 30, no. 2 (2000): 14–19.

Moore, Adam, ed. *Privacy, Security, and Accountability.* London: Rowman & Littlefield, 2016.

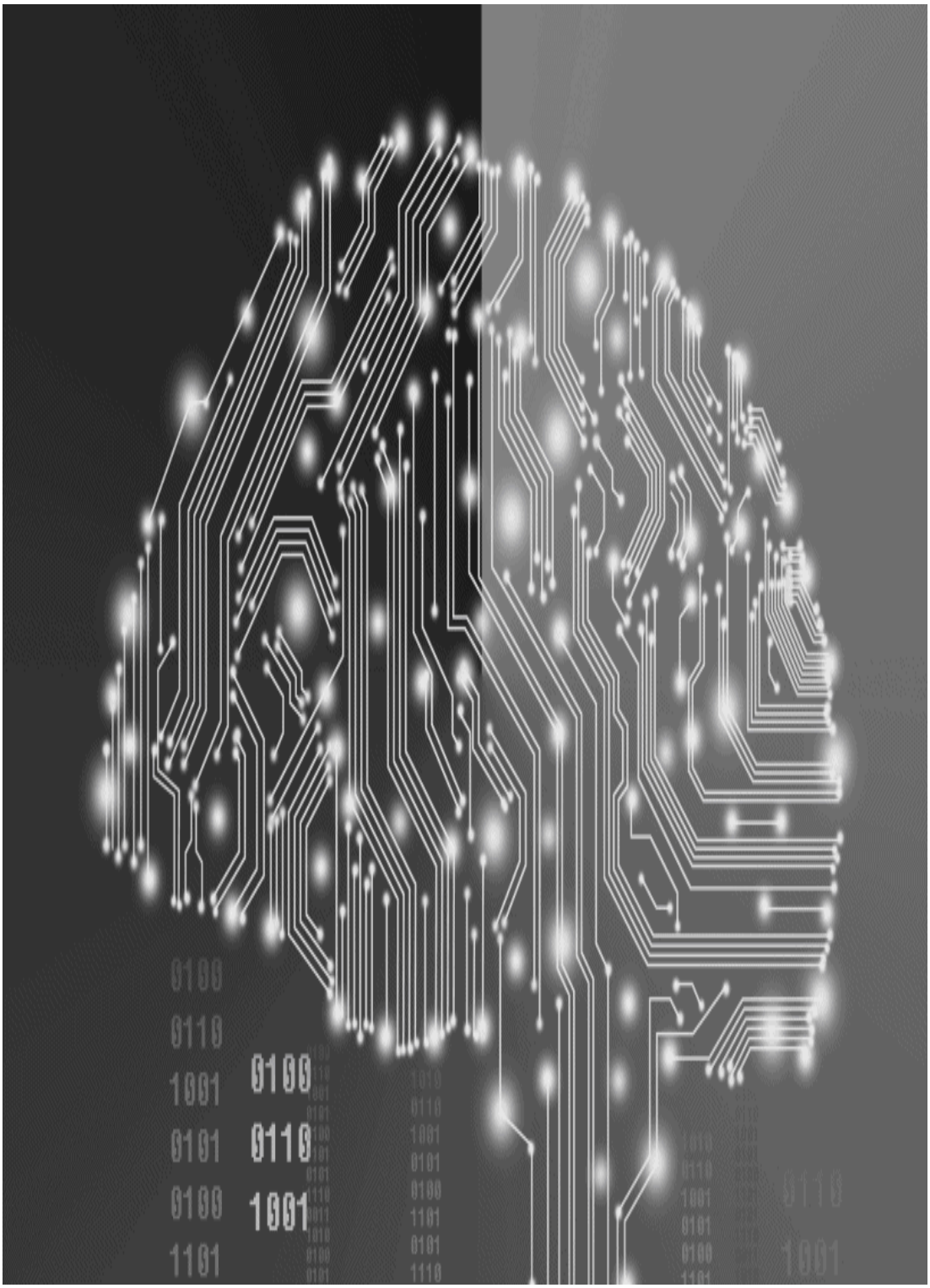
O’Brien David, et al., “Privacy and Cybersecurity,” Research Briefing, Berkman Klein Center, Harvard University, September 2016.

Singer, Peter W., and Allan Friedman. *Cybersecurity and Cyberwar*. Oxford: Oxford University Press, 2014.

Spafford, Eugene. “Are Computer Hacker Break-Ins Ethical?” *Journal of Systems Software*, (January 1992): 41–47.

