CYBERSECURITY ETHICS

An Introduction

MARY MANJIKIAN

Cybersecurity Ethics

This new textbook offers an accessible introduction to the topic of cybersecurity ethics.

The book is split into three parts. Part I provides an introduction to the field of ethics, philosophy and philosophy of science, three ethical frameworks – virtue ethics, utilitarian ethics and communitarian ethics – and the notion of ethical hacking. Part II applies these frameworks to particular issues within the field of cybersecurity, including privacy rights, intellectual property and piracy, surveillance, and cyberethics in relation to military affairs. Part III concludes by exploring current codes of ethics used in cybersecurity.

The overall aims of the book are to:

- provide ethical frameworks to aid decision making;
- present the key ethical issues in relation to computer security;
- highlight the connection between values and beliefs and the professional code of ethics.

The textbook also includes three different features to aid students: 'Going Deeper' provides background information on key individuals and concepts; 'Critical Issues' features contemporary case studies; and 'Application' examines specific technologies or practices which raise ethical issues.

The book will be of much interest to students of cybersecurity, cyberethics, hacking, surveillance studies, ethics and information science.

Mary Manjikian is the Associate Dean and an Associate Professor in the Robertson School of Government, Regent University, Virginia Beach, Virginia, USA. She is the author of three books, including *Threat Talk: Comparative Politics of Internet Addiction* (2013).

'This book is a bold and innovative synthesis of thinking from diverse yet interlinked disciplines. It is vital reading for scholars, policymakers, security professionals and organizational leaders. Manjikian's explication of the ACM Code of Ethics shows why it is a foundational concept for cybersecurity.'

Steven Metz, US Army War College, USA

'As cyber conflict, espionage and crime increasingly challenge nations and their citizens, Manjikian's *Cybersecurity Ethics* provides a comprehensive and needed addition to the cyber literature cannon. This work constitutes a robust framework for decisions and actions in cyberspace and is essential reading for policymakers, practitioners, and students engaging in the field of cybersecurity.'

Aaron F. Brantly, Army Cyber Institute, United States Military Academy, West Point, USA

'Mary Manjikian's introduction to cybersecurity ethics nicely links philosophy to practical cyber concerns of students, corporate and government information managers, and even cyber warriors. Complicated concepts are easy to understand and relevant to personal decision-making.'

John A. Gentry, Georgetown University, USA

'Dr Manjikian has done a masterful job of outlining ethical standards to the constantly evolving cybersecurity domain. This book is a vital reference for those who are concerned with ethics related to hacking, privacy, surveillance, and cyberwarfare in an ever-changing virtual environment that transcends boundaries and cultures and challenges the traditional ways that humans have dealt with each other. Ground-breaking and should be required reading for any serious cybersecurity professional.'

Keith Dayton, George C. Marshall European Center for Security Studies, Germany

'A great introductory text to complex conceptual and practical issues in cybersecurity.'

Heather Roff, Arizona State University, USA

Cybersecurity Ethics

An Introduction

Mary Manjikian

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2018
by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN

and by Routledge
711 Third Avenue, New York, NY 10017

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for this book has been requested

ISBN: 978-1-138-71749-7 (hbk)
ISBN: 978-1-138-71752-7 (pbk)
ISBN: 978-1-315-19627-5 (ebk)

Typeset in Times New Roman
by Apex CoVantage, LLC

To my husband Ara, whose paranoia in relation to social networking teaches us all to be more careful.

Contents

Figures

Boxes

Acronyms and abbreviations

ACM	Association for Computing Machinery
CAN SPAM Act	United States "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003"
CCTV	Closed Circuit Television
CFAA	Computer Fraud and Abuse Act of 1986
CIA	United States Central Intelligence Agency
CJEU	Court of Justice of the European Union
CIPS	Canadian Information Processing Society
CNA	Computer Network Attack
DARPA	United States Department of Defense Advanced Research Projects Agency
DDoS	Dedicated Denial of Service Attack
DHS	United States Department of Homeland Security
DOD	United States Department of Defense
ECPA	Electronic Communications Privacy Act
EC Council	International Council of e-Commerce Consultants
FBI	United States Federal Bureau of Investigation
FCC	United States Federal Communications Commission
FERPA	United States Family Education Rights and Privacy Act
GCHQ	United Kingdom Government Communications Headquarters
GPS	Global Positioning System

HIPAA	United States Health Insurance Portability and Accountability Act
IACC	International Anticounterfeiting Coalition
IACR	International Association for Cryptological Research
IEEE	Institute of Electrical and Electronic Engineer
IFPI	International Federation of the Phonographic Industry
IP	Intellectual Property
ISACA	Information Systems Audit and Control Association
ISC	International Information Systems Security Certification Consortium
ISIS	Islamic State of Iraq and Syria (a.k.a., ISIL—Islamic State of Iraq and the Levant, or just Islamic State)
LOAC	International Law of Armed Conflict
MLAT	Mutual Legal Assistance Treaty
NATO	North Atlantic Treaty Organization
NSA	United States National Security Agency
PbD	Privacy by Design
PET:	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
RFID	Radio Frequency Identification
SCOT	Social Construction of Technology
SOPA	Stop Online Piracy Act
Tor	The Onion Router anonymizing protocol
TRIPS Agreement	United Nations Agreement on Trade-Related Aspects of Intellectual Property Rights
WIPO	World Intellectual Property Organization of the United Nations

Preface

I first began thinking about what a cybersecurity ethics curriculum should contain several years ago, when a colleague approached me. He asked, "Besides the Tallinn Manual and international law, what should I be covering in cybersecurity ethics?" As I thought about how best to respond to his query, I realized that individuals who teach cybersecurity come from a variety of backgrounds – some from academic computer science or engineering, some from policy studies and some from the military. Some individuals may be philosophers by training while others may be practitioners in the computer industry who occasionally teach a course as an adjunct. Those of us who are not philosophers may be somewhat intimidated by the philosophical aspects of ethics, while those who are not computer scientists may be intimidated by the technical aspects of the conversation. How, for example, can we talk about the ethics of encryption without both understanding the technology, its limitations and its strengths, as well as the philosophical issues raised by this technology? Similarly, students who take a course in cybersecurity ethics may find parts of the material accessible and familiar, while other parts of this material seem arcane, confusing or even irrelevant.

I have created a resource designed to appeal to this broad spectrum of professors and students. This textbook assumes no prior study in philosophy, nor does it assume a high level of technical knowledge. I hope that it will help those in different fields of study to begin to have conversations across disciplinary boundaries – so that philosophers may talk to policy experts,

lawyers and engineers, as we all work together to model, create and practice ethical behavior in cyberspace.

An ethics course does not aim to teach you exactly what you should do in every ethical dilemma you will encounter professionally. However, as much as possible the focus in this course is on real-world situations that you might encounter in your day to day work. Part I of this text (Chapters 1, 2 and 3) are the most abstract but you will rely on the concepts introduced here throughout the course.

This book has four goals:

1. To provide you with ethical frameworks which you can use to make decisions regarding ethical issues you may face in your work;
2. To expose you to key ethical issues currently being discussed and argued about in relationship to computer security. These issues include: the problem of surveillance, issues of privacy, problems related to cyberwarfare, problems related to ownership of information and information piracy and issues related to deception in cyberspace;
3. To encourage you to make the connection between your own values and beliefs and the professional code of ethics you will rely upon in your work as a coder, computer forensics expert, cryptographer or other specialist within computer science; and
4. To encourage you to get involved in discussing these issues with your professional colleagues and with your professional organization (if you wish to join a project concerned with these issues, see the resources in the final section of this text).

This text contains eight chapters. Chapter 1 introduces the field of ethics, describing how it differs from either law or religion, and why it is still necessary when we have both law and religion. It lays out some of the differences and debates between philosophers as well. Chapter 2 introduces three stances which can be applied to thinking about ethics: virtue ethics, utilitarianism, and deontological ethics. Chapter 3 introduces the notion of

ethical hacking, the hacker code and the particular problem of penetration testing. Chapter 4 examines ethical issues related to privacy, while Chapter 5 looks at surveillance practices. Chapter 6 considers the problem of piracy and intellectual property theft. Chapter 7 looks at the specific ethics of cyberwarfare, and Chapter 8 concludes with some thoughts about what a Code of Ethics contains and what it means to practice professionalism in one's craft. It also looks towards the future, introducing some ethical issues which we can anticipate and begin to plan for now.

The book also contains three different types of added features. 'Going Deeper' features provide background on individuals like philosophers and add some background as we delve deeper into key concepts. 'Critical Issues' features look at stories which you might see in the news – from the ethics of WikiLeaks to the figure of Edward Snowden. 'Applications' features look at specific technologies or practices within computer science which raise ethical issues. These features provide a great conversation starter for in-class discussions and may also be used for creating discussion board posts for an online class.

Instructors and students are also encouraged to visit my own personal website: marymanjikian. com, where you will find updated features related to stories which are in the news. There you may also find PowerPoint resources to accompany each chapter. You may also contact me to share feedback about the book, which I will take into account in future updates. The website also contains a Discussion Forum where you can connect with others using this text.

Acknowledgments

I'd like to thank all of the people who inspired me to write this book and those who helped.

First, my thanks to Joe Saur at Regent University, who first asked me what I thought a good cybersecurity ethics course should include. This led me to begin compiling texts and references, as well as to begin thinking about what our students – both undergraduates and graduates – might need. My aim in this textbook is to 'meet students where they are' by not assuming that anyone is already a philosopher. My hope is that students will be able to see how a variety of fields – including moral philosophy, military ethics, legal ethics and the social sciences – have all contributed to the emergence of this new field of cybersecurity ethics. In addition, I hope that students can gain an understanding of how philosophy, domestic and international laws and norms and culture are all interrelated.

Thanks to my many colleagues at Regent – Young Choi from the College of Arts and Sciences, and Gary Roberts and Eric Patterson from the School of Government for asking me thought-provoking questions, as well as supporting my research efforts. I appreciate the support provided by my research assistants Jacob Stephens and Linda Waits-Kamau. I am particularly grateful to our fine library staff, including Sandra Yaegle, for help in tracking down obscure citations and materials.

I'm also grateful to Regent University's administration – including Jason Baker, Gerson Moreno-Riano and Douglas Cook – for providing me a Faculty Research Grant which enabled me to participate in conferences and meet with colleagues as I clarified my thoughts on these issues. In addition, I

am grateful to the Women in Cybersecurity conference, hosted annually, for the initial introduction to cybersecurity ethics issues and their importance both to policymakers and to society. Thanks also to Jennifer Jefferis of the National Defense University for the invitations to speak to our leading American and international military officers on the topic of cybersecurity. Such conversations were enlightening and helped to shape my thinking about this project.

In addition, I want to thank my editor, Andrew Humphrys, for his support of this project, as well as the two anonymous reviewers who saw an early version of this text and provided me with terrific feedback – including pointing me towards new texts with which I was unfamiliar.

Any errors in the text are of course my own.

Part I

1 What is ethics?

Learning objectives

At the end of this chapter, students will be able to:

1. Define philosophy and describe its aims as a field of inquiry
2. Define ethics and cybersecurity ethics and give at least three examples of practical ethical dilemmas which cybersecurity professionals encounter
3. Define epistemic community and profession and describe the ethical responsibilities of a professional
4. Describe the role of computer engineers in affecting political, social and economic life through making engineering decisions which have ethical consequences
5. Define major terms associated with the study of ethics
6. Describe the relationship between ethics, religion and laws

What is ethics?

Turn on the nightly news and chances are you will hear the word ethics bandied about. You might hear references to a parliamentary or congressional ethics inquiry, or you might hear about a public official being brought up on ethics charges. You might associate ethics with law enforcement, lobbying and corruption in government or investigations related to a person's character, marital fidelity or proclivity to accept bribes. You might think that ethics are only important to lawyers and public officials. But what does ethics then have to do with cybersecurity? Although these examples involve current events and law

enforcement, ethics is actually a broad academic discipline with historic roots, encompassing much more than what you see on the nightly news.

To begin our study, we define ethics and consider its academic origins and ways of studying ethics. Ethics is a branch of **philosophy**, an academic subject concerned with the fundamental nature of knowledge, reality and existence. Within philosophy, ethics considers people's values, where they come from, if they differ over time and from place to place and how people translate those values into behavior. Some of the values that philosophers consider include justice, equality and human rights.

In many of your other academic courses – in the sciences or social sciences – you may have encountered empirical methodology. In both the hard and soft sciences, analysts attempt to observe and measure things that exist in reality (from molecules to patterns of immigration) in order to formulate and test rules which both describe and predict likely results. They ask **empirical questions**, or questions based on observations which are measurable and observable. These questions might have a yes or no answer, or an answer that is a number. Thus, a social scientist like a sociologist might consider evidence that income inequality is increasing in the United States. He might ask whether or not there are greater gaps between those who are wealthy and those who are poor then there have been in the past and what the causes are.

An ethicist, who is a moral philosopher, in contrast, considers **normative questions** – questions which do not merely ask about what occurred, how often it occurred or about the size of a phenomenon, but questions which ask what we as humans *should do* in response to a phenomenon. Thus, an ethicist concerned with income inequality would ask whether people are less generous or community-minded then they were in the past, why that is and how one could encourage generosity. Both the ethicist and the economist study income inequality, but their methods, assumptions and research questions differ. Audi describes ethics as "the philosophical study of morality." He tells us that it asks question like "what ends we ought, as fully rational human beings, to choose and pursue and what moral principles should govern our choices and pursuits" (Audi, 1995, 284–285).

Where do ethics and values come from?

Do humans have an innate capacity to consider questions of right and wrong, and are there particular acts which every culture finds morally repugnant (like torture or infanticide) as well as others which all cultures regard as morally acceptable or worthy of respect? Are there universal values which all ethicists and cultures should view as worthy of pursuing, and which provide the foundational assumptions for ethical theorizing?

Philosophers called **objectivists** see the project of ethics as identifying the right thing to do or the right action to take morally. They believe that it is possible to identify solutions to ethical problems using reasoning and the tools of ethics. They believe that there are answers to ethical problems which can be identified and then enacted.

The Christian theologian Thomas Aquinas, who lived in the 13th century, referred to **natural law** in describing how values emerge. He believed that certain core values – such as the idea that all human life is worthy of respect – are found in all human beings. He believed that a creator had placed these 'laws' into every individual. Similarly, the school of ethics known as **Divine Command theory** proceeds from the assumption that a God who exists provides an objective set of ethical standards and that humans can behave ethically if they treat the fulfillment of these standards as their duty (Austin, No date; Brackman, No date).

However, one does not need to be religious to be an objectivist. In reaching back to ancient Greece, we can point to Plato's **Theory of Forms**, which suggests that we have an ideal in mind that we use in comparing a particular experience to that ideal. For example, if asking if something is beautiful, we compare it to an ideal standard of beauty which we hold and are able to access in our minds. The universal existence of these ideals thus suggests that there may be universal values which we all hold to, and which could provide the basis for some universal ethical values and recommendations.

However, not all ethicists are objectivists. A **moral relativist** believes that there is no one absolute position which is right or wrong. Instead, they argue that the most moral thing to do may be determined by your own subjective perceptions. That is, not everyone will see a moral problem in the same way. Some may emphasize one facet of a problem while others emphasize something different. And some relativists believe that our perception of ethical behavior depends on social conventions which vary from society to society. They point to

the fact that less than just 500 ago, many people found slavery socially acceptable. While it was still objectively wrong, many people did not yet see it that way. And they point out that virtues which were considered very important in Victorian England – like chastity or piety – are less important today in many parts of the world. (We should note here that this relativistic view is more commonly found among social scientists who write about ethics than it is among philosophers who practice ethics.)

Critics of this approach often use moral relativism in a negative sense, suggesting that it 'let's people off the hook' or does not hold them morally accountable for holding morally repugnant positions. They argue that we shouldn't overlook a culture's abuse of women or gay people through stating that 'according to their culture's understanding at this time, such behavior is moral,' for example. What's wrong is wrong, an objectivist would say.