Tavani, Herman. “Defining Computer Crime: Piracy, Break-Ins, and Sabotage in Cyberspace.” In *Readings in Cyberethics*, 2nd ed., edited by Richard Spinello and Herman Tavani, 513–24. Sudbury, MA: Jones and Bartlett Publishers, 2004.

Whitfield, Diffie, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption.* Cambridge, MA: MIT Press, 1998.



GLOSSARY

The Language of the Internet

Advanced Standard Encryption (AES):
Symmetric encryption algorithm that supports strong 128-bit encryption.

Application Programming Interfaces (APIs):
Prewritten methods or blocks of code to handle basic programming functions that work as software interfaces.

Bot:
Software device that enters a website and compiles information at superhuman speed.

Browser:
A software tool that enables users to navigate through the internet and link from one website to another.

Cache:
A means of storing information so that the end user can access it more quickly; a web browser caches or stores previously visited webpages on the user's hard drive.

Clipper chip:
System developed by the U.S. National Security Authority (NSA) for the encryption of telephone communications; this system was never implemented because of concerns about privacy.

Cookie:
A small file deposited on a user's hard drive from a web server that often contains concise data about what that user examined at the website.

Cybersquatting:

The practice of registering a domain name incorporating a trademark for the purpose of ransom, that is, offering it for sale at an exorbitant price to the trademark holder.

Data encryption standard (DES):

Symmetric private key cryptography system once approved and used by the U.S. government.

Digital certificate:

Electronic validation of the identity of someone sending a message or transmitting other data in cyberspace.

Domain name:

Worldwide naming convention that permits each website to have a unique, identifiable name, which is linked to a URL address.

Eavesdropping:

Electronic snooping of internet data as they are transmitted through multiple computer systems to their final destination.

E-book:

The digital version of books for sale online by distributors like Amazon**.**

E-commerce (electronic commerce):

A business model in which revenue is generated by taking advantage of the internet and technology-mediated relationships.

Encryption:

A process whereby data are encoded or scrambled to be unintelligible to eavesdroppers; the data are decoded or converted back to their original form by means of a key available only to the intended recipient of the data.

Filter:

Software programs, installed on computers or routers, used to censor internet content.

Firewall:

Security mechanism that positions hardware/software between an organization's networked server and the internet.

Framing:

Webpage element in which the author includes material from another webpage in a "frame" or block on the screen, usually with its own advertising and promotional material.

Hacktivism:

The use of hacking and online disruption as a means of protest or civil disobedience.

Hypertext Markup Language (HTML):

A language of formatting commands used to create multimedia hypertext documents or webpages.

Internet protocol (IP) address:

Unique four-part numeric address for any computer system connected to the internet so that information being transmitted over the network can be sent to its proper destination.

Internet service provider (ISP):

Service that enables individual subscribers or organizations to link to a worldwide computer network (i.e., the internet), usually for a monthly fee.

Java:

General-purpose programming language developed by Sun and used to write apps for systems such as Android.

Key:

Tool used in cryptography to encrypt and decrypt data; key length determines the strength of the encryption algorithm.

Linking:

Connection between two different webpages or between two different locations within the same webpage; a “hyperlink” within a webpage contains the address for another website and appears in the form of an icon and is activated with the click of a mouse.

Macrovirus:

Rogue software that exploits programs called “macros” found in applications such as Microsoft Word.

Malware:

Software designed to cause damage such as a computer virus or worm.

MP3 (MPEG-1, Layer 3):

Compression standard that allows music to be stored on a computer hard drive without any degradation of sound quality.

Open Source Code Movement:

A movement advocating that the source code of application or operating system software be made freely available for modification, corrections, and redistribution (source code consists of a computer program’s statements written in a high-level language such as Java or C++).

Opt-in:

An approach to privacy based on *informed consent*; it requires vendors to seek permission before selling or

reusing someone's personal information.

Opt-out:

An approach similar to opt-in, but in this case users are notified that their personal data will be used for secondary purposes unless they disapprove and they notify the vendor.

Organic search results:

Unpaid search results offered by search engines like Google.

Peer-to-peer (P2P) network:

A network that enables two or more personal computers to share files directly without access to a separate server.

Phishing:

Use of email to illicitly get someone's sensitive information such as a bank account number.

Portal:

Web-based interface that gives users access to multiple applications such as news services, commercial websites, and email all through one main screen; most portals such as Yahoo also provide search functionality.

Private key encryption:

A symmetric encryption scheme that uses the same secret binary key to encode and decode data.

Proxy server:

An internet server that controls client computer systems' access to the internet.

Public key encryption:

An asymmetric encryption scheme in which one of the two keys used in the encryption process is published in a

directory or otherwise made public and the other is kept private.

Ransomware:

Intruders encrypt a victim's computer files and hold them for ransom.

RSA:

A standard public key encryption system available from RSA Data Security, Inc.

Secure Sockets Layer (SSL):

A security protocol that protects data sent between web browsers and web servers.

Spam:

Unsolicited, electronic junk mail sent in bulk form from an individual or organization, usually promoting their goods or services to potential customers on the internet.

Spider:

Robotic software that explores the web by retrieving and examining documents by following hyperlinks.

Spyware:

Software that installs itself on people's computers, usually when they download free programs; this software tracks users' movements around the internet and serves pop-up ads.

TCP/IP:

The network protocol that enables data to be transferred on the internet.

Top-level domain (TLD):

The last extension in a domain name that identifies a website; examples include .edu and .com.

Trusted system:

Hardware and/or software programmed to enforce copyright protection by enforcing access and usage rights that dictate how and when a digital work can be used.

Uniform resource locator (URL):

The unique electronic address for a website.

Virus:

Self-replicating code that changes computer programs or files by inserting itself, thereby infecting a user's computer system.

Web server:

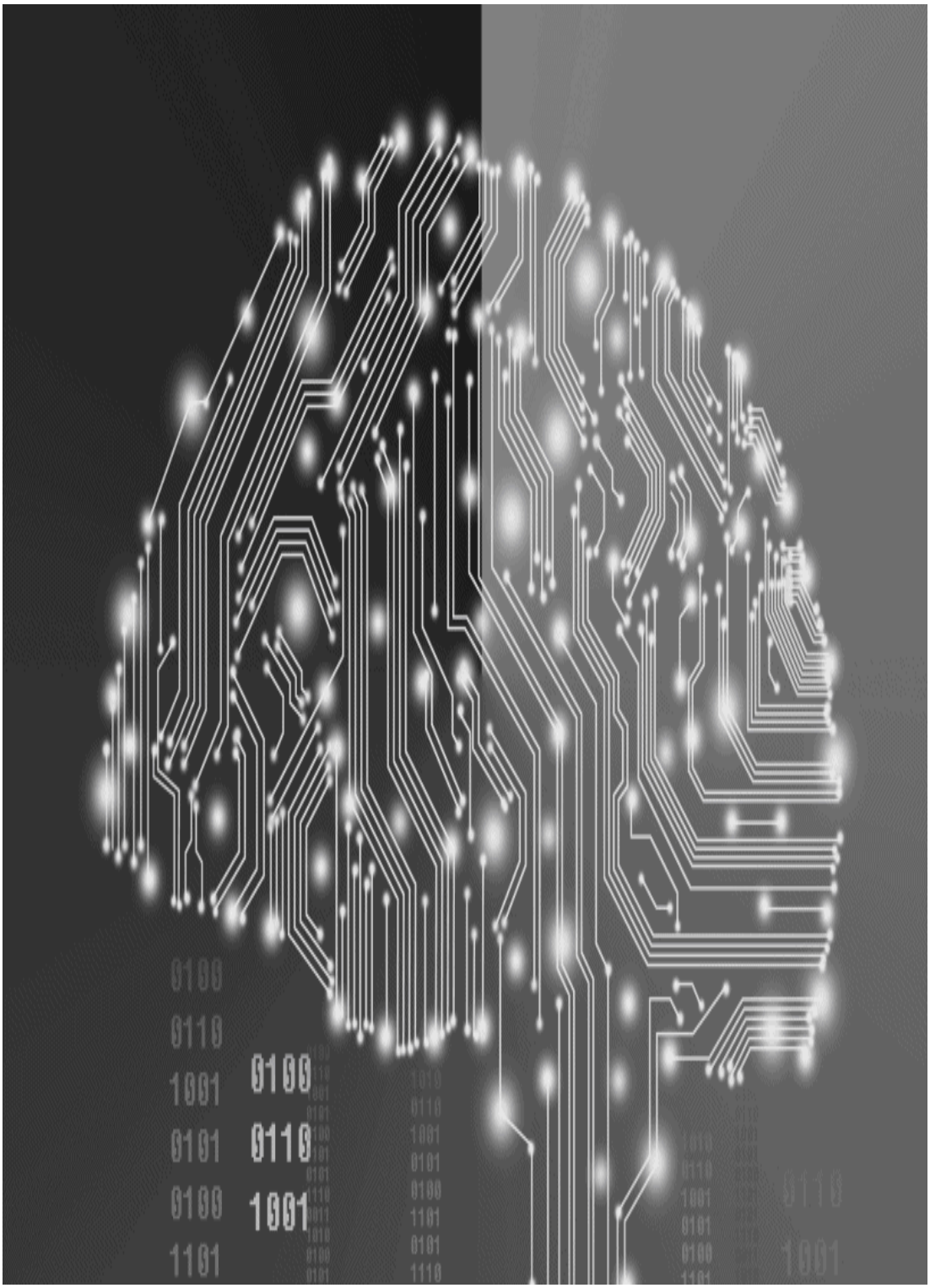
The hardware system on which a website resides.