In the information technology field, some analysts argue that cultures think differently about concepts like intellectual property. Chang argues that Asian nations have a collectivist culture which prizes equality and the good of the group as a whole while Western nations are more individualistic, prizing individual equity and fairness more than equality and the group good. She says that in Asian cultures, people might regard their activities as sharing rather than theft. She worries that any international code of information ethics which outlawed information sharing might seem like a foreign code imposed on citizens in Asian and developing nations, and that it would be difficult to get people to adhere to that code (2012, 421). However, Falk says that there is a difference between values which are universal and value opinions which are not (2005). She states that people might all subscribe to the same values, but that different cultures might order their preferences (or values opinions) differently. Thus, the fact that some cultures prize the value of sharing more than the value of honesty does not mean that the values are not universal, even though cultures might order their value preferences differently.

Ethicists also disagree about whether ethical values change over time. Moral relativists argue that as technologies advance, ethical values can change too. For example, they argue that many people today enjoy sharing on social media and no longer prize privacy as a right the way they did in the past. But objectivists argue that ethical decisions rest on core values which are stable, regardless of one's environment (Calman, 2004). Here we can consider a simple example: In

the past, doctors often had a paternalistic relationship with patients. The doctor was an authority who informed the patient of his diagnosis, his health prospects (prognosis) and his treatment. But today many patients come to the doctor's office having researched their condition online. They already know their diagnosis, prognosis and treatment options. Here a relativist might identify the emergence of a more cooperative model of medical ethics. But an objectivist would note that 'old' and 'new' doctors still share a common value – caring for and respecting patients. Thus, they would argue, the ethics have not changed, even in a new environment, because the core values endure.

In this text, we present both objectivist and relativist arguments in order for you to understand the range of ways in which people have considered cybersecurity ethics. However, the main document which we refer to throughout this text is the Association for Computing Machinery's (ACM) Code of Ethics. This document presents the values and ethics for the world's largest professional association for computer scientists. This Code of Ethics is regarded as universally applicable and relevant to all computer scientists internationally. It is not applied or interpreted differently in different cultures. This professional organization does meet from time to time to update this code, and it is possible that in the future it might be modified. However, it presents objectivist, not relativist, ethics.

The first ethicists

Although we introduced ethics by talking about questions of income inequality, ethics doesn't just consider wealth and poverty. Philosophers like Plato and Aristotle in ancient Greece asked questions like: what constitutes a good life? How can one live a good life – both individually and collectively – in concert with others?

Plato (born 428 BC; died 348 BC) first asked questions about the virtues or values that people should attempt to cultivate in their lives. Plato's published works, most of which appear as a series of Socratic dialogues, in which individuals come together to ask questions in order to arrive at new knowledge, help us to understand his ethics. He believed that human well-being (or ***Eudaimonia***) should be the goal of life and that individuals should cultivate and practice excellence (***arête***) in order to achieve it. He believed that individuals who lived a well-ordered life could work together to create a well-ordered

society. He rejected the idea that people should retaliate against others who harmed them, and argued that people were harmed in their souls when they committed injustices. Plato argued that individuals needed to be disciplined in their own lives, sacrificing individual wants and needs to create a good society.

However, ethical thinking has always been global. While the Western tradition of philosophy and ethics often treats Plato and the ancient Greeks as foundational, many cultures produced philosophers. Chinese thinking about information ethics draws upon Confucius, a scholar who lived in approximately 500 BC. Chang (2012) identifies loyalty, duty and respect for the ties one cultivates with one's community as values central to Chinese culture. African ethical thinking rests on tribal values like Ubuntu, or a concern for harmony within society and groups. (Chasi 2014.) All cultures ask questions about justice and equity, conflict and cohesion, but they may answer these questions in different ways.

As these examples show, ethics is really a label for two different types of ideas: rules for how one should behave or act in the world and rules for how one should regard the world, oneself and one's place in it and others. Ethics are thus both rules for action and statements about the attitudes people should have, what they should love or value, or what they should consider important.

An ethic thus rests on foundational assumptions about what is valuable and what is important. An **assumption** is a starting point for an argument that is taken as a given. The theorist may not require proof of his assumptions but instead may make a choice to accept that something is true or to behave as if it is true. For example, a journalist may adopt a journalistic code which states that the journalists' greatest responsibility is to produce news which is true or accurate. A doctor may adopt a medical ethic which states that her greatest responsibility is to her patient and that her responsibilities include working to cure her patient, alleviate his pain and to treat him with respect. In considering ethics and ethical decisions, the values on which an ethic rests may be explicit or clearly stated or implied. In evaluating different courses of action and deciding which one is the most ethical, it is thus important to be aware of the values and assumptions on which the ethic rests, whether or not the author whom you are reading spells these out directly or not.

The relationship between ethics and religion

As you may have noticed in considering Plato's thought, many ethical questions overlap with religious and legal questions. Ethical arguments establish a set of standards for behavior and practices, and also provide the grounding for describing what constitutes a breach of ethics by an individual or group. They set expectations for behavior and describe the conditions under which people can be held accountable for violating those expectations.

As Inacio argues, ethics requires **accountability**. Thomas Aquinas, a Christian scholar who wrote and taught in the Middle Ages, asked questions about the morality or ethics of warfare. He asked whether moral people could be soldiers and whether fighting to defend someone else was an inherently moral act. In Aquinas' mind, he was accountable to God; he believed that religion provided the basis for his values, and that God would ultimately judge him for whether or not he had acted morally in his lifetime. For those who are religious, accountability may be to their god.

For those who are not religious, accountability is often to society. We can identify ethical schools of thought associated with the world's major religions (including Buddhism, Confucianism, Judaism, Islam and Christianity) but we can also identify ethics based on the values of a community, including those of a profession. Within the environmentalist community, we encounter an ethics of deep ecology, a belief system that advocates for the rights of animals and living creatures like trees as being equal to that of humans. People involved in international development often make reference to care ethics, which considers the responsibilities which one group of individuals or states may have to others, including the idea that wealthy nations should demonstrate concern in regard to poorer nations and work for justice and equity. For military members, military ethics arguments – with an emphasis on military values like duty, honor and country – may resonate and help to inform their own thinking and practices as members of the military.

Luciano Floridi's (1998) **information ethics** considers people's obligations in regard to how they treat information – whether they engage in practices like deception or censorship and whether they hoard information or share it. His work has many implications for cybersecurity. Finally, we can see professional codes of ethics like the ACM (Association of Computer Machinery) and the IEEE

code of ethics for software engineers as sources of moral values. These two professional codes make it clear that information specialists are accountable to the public, whom they should seek to serve in their work.

The relationship between ethics and law

You might wonder why ethics matter when we have laws. Presumably, many ethical queries could be solved simply by stating that certain practices are wrong because they are illegal or criminal without delving further into the philosophy behind them. As long as I obey the laws, you might think, why should I think about ethics?

Indeed, some analysts follow this view in thinking about cybersecurity. Levy (1984) describes cyberethics violations as acts which depart from the norms of a given workplace and suggest that better socialization into workplace norms can effectively solve the problem of cyberethics violations. Similarly, Chatterjee et al. (2015, 55) define unethical information technology use as:

> … the willful violation – by any individual, group or organization – of privacy and/or property and or/access and /or accuracy – with respect to information/information goods resident within or part of an information system, owned/controlled by any other individual group of organization.

They describe an act as unethical if it breaks rules or causes harm to others – even if the individual who carried out the actions feels that he or she was acting ethically or in line with his or her convictions. That is, they argue that rule-breakers always act unethically. They believe that an outside observer can decide whether someone has acted ethically by comparing their behavior to an objective standard like an organization's professional code of conduct. (See Appendix A for the ACM Code of Ethics.)

But there are good reasons why we need to learn about ethics, even when laws exist covering the same questions.

First, some analysts argue that ethics precede laws, or that laws are often formulated based on existing ethical thinking. MacDonald (2011) argues that, traditionally, society's codes of law have rested on foundational understandings about what constitutes a moral action, what an individuals' obligation to others is

and what actions society should regulate and to what end. We can look all the way back to the first written legal code, the Code of Hammurabi, written down in ancient Mesopotamia, almost 2000 years ago, to see that societies had understandings of what constituted justice, fairness and acceptable retribution, which then became codified into laws.

Today, Koller (2014, 157) refers to **conventional morality**, or "those laws or rules which hold sway in a group, society or culture because they are acknowledged by a vast majority as the supreme standards of conduct," as the basis for ethical behavior in a society. For example, conventional morality sets the expectation that parents should be willing to care for their children and even to make personal sacrifices in order to provide for them. Or we might expect that a doctor will care for patients – even in situations where he may not be formally on duty, like at a roadside accident; and even when he might not be paid for his services. Most people believe that doctors should ensure health in society and that they have greater obligations in this regard. (For example, we expect them to undertake personal risks in carrying for contagious patients during an epidemic.)

Such moral understandings are often codified into laws. Here, we can refer to **normative validation**, or the idea that people are more likely to conceptualize of an activity as morally wrong if it is also legally wrong. (D'Arcy and Deveraj, 2012, 1100). Thus, we are not surprised if parents who fail to care for children or doctors who fail to care for patients are the subject of legal proceedings – as they are seen to have violated both conventional morality and the law.

But while MacDonald (2011) sees laws as reflecting or codifying a preexisting and ethical consensus, other thinkers have suggested that laws and codes of behavior provide the basis for establishing trust between citizens in a community, and that it is only in a stable, established community where people trust one another that ethics can then develop. The German theorist Immanuel Kant (see Going Deeper: Immanuel Kant in Chapter 2) espoused this view, that law necessarily preceded the establishment of ethics since law provided the necessary constraints on human action that made ethical behavior possible.

This "chicken or the egg problem" (whether law precedes ethics or ethics precedes laws) appears in current debates about the foundation of ethics in cyberspace – a place where matters of laws, codes of conduct and even legal jurisdictions have not yet been settled. Some analysts believe that norms and values, and ultimately legal understandings, will emerge organically in

cyberspace over time. That is, at some point, everyone will be convinced of the rightness of certain values and norms in cyberspace which will be regarded as universal. Myskja (2008) argues that strong legal regimes need to be set in place which spell out the rights, responsibilities and constraints on human behavior in cyberspace. Once that is done, he argues, ethical understandings will naturally emerge.

But others believe that individuals, corporations and even nations need to intervene in order to build this consensus since it will not emerge organically. Indeed, some believe that given the global and multiethnic nature of cyberspace, it is possible that a consensus on values may never emerge. Luciano Floridi (2013), in his seminal work on the ethics of information calls for the creation of ethical norms and understandings in cyberspace while technology is still advancing so that the two develop in conjunction with one another. He refers to this process as 'building the raft while swimming,' proposing an information ethics which engages with current moral and judicial understandings and also anticipates and responds to problems which might arise later. Similarly, Brey (2007) argues that while legislation may be informed by ethical principles, laws by themselves are insufficient to establish or substitute for morality. Individuals still need to think of themselves as moral decision makers, and to consider their actions and how they will be perceived and affect others.

Next, in the real world and in cyberspace, laws, morality and ethics do not always line up neatly. Koller (2014) speaks of **moral standards** – which differ from laws in that individuals can decide whether or not to conform to them, unlike laws which are seen as having sway over everyone who resides in a region or is a citizen of the region. He notes that moral standards are often seen as having greater force than law and as taking priority over laws and social customs when there is a clash or contradiction between them.

Throughout history, individuals and groups have opposed laws which they regarded as unjust or unethical. Mahatma Gandhi opposed British imperialism in India and fought for India's independence while Martin Luther King opposed discriminatory racial laws in the US. Each man felt an ethical duty to oppose unjust laws. Here we see that ethics is related to religion and law but does not always neatly parallel either one. Ethical arguments may contradict both faith systems and laws – and frequently do.

In considering cybersecurity, many activists who have engaged in DDoS attacks against corporations, terrorist groups or authoritarian governments regard their activity, called **hacktivism**, as a form of civil disobedience which they are performing against unjust laws or decisions. In 2006, German activists carried out DDoS attacks against Lufthansa, Germany's airline, to protest the fact that the airline was cooperating in the deportation of asylum seekers. The legal verdict upheld the finding that this was a form of civil disobedience (Morozov, 2010).

Thus, cybersecurity practitioners need to be able to think ethically and critically. One difference between a profession and a mere job is that professionals often work independently, without a lot of supervision. And professionals are expected to be able to go beyond merely reading a manual or applying a technique. They need to be able to think critically when the rules are unclear or ambiguous or when more than one set of rules apply (Whitehouse et al., 2015, 3).

Box 1.1 Going deeper: Lawrence Kohlberg

How do people make moral decisions and how do they acquire the capacity to do so? This is the question that fascinated psychologist Lawrence Kohlberg. Kohlberg is best known for his theory on moral development. In this theory he suggests that we grow in our capacity to make moral decisions, just as we develop in our intellectual and physical abilities. In his work, he built upon the ideas of the French theorist Piaget who had explored how young children pass through stages of intellectual and social development. Over time, children begin to take on more complex reasoning tasks, to perform sequences of actions and to plan.

Kohlberg broke moral reasoning into three stages. In stage one, young children are rule followers. They recognize situations where they are not in authority and where they must obey rules either because someone else compels them to or because they feel a sense of attachment or duty to the person who makes the rules. This stage is referred to as the stage of **pre-conventional morality**.

In stage two (which begins at about age nine), children understand rules as being about society, rather than exclusively the province of one person.

They may follow rules because they feel a duty as members of a society. They may also enjoy enforcing rules and feel that they have a stake in making sure that everyone follows rules. This is referred to as the stage of **conventional morality**.

In stage three, beginning at about age 11, Kohlberg (1981) suggests that individuals begin to think in a more nuanced way about rules. They may recognize some rules as being just, but might also make an independent decision to appeal or even to break a rule that they see as unjust. This stage is termed the stage of **post-conventional morality**, since individuals may sometimes violate conventions and norms in search of what they see as a greater good. In Kohlberg's class example, an individual whose wife was dying but who could not afford the medicine which could save her might decide to steal the medicine from the pharmacy since saving his wife was a more important goal than obeying the rules about not stealing.

Kohlberg's work helps us understand the relationship between law and ethics. Using his framework, we expect adults with a developed critical reasoning capacity to distinguish between good and bad rules, and to decide whether following a rule is appropriate in a particular situation. The most ethical solution to a problem is not always the most lawful, and law alone is not a sufficient guide to ethical decision making.

In looking at the behaviors of ethical hackers (see Chapter 3), we see that often hackers argue that they subscribe to a different or higher set of ethics than those of conventional morality. Hackers have, for example, suggested disregarding rules and laws prohibiting the sharing of copyrighted files, programs and information. Here, hackers argue that making information freely available to all who need it is a higher goal, since it facilitates intellectual progress in their field. However, while hackers might see themselves as engaged in post-conventional morality thinking, others might regard these activities simply as criminal or deviant behavior (Pike, 2013, 70).

Some analysts (Regalado, 2013) have argued that the actions of American defense contractor Edward Snowden in spring 2013 – when he released classified documents to the press which showed that the US National Security Agency was engaged in surveillance of American citizens – can be explained by Kohlberg's theory. Regalado (2013) argues that Snowden

decided to transcend obedience to the US government in order to obey a higher set of ethical concerns, including a belief that Americans should have the right to carry out their affairs without the threat of government surveillance.

Kohlberg's theory also suggests that hackers who violate laws know the laws but knowingly and willingly choose to oppose them. Therefore, programs which merely seek to better educate individuals about these laws will not be sufficient to end practices like hacking and piracy (King and Thatcher, 2014).

Sources

Gilligan, Carol. 1998. *In a Different Voice: Psychological Theory and Women's Development*. Cambridge, MA: Harvard University Press.

Kohlberg, Lawrence. 1981. *The Philosophy of Moral Development: Moral Stages and the Idea of Justice*. New York: Harper and Row.

King, Bernadette, and Thatcher, Andrew. 2014. "Attitudes Towards Software Piracy in South Africa: Knowledge of Intellectual Property Laws as a Moderator." *Behavior and Information Technology* 33(3): 209–223.

Pike, Ronald E. 2013. "The 'Ethics' of Teaching Ethical Hacking." *Journal of International Technology and Information Management* 22 (4): 67–78.

Regalado, Antonio. 2013. "Cryptographers Have an Ethics Problem" *MIT Technology Review*. September 13. Available at www.technologyreview.com/s/519281/cryptographers-have-an-ethics-problem/. Accessed December 9, 2015.