World Wide Web:

A location within the internet that provides for the multimedia presentation of information in the form of websites.

Worm:

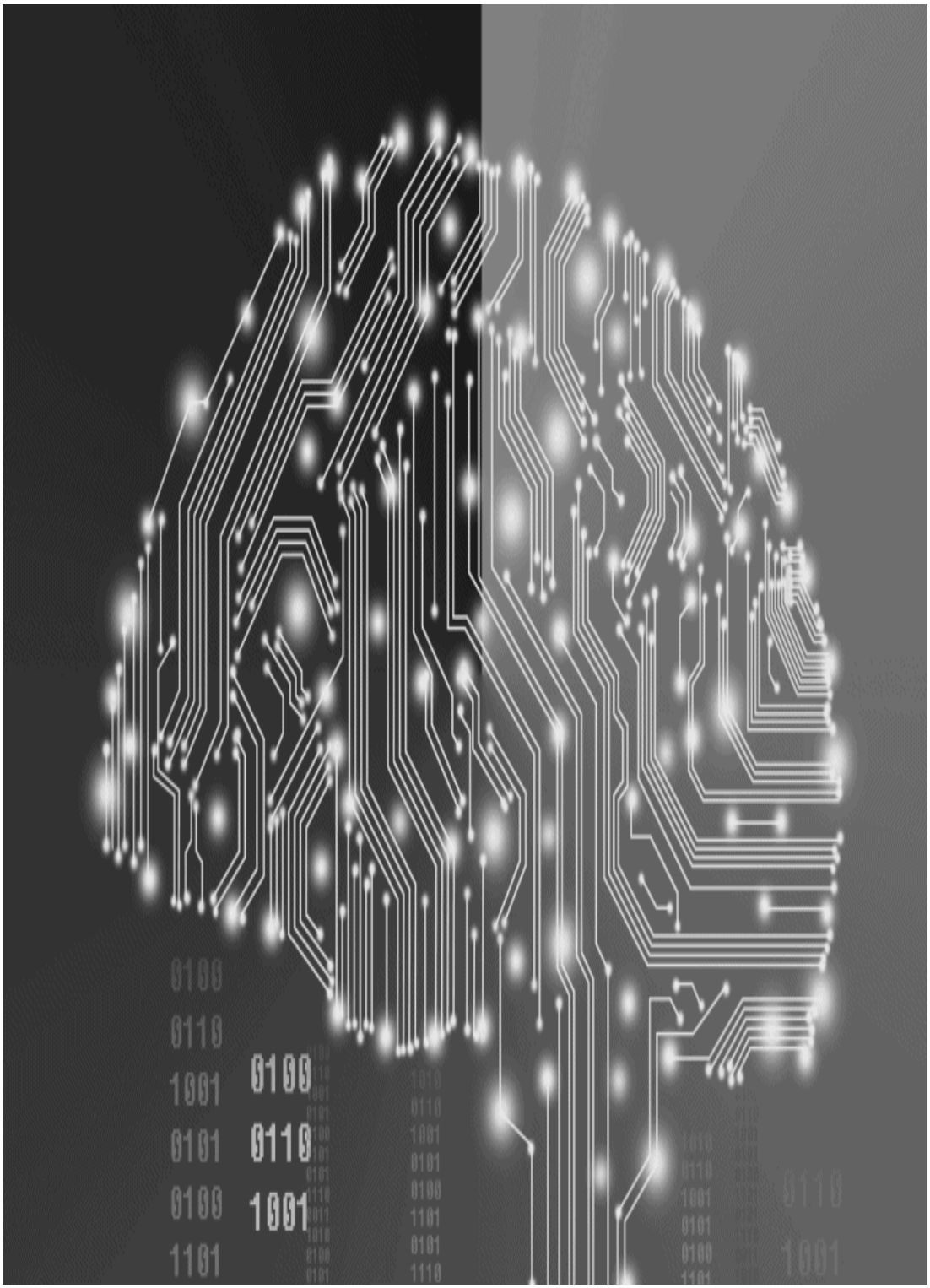
A malware program that replicates itself automatically across computer networks.