Introducing cybersecurity ethics

Within the field of computer ethics, many analysts ask questions related to cybersecurity. We should note here that cybersecurity actually has two different definitions. Social scientists, including policy analysts, often define cybersecurity as those aspects of computer security specifically related to national security issues, like cyberterrorism and protection of national assets, like those belonging to the Department of Defense. These practitioners consider the political, economic and social vulnerabilities created by vulnerabilities in the cybersphere.

Nissenbaum (2005) describes these individuals as concerned with three types of dangers: the ways in which connectivity allows for the creation of social disruption (including the ability of hate groups to organize); the threat of attack on **critical infrastructures** and threats to the information system itself through attacks on that system.

However, individuals in technology fields define cybersecurity more specifically, referring to practices and procedures used to secure data and data systems in cyberspace, regardless of who the systems belong to or are used by (Brey, 2007). Here, cybersecurity protocols refer to technologies like encryption, as well as procedures like scanning for viruses, making sure a corporation and its employees are well-versed in cyberhygiene practices and that they are not vulnerable to vectors of cyberattack like phishing or social engineering. Brey further distinguishes between system security and data security. System security refers to securing hardware and software against programs like viruses. Data security or information security refers to the protection of information as it is stored in a system or transferred between systems (Brey, 2007, 23).

The main professional organization associated with cybersecurity, the Association of Computing Machinery (ACM) Joint Task Force on Cybersecurity Education, defines cybersecurity as:

> A computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics and risk management in the context of adversaries.
>
> (Burley et al., 2017, 683)

In this text, we consider cybersecurity ethics. Cybersecurity ethics are **professional ethics**, providing contextualized, specific knowledge to a group of practitioners who share certain characteristics (Didier, 2010). Each profession asks "How can I most ethically enact my profession and the project of my profession, given the constraints which I face?" Those who work in cybersecurity form an **epistemic community** – they have had similar training, share a specific vocabulary and set of ideas and belong to the same professional organizations. (see Going Deeper: What is an Epistemic Community?) Over the years, many

professions have developed their own ethical codes which delineate the values and understandings associated with a particular occupation. The code of ethics document lays out a list of key organizational values and describes both the values which practitioners should subscribe to as well as a vision for how they should view their job and role in society. The code of ethics is both a statement of the organization's values and often a fairly detailed guide to practical ethics, laying out specific steps which practitioners should take in regard to ethical issues in a variety of situations. We can distinguish between abstract questions like "What is justice?" and more practical ethical queries like "Should I report a professional colleague for this type of misconduct?"

Box 1.2 Going deeper: what is an epistemic community?

An **epistemic community** is "a network of experts who persuade others of their shared norms and policy goals by virtue of their professional knowledge" (Cross, 2015, 91). Medical personnel, social workers, educators and military personnel, for example, can all be seen as epistemic communities.

All social workers have a similar educational background (usually a Master's in Social Work), perform similar tasks in their daily employment, and possess a shared set of beliefs about the importance and utility of social work. Epistemic communities share knowledge, concepts and a common language for problem-solving in their field of endeavor – but they also include people who share similar values. Social workers generally believe that societies function better when all members of society are taken care of, and that societies should take care of all citizens, including those who are least able to care for themselves. The professional organizations, professional organization periodicals and academic journals of a group like social workers thus use a shared language, rely on shared concepts and demonstrate a shared set of normative commitments and often policy stances.

Epistemic communities are important for two reasons: First, these networks of experts can work together both formally and informally to

define the norms of their own professional conduct. For example, the American Medical Association defines the norms and values governing doctor-patient relationships including the need for doctors to maintain the confidentiality of patient information. Second, a network of experts can articulate and define the norms and values which they believe society and policymakers should adopt in relation to these issues. Thus they can influence society politically through helping to create and shift a debate about a particular policy issue. For example, the American Psychological Association and the American Medical Association weigh in as organizations on policy debates regarding issues like the right of all citizens to have access to medical care; the moral unacceptability of torture (Miles, 2006) and organ trafficking (Efrat, 2015) and whether homosexuality should be viewed as a mental illness, a lifestyle choice or a normal variant of human sexuality. Epistemic communities can help define a policy problem, including providing the ideas and concepts which should be used in considering the problem.

Epistemic communities are thus described as **norm entrepreneurs**, since they often invent and then publicize new norms, persuading others to adopt them as well. Epistemic communities can come together to make a difference – through adopting rules and conventions or testifying in international bodies like the United Nations or International Criminal Court on ethical issues and policies that affect the world around them. Climatologists have weighed in regarding the existence of climate change and the steps which they feel states and international actors need to take in regard to these problems (Gough and Shackley, 2001; Haas, 1992). Biologists and chemists have pushed for an international treaty which would outlaw the use of biological and chemical weapons in warfare (Manjikian, 2015). Nuclear experts have helped persuade policymakers to adopt nuclear arms control treaties (Adler, 1992).

Are cybersecurity experts an epistemic community? Professionals have shared expertise – usually acquired through a Master's in Cybersecurity. We can identify shared professional organizations, professional periodicals and academic journals concerned with cybersecurity issues. Cybersecurity policy groups have also testified in Congress and attempted to influence legislation.

But what shared norms and ethics do cybersecurity practitioners share? A group must share a consensus amongst itself before it can go on to influence others outside the group (Haas, 1992). Tim Stevens (2012) argues that cybersecurity practitioners share concerns about cybercrime, the threat of cyberwar and cyberterrorism.

However, at present, it appears that not everyone who works in cybersecurity thinks the same way, for example, about the need to safeguard user privacy; the role of surveillance in preserving security; and the dangers presented by piracy of materials found online.

In this textbook, you will encounter examples of the debates which exist in the area of cyberethics, and you may begin to think about what an epistemic community of cybersecurity experts may look like in the future. What values will this community share and how will it then go on to influence policy?

Sources

Adler, E. 1992. "The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control." *International Organization* 46(1): 101–145.

Cross, Mai'a. 2015. "The Limits of Epistemic Communities: EU Security Agencies." *Politics and Governance* 3(1): 90–100.

Efrat, Asif. 2015. "Professional Socialization and International Norms: Physicians Against Organ Trafficking." *European Journal of International Relations* 21(3): 649–671.

Gough Clair, and Shackley, Simon. 2001. "The Respectable Politics of Climate Change: The Epistemic Communities and NGOs." *International Affairs* 77(2): 329–346.

Haas, Peter. 1992. "Banning Chlorofluorocarbons: Epistemic Community Efforts to Protect Stratospheric Ozone." *International Organization* 46(1): 187–224.

Manjikian, Mary. 2015. *Confidence Building in Cyberspace: A Comparison of Territorial and Weapons-Based Regimes*. Carlisle Barracks, PA: United States Army War College Press.

Miles, Stephen. 2006. *Oath Betrayed: Torture, Medical Complicity and the War on Terror*. New York: Random House.

Stevens, Tim. 2012. "Norms, Epistemic Communities and the Global Cyber Security Assemblage." March 28. Available at http://www.e-ir.info/2012/03/27/norms-epistemic-communities-and-the-global-cyber-security-assemblage/

But not all professional ethical codes are alike. They may be largely aspirational – laying out standards which practitioners should regard as ideal behaviors – or they may be regulatory – laying out both standards and specific penalties which practitioners face if they do not comply with the profession's ethical code. Codes also differ in terms of their specificity. A **normative code** can spell out general principles (i.e. specifying that a lawyer, physician or teacher should attempt to treat all clients equitably and fairly) or go into great detail about the behavior expected (i.e. stating that physicians cannot refuse patients treatment on racial, gender, national or other grounds; Gotterbarn, No date). A code can thus inspire members and create a unity of purpose, but it can also – depending on its regulatory power and level of detail – elicit member compliance to standards by requiring adherence for those wishing to enter the profession, and revoking privileges and licenses for those who are found to have violated the standards. In some professions a member may face professional censure or penalties for a legal or ethical breach. Often the two categories of breaches overlap. For example, a physician who sells a medical prescription commits both a legal and an ethical breach. He would face legal charges and in addition, the state medical board would revoke his medical license, rendering him unable to practice medicine.

Not all professions have the ability or desire to engage in this regulatory or policing function of their member's character and ethical behavior – instead laying out an ethical code which is aspirational or inspiring, and which does not have strong measures for regulation or compliance. Gotterbarn suggests that as a new profession evolves and becomes more professional, its code of ethics will usually move from being merely aspirational to being more specific and more regulatory. In the fields of cybersecurity, we can identify several sets of ethical codes which vary in their specificity and their regulatory potential. The Canadian Information Processing Society (CIPS) Code of Ethics and Standards of Conduct is regarded as highly specific, and it includes measures for filing a complaint if a member does not adhere to the code. The Association of Computing Machinery Code of Ethics, developed in 1972 and revised in 1992, and in use throughout the world, is regarded as a code of conduct as well as a code of ethics, since it has three sections: canons or general principles; ethical considerations; and disciplinary rules, which involve sanctions for violators.

Because cybersecurity experts work in a variety of different settings – including hospitals, corporations, government offices and in the military – throughout this text, we draw upon other sets of professional ethics as well. Cybersecurity ethics is thus an interdisciplinary practice incorporating ideas drawn from fields of study including medical ethics, military ethics, legal ethics and media ethics (see Going Deeper: The Hippocratic Oath for more on medical ethics). In addition, cybersecurity ethics often draws upon ideas from ethics of technology. The **ethics of technology c**onsiders how new technologies can be shaped and harnessed to contribute to our living a good life.

Box 1.3 Going deeper: the Hippocratic Oath

The Hippocratic Oath is believed to have been written around 400 BC. It is named after Hippocrates, the Greek 'father of medicine' but no one knows who actually wrote it. Now nearly 2500 years later, almost all doctors in the United States receive a modern version of this oath as part of their medical school graduation ceremony. The oath serves as a code of conduct and unifying statement of the ethics of the medical profession for all doctors. In it, doctors promise to 'do no harm,' not to fraternize with their patients, to respect their patients' privacy and confidentiality and to treat them with respect.

Hippocratic Oath: modern version

- I swear to fulfill, to the best of my ability and judgment, this covenant:
- I will respect the hard-won scientific gains of those physicians in whose steps I walk, and gladly share such knowledge as is mine with those who are to follow.
- I will apply, for the benefit of the sick, all measures [that] are required, avoiding those twin traps of overtreatment and therapeutic nihilism.
- I will remember that there is art to medicine as well as science, and that warmth, sympathy, and understanding may outweigh the surgeon's knife or the chemist's drug.

- I will not be ashamed to say "I know not," nor will I fail to call in my colleagues when the skills of another are needed for a patient's recovery.
- I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know. Most especially must I tread with care in matters of life and death. If it is given me to save a life, all thanks. But it may also be within my power to take a life; this awesome responsibility must be faced with great humbleness and awareness of my own frailty. Above all, I must not play at God.
- I will remember that I do not treat a fever chart, a cancerous growth, but a sick human being, whose illness may affect the person's family and economic stability. My responsibility includes these related problems, if I am to care adequately for the sick.
- I will prevent disease whenever I can, for prevention is preferable to cure.
- I will remember that I remain a member of society, with special obligations to all my fellow human beings, those sound of mind and body as well as the infirm.
- If I do not violate this oath, may I enjoy life and art, respected while I live and remembered with affection thereafter. May I always act so as to preserve the finest traditions of my calling and may I long experience the joy of healing those who seek my help.
- Written in 1964 by Louis Lasagna, Academic Dean of the School of Medicine at Tufts University, and used in many medical schools today.
- Found at: www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html

Ethics in policy

As we see in considering subfields like medical ethics, an ethical framework lets us ask questions about an individual's ethics, the ethics of a profession, and the ethics of a society or group of people. An ethic may refer to a set of rules about what an individual should value (as Plato believed) and how an individual should

behave, but might also refer to upholding the values and beliefs associated with one's profession or community or even one's nation.

As we will see throughout this text, sometimes ethical concerns overlap with policy concerns. An ethical stance may lead individuals to advocate for specific laws and policies. Thus, a US government official who works on refugee issues may wish to choose the right and just response, but may also face questions about which solutions are politically feasible, which are legal and which will require substantive changes to legislation and policies.

In this textbook, we focus primarily on the first two levels of analysis – the ethics of the individual computer practitioner and the ethics of the profession of cybersecurity. We will not focus on the ethics of the technology itself, nor on the ethics of companies or corporations like Google, Microsoft or the Department of Homeland Security. We will not consider legislative or policy changes or dwell on the morality of specific policies, such as US national security policy in cyberspace.

Instead, beginning in Chapter 2, we introduce frameworks for asking ethical questions. We also provide you with information on your own professional obligations as a member of the cybersecurity profession. However, in the next section, we look at the larger question of the ethics of technology itself, in order to provide you with the necessary background to move forward in thinking about your own ethics in this field.

The history of computer ethics

Computer ethics is an interdisciplinary field. Norbert Weiner was the first computer scientist to pose ethical questions about the field. A mathematics professor at the Massachusetts Institute of Technology in the 1950's, he asked, for example, whether information was matter or energy. He suggested that computing technologies differed in fundamental ways from other technologies, and spoke about a future of 'ubiquitous computing' in which we would live in a world surrounded by computers which both collected data about us and provided us with data continuously (in this way anticipating what we now refer to as the Internet of Things). His work, considered very revolutionary at the time, provided a basis for studies today in fields as diverse as library ethics, journalism ethics and medical ethics.

Other philosophers added to the debate later, shaping it in new directions. In 1976, Walter Maner posed questions about technology and its use in medicine. He argued that developments in computing, like connectivity, had created new, unique ethical problems that had not existed before. His colleague at Old Dominion University, Deborah Johnson, disagreed. In her work, she argued that computers might give preexisting ethical problems 'a new twist,' but that existing philosophical ideas could be shaped and applied to these new and emerging issues. Johnson went on to write the first textbook in computer ethics (Bynum, 2015).

In 1976, Joseph Weizenbaum, an MIT computer scientist, published the landmark book *Computer Power and Human Reason*. He had developed a computer program called ELIZA which simulated the interactions a person has in conversing with a psychotherapist. He began thinking about how humans interact with computers and the ethical issues which this raises after observing the attachments which his students and others developed to ELIZA (Bynum, 2000).

James Moor moved the '**uniqueness debate**' along with the publication of an article in 1985 in the journal *Metaphilosophy*. He argued that computers actually allowed humans to go beyond their previous human abilities to do things that previously would have been impossible (i.e. performing mathematical calculations at superhuman speed). As a result, he argued, a computer specialist might find himself or herself in a situation where a **novel problem** or **policy vacuum** emerges for which there is not yet any clear law or even ethical framework. For example, in recent years, developers have created websites for those who wanted encouragement to adopt an anorectic lifestyle; for individuals who wished to receive support from others before engaging in the act of committing suicide; or for the sale or resale of illegal drugs. In each of these situations, the crime was so new that it was unclear what, if any, existing legal statutes applied. Today, novel problems exist in regard to ownership rights of materials which are being held in cloud storage, data being created through the Internet of Things, and monetary issues arising from the use of digital currencies like Bitcoin. Scholars and analysts are also attempting to formulate rules regarding whether an individual who has a warrant to collect data also has the right to store that data, compile that data into some form of aggregate file – with or without removing identifying information – or pass on that data including selling it, sharing it or giving it to the government.

In situations like technology lags, **grey areas** or unjust laws, a coder or security professional needs to hone his or her own ability to think ethically, so that they can act independently or even provide guidance to others within their organization or corporation. (Note here that in this course when we address these grey areas, if laws are addressed the assumption is that the student is an American student in an American classroom. Most references are to US law – for example in relation to copyright – and the assumption is that the norms prevalent in the United States in regard to these issues are the default. We are also not necessarily advocating that readers take particular actions – including those that would violate any type of laws or rules within their organizations, or locally, on the state level or on the federal level.)

Today, many professional organizations and publications consider information ethics and the professional ethics which must evolve to accompany thinking in this field. We can point to Donald Gotterbarn's Software Engineering Ethics Research Institute (SEERI) at East Tennessee State University as well as to the annual ETHICOMP conference on Ethical Computing. Gotterbarn's emphasis on the development of professional ethics is reflected in the creation of a Code of Ethics and Professional Conduct in 1992 by the Association of Computing Machinery, and the creation of licensing standards through the Computer Society of the IEEE (Institute of Electrical and Electronic Engineers). Many of these initiatives were international in scope, reflecting the understanding that computer ethics are universal and not specific to a particular nation, belief system or type of educational institution.