LEGAL CASES CITED

A&M Records, Inc. et al. v. Napster, Inc.
Alice Corporation Ltd v. CLS Bank
***Amazon.com**, Inc. v. **BarnesandNoble.com**, Inc.*
American Banana Co. v. United Fruit Co.
American Library Association v. Pataki
Apple Computer v. Franklin Computer Corp.
Apple, Inc. v. Samsung Electronics Co.
Arista Records v. Lime Group
Aschcroft v. ACLU
Bilski v. Kappos
Brookfield Communications, Inc. v. West Coast Entertainment Corp.
Brown v. Entertainment Merchants Association
Campbell v. Acuff-Rose
Diamond v. Diehr
Dow Jones & Company, Inc. v. Gutnick
eBay v. MercExchange, L.L.C.
Eldred v. Ashcroft
Elonis v. U.S.
Falmouth Firefighters Union v. Town of Falmouth
Gershwin Publishing v. Columbia Artists Mgmt.
Ginsberg v. New York
Griswold v. Connecticut
Harper & Row Publishers, Inc. v. Nation/Enters
Lexmark International v. Static Controls
La Ligue Contre Le Racisme et L'Antisemitisme et al. v.

Yahoo, Inc.
Lotus Development Corp v. Borland International Inc.
Mazer v. Stein
Metro-Goldwyn-Mayer Studios, Inc. et al. v. Grokster, Ltd. et al.
Miller v. California
Multnomah Public Library et al. v. U.S.
Oracle America Inc. v. Google Inc.
Panavision International v. Toeppen
People for the Ethical Treatment of Animals v. Michael T. Doughney
***Priceline.com**, Inc. v. Microsoft Corporation and Expedia, Inc.*
Planned Parenthood v. American Coalition of Life Activists
Reno v. American Civil Liberties Union
Schwarznegger v. Entertainment Merchants Association
Smyth v. Pillsbury Co.
Snyder v. Phelps
Sony Corp. of America v. Universal City Studios
Sony Computer Entertainment v. Connectix Corp.
Sporty's Farm v. Sportman's Mkt.
State Street Bank and Trust Co. v. Signature Financial Group, Inc.
United Christian Scientists v. Christian Science Board of Directors
United States v. Apple
United States v. Reporters Comm.
Universal City Studios, Inc. v. Remeirdes et al.
Utah Lighthouse Ministry v. FAIR
Video Game Dealers Assoc. v. Schwarzneger
Washington Publishing Co. v. Pearson



INDEX

A

B

D

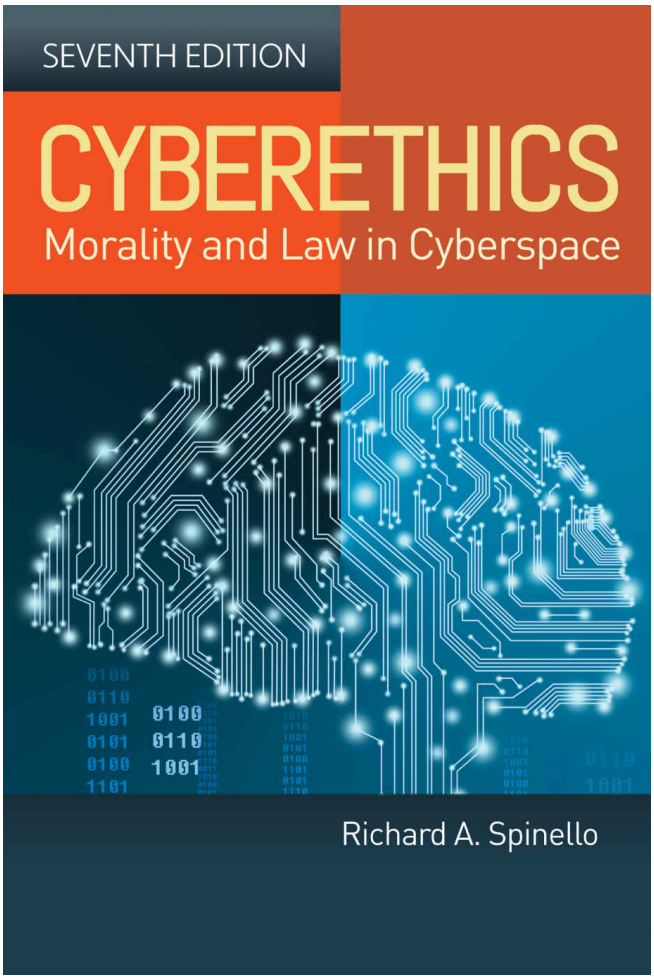
F

M

N

O

P


SEVENTH EDITION
CYBERETHICS
Morality and Law in Cyberspace
Richard A. Spinello