Information ethics is a diverse and interdisciplinary field in which scholars from sociology, anthropology, psychology, engineering and computer science, business and the law come together to consider how individuals think about computers, how they interact with them and what their relationships are with computers – even what their emotions are (Sellen et al., 2009, 60). Libraries attempt to clarify the credibility of internet sources while those involved in local, state or national government discuss equitable access to internet resources to questions about privacy and secrecy. Information ethics can also include media ethics and increasingly the ethics of information management (i.e. how corporations and government agencies treat your data). Ethical thinking regarding whether and under what circumstances information generated or stored should be regarded as private affects medical practitioners, teachers and

professors, lawyers and others. It may be the subject of policymaking both in government and in associations and organizations.

However, some questions which computer ethics specialists ask also overlap with a larger domain known as **philosophy of technology**. Philosophy of technology is a relatively new field of study in comparison to other branches of philosophy which can be traced back to Confucius and the ancient Greeks. However, even the ancient Greeks asked questions about the nature of scientific knowledge, and the 19th-century thinker Karl Marx asked questions about labor, machines and their relationship with human freedom (Scharff and Sudek, 2013). Philosophers in this field practice descriptive or comparative, rather than normative ethics. That is, they study and describe how people develop their beliefs about technology rather than asking questions about what we 'should do' in relation to new technologies.

One of the main questions which philosophers of technology ask is whether technology automatically enables human progress and the achievement of human flourishing. Here, they ask whether technologies are deterministic, proceeding in a linear fashion through history and necessarily arriving at a specific end. Philosophers of technology ask questions like:

- How can we understand the relationship between humans and machines?
- Do humans always control machines or do machines also have the ability to shape the natural world and human behavior?
- Does technology enable human freedom through changing man's relationship to his labor and the products of his labor?

As you consider computer ethics, you may encounter some **policy arguments** which talk about what citizens and policymakers should or should not do in relation to information technology in general and cybersecurity in particular. These arguments may sound like moral philosophy arguments since they are normative, but often they are not based on moral philosophy but instead on philosophy of technology principles. Writers often make reference to specific *qualities* of the internet or internet communications, and imply that it is a decision maker's moral duty to seek a solution to a dilemma which best *preserves that quality*.

For example, Schejter and Yemini (2007, 170) argue that the internet enables political participation by a wide variety of people from different walks of life. They write:

> It is the unique position of the Internet, and in particular the potential of broadband access, that renders it a forum that enables the participation of all, and not a closed community in which rules of seniority, aristocracy, and exclusivity may apply. Consequently, it creates the need for rules that negate all forms of tyranny and oppression, whether initiated by government or by dominance through wealth.
>
> (171)

Thus, they imply that the *technology itself* creates goods like justice and equity – rather than the actions of specific people, like designers or users. Thus, they argue, anyone (like an engineer or a bureaucrat) who attempts to implement proposals which would fundamentally alter the character of this technology – through requiring that users register or pay a fee, for example – is behaving unethically.

Here we can consider policy arguments about the desirability and advisability of governments and corporations adopting a principle of net neutrality. **Net neutrality** is the principle that all information which travels over the internet should be treated in the same way, including traveling at the same speed – regardless of its content or its origination point. A policy of net neutrality would mean that it was not possible for some people to pay more to have their information travel by 'express' and that medical information, for example, would not automatically travel and load faster than someone else's cartoons or celebrity gossip.

You might encounter an argument suggesting that implementing controls over what type of information can travel and what speed is wrong because it somehow contravenes the nature and purpose of the internet itself. Such writers might build an argument like this:

1 Freedom of speech is a constitutional right in the United States, and is recognized internationally as a right through the United States.
2 The internet is – or is meant to be – a place where democratic discourse occurs.

3 Therefore, it is people's (and government's) ethical and moral duty to take steps to preserve the real character of the internet through opposing actions which seek to regulate people's activities on the internet through the use of differential speeds for information to travel at.

Although this sounds like an argument about ethics, it is based not on moral philosophy but rather on stances and assumptions drawn from philosophy of technology – including those ideas about what a technology means, whether or not it has embedded values, and where those values come from. When you encounter an argument about what people *should do* in cyberspace, which references the nature of the internet itself (rather than the character or values of the decision maker, the outcome of the decision or the impact which it might have on citizens), you should understand that this is an argument not about moral philosophy but about philosophy of technology. In the social sciences in particular, analysts may mix together moral philosophy and philosophy of technology arguments. For this reason, you need to be familiar with three major stances within philosophy of technology which are discussed in the following Going Deeper and Application articles – so that you may identify them when they occur as assumptions in articles about ethics.

Box 1.4 Going deeper: do tools have embedded values?

Every day you probably use a variety of tools to carry out many functions – chopping vegetables, looking up facts on the internet or working in your garden. But this question – what does a tool represent, what does a tool do, and who or what decides what a tool will represent and do – are contentious philosophical questions. We can identify three answers to the question: "who decides what a tool will represent or do?"

The first view is that of **technological determinism**. In this view, humans have only a limited amount of **agency** or free will in deciding how a technology will be used. Instead, adherents of this view may speak about how tools can make us do certain things. You have probably encountered this argument in your daily life. Individuals suggest that social media is

changing how we communicate with one another, or that the availability of birth control led to changes in the ways in which humans think about their sexuality, including marriage and relationships. In the most extreme version of this view, technologies can evolve and reach a particular state, and humans have little control over what a technology becomes or how it affects society. In the period when a new technology is introduced, people are particularly likely to make technologically deterministic arguments.

The second answer to the question "Who or what decides what a tool means?" is that the designers or creators of a tool affect how the tool is used and understood within a society. Thus, we can speak of d**esigner's intent**. For example, a designer might create a piece of farm equipment which is extremely heavy and therefore more likely to be used by men. Or a kitchen designer might create appliances which are inherently 'feminine' in appearance – such as a pink refrigerator. An object may come to be associated with a certain social class, certain set of practices or values (Zachmann and Oldenziel, 2009) or a certain gender either because a designer consciously decides to create tools which are exclusionary, or less consciously, makes design decisions which reflect the biases which exist within a particular era (Faulkner, 2001). Shannon Vallor suggests that "every technology presupposes a vision of what the 'good life' is" (in Raicu. 2016). This view suggests that objects have an ethics as well as a politics: Design decisions affect who may use or be drawn to use an object and as a result, who can have access to the empowerment which may result from that object (Manjikian, 2012). Those who design new technologies frequently work with sociologists and anthropologists who consider how technologies will be used, and the values which designers may be consciously or unconsciously building into new technologies. Designers today are encouraged to consciously build technologies which are secure as well as those which respect privacy (Mulligan and Bamberger, 2013) and allow for the dignity of their users (Pereira and Baranauskas, 2015).

The third answer to the question "Who or what decides what a tool means?" is that societies construct the meaning of technologies. (This view is sometimes abbreviated as **SCOT – Social Construction of Technology**.) In this view, an object does not have a certain ideology or set of values attached to it. Instead, the same tool might play very different roles,

depending on the society or culture in which it is introduced, and the rules and norms which that society creates to discipline users or control the uses of that technology. In their work, Pinch and Bijker (1984) described how early bicycle designers attempted to position bicycling as a leisure time activity to be practiced by upper-class men. However, over time, the bicycle came to be used by all classes and genders, not only for leisure, but also for commerce. Culture determined the use patterns for the tool, which differ from the intent of the designers.

The question "Where do a technology's meaning and values come from?" is important as we begin to think about cybersecurity ethics in particular. Some analysts argue that the architecture of the internet itself helps to engender corruption, deceptive practices and danger. Others argue that if such problems occur, it is due to design decisions made by those who write code. Still others argue that users, including governments, make decisions which ultimately lead to the growth or lessening of particular unethical practices in cyberspace.

Sources

Faulkner, Wendy. 2001. "The Technology Question in Feminism: A View From Feminist Technology Studies." *Women's Studies International Forum* 24(1): 79–95.

Manjikian, Mary. 2012. *Threat Talk: The Comparative Politics of Internet Addiction*. New York: Routledge.

Mulligan, Deirdre, and Bamberger, Kenneth. 2013. "Privacy and Security: What Regulators Can Do to Advance Privacy Through Design." *Communications of the ACM*. November 1.

Pereira, Roberto, and Baranauskas, Maria Calani Cecilia. 2015. "A Value-Oriented and Culturally Informed Approach to the Design of Interactive Systems." *International Journal of Human-Computer Studies* 80: 66–82.

Pinch, Trevor J., and Bijker, Wiebke. 1984. "The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other." *Social Studies of Science* 14: 399–441.

Raicu, Irina. 2016. "Virtue Ethics on the Cusp of Virtual Reality." *Markkula Center for Applied Ethics*. Available at https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/unavoidable-ethical-questions-about-hacking/ May 25. Accessed June 17, 2016.

Zachmann, Karin, and Oldenziel, Ruth. 2009. *Cold War Kitchen: Americanization, Technology and European Users*. Cambridge, MA: MIT Press.

Box 1.5 Application: does the internet have embedded values?

Philosophers of technology fall into three schools of thought regarding where a tool derives its ideology from – whether it resides within the object itself; whether it is given to the object by its creators; or whether users themselves decide what a tool means and what it will be used for (see inset: Do Tools have an Ethics?). Similarly, we can tell three different stories about the internet's evolution and the values and ethics associated with the internet.

Story one: the internet has inherent characteristics that can affect and reflect values

The first story is one of technological determinism. In this narrative, certain inherent characteristics of a technology cause effects which can change a culture. Department of Defense representatives point to the attribution problem, or the fact that it is often impossible to determine where a message originated, as an inherent characteristic of the internet. They also argue that the internet's open and nonhierarchical nature makes incursions into systems more likely. Thus the analysts suggest that it was inevitable that the internet would become a site of warfare and conflict and an American strategic vulnerability (Manjikian). Intellectual property experts describe the ease of replication of information in cyberspace, since copies are actually cloned rather than loaned when a request is made to access a document. Thus, they argue that intellectual property violations may be an inherent aspect of the internet environment.

This view suggests that the technology itself has had a number of effects on society: speeding up the pace of life and the pace of interactions between citizens and with their government (Virilio, 2000); making individuals more

vulnerable to new kinds of crimes; and increasing political discord and rancor (Sunstein, 2009). The values which the internet contains might thus be danger, violence, instability and perhaps even chaos.

Story two: the designers built the internet and they determine what it means

The second narrative is more optimistic. Those coders who created the internet hoped it would be better than the real world, rather than an extension of the real world. They envisioned a vast library where individuals could become better educated and informed and a network of individuals which would be a 'global village.' The Electronic Frontier Foundation is an organization which espouses this viewpoint, fighting to keep the internet free from what they see as unnecessary and unwarranted national and international regulation. This group's famous slogan "Information wants to be free" suggests that decisions about what the internet means and the values it enshrines should be made by those who designed it, and that it should evolve in line with those understandings.

Story three: it is the users who determine what values the internet will have

In the final story, even the internet's creators might be surprised by what it has become. In his recent autobiography, United States Army General Michael Hayden (2016) notes that he was part of the group of officials who originally approached the United States Department of Defense Advanced Research Projects Agency (DARPA) in 1983 with a simple request: Was there a way to create a 'network of networks' such that individual contractors using modems to connect to Department of Defense computers would be able to interact with one another?

But he states that he and his colleagues had no grand vision of what was going to emerge out of the earliest internet prototype, ARPANET. They never envisioned e-governance, e-commerce or the development of social networking. He describes being surprised by the system's vulnerabilities,

since the original architects never anticipated the development of activities like the development of cyberweapons or the carrying out of cyberwarfare. In this way, his story supports the 'Social Construction of Technology School', which argues that ultimately users define and refine a new technology, making it into something which often does not resemble the original prototype in either form or function.

As we consider these stories, ask yourself which one you believe. Each recognizes different limitations to the internet's potential and establishes different limitations for what programmers and architects may hope to achieve in creating ethical cybersecurity policies. In the first story, it is unclear how cybersecurity professionals can go about securing the safety of citizens, corporations and states in cyberspace – since the technology is seen as having a mind of its own. Similarly, in the third story, it is possible to acknowledge that programmers and designers may be surprised by the ways in which programs, networks and individuals may behave in cyberspace.

Sources

Hayden, Michael. 2016. *Playing to the Edge: American Intelligence in the Age of Terror*. New York: Penguin Books.

Sunstein, Cass R. 2009. *Going to Extremes: How Like Minds Unite and Divide*. Oxford: Oxford University Press.

Virilio, Paul. 2000. *The Information Bomb*. London: Verso.

Why cybersecurity ethics matters

Computer scientists have the ability to impact the environment of the internet. As a result they affect events both online and in the real world. As we see throughout this book, internet technology provides the foundation for other institutions – allowing people to contact their legislators and government, to educate themselves and to access other social and political institutions like housing offices and emergency services. Internet technology also provides the

foundation for other rights – making it possible for people to engage in activities like freedom of assembly, freedom of religion and freedom of speech. A free and open internet is thus part of a free and open society and decisions which individuals make about the design and functioning of that system have ramifications which are global, powerful and permanent (Turilli et al., 2012, 134).

Alec Ross, Senior Advisor for Innovation to Secretary of State Hillary Clinton, famously referred to data as the world's greatest resource. In his book, *The Industries of the Future* (2016), he notes that cybersecurity must be a central feature in all products being developed today. Thus people who shape this resource need to have a developed ethical framework and a way of thinking about issues which arise in this arena.

Box 1.6 Application: a single line of code

Cybersecurity experts need to consider ethics because the environment they work in is so unique. Engineers, coders and designers can both create and destroy the entities which they build in cyberspace simply by typing into a keyboard. In a few keystrokes, a computer programmer can delete an entire company, carry out a financial transaction with large real-world repercussions or launch a cyberweapon which can destroy data or physical infrastructure. In addition, as the analyst Paul Virilio (1986) points out in his famous essay "Dromology," technological decisions and actions can occur today at very high speeds. Three recent events illustrate the ways in which even a seemingly small action by a computer programmer can immediately have large-scale repercussions not just in cyberspace but in the real world as well.

In April 2016, the British newspaper *The Independent* described how British businessman Marco Marsala accidentally typed the Linux command "rm-rf" into his computer. This command, which appears on a list of "commands you should never use," immediately deleted everything in all of his servers, including back-up copies, without first asking him, "Are you sure you really want to do this?" As a result, Marsala, who ran a business hosting internet websites and files for other companies, destroyed his company, deleting all of his files with no hope of recovering them. Later,

Marsala claimed that the reports that he had done this were actually a hoax and that he was only trying to get publicity through 'guerilla marketing'. Nonetheless, this tale shows how one line of code can have major real-world repercussions for a large number of people.

Around the same time, reporter Pierluigi Paganini (2016) reported that Eddie Raymond Tipton, the Information Security Director of Iowa's Multi-State Lottery Association (MSLA), had been 'rigging' the lottery systems in several states over a period of six years. A DLL (dynamic link library) was used to generate specific winning numbers on three days of the year on two days of the week, after a certain time of day. The code was written onto a computer in Wisconsin, and was used to affect lottery winnings in Iowa, Texas, Oklahoma, Colorado and Wisconsin. Using this system, Tipton was able to illegally win 16.5 million dollars for himself.

Finally, in spring 2016, a computer programmer in California named Azer Koculu deleted all of his code packages from NPM, a company which runs a directory of open-source software, after he had a dispute with another company about the name of one of his products. The small snippet of code, known as left-pad, allows an individual to add characters to the beginning of a text string. This snippet was apparently embedded in dozens of other programs used by hundreds of other internet companies. As a result, several other company's software could not run until the problem was addressed. This story shows how common it is for programmers to borrow code and how closely these actors then depend on each other to act forthrightly and with good intentions on the internet.

All three stories show that coders are powerful actors in cyberspace and in the real world. They should not misuse the power that they have or take this responsibility lightly. This is why it is important to study ethics.

Sources

Paganini, Pierluigi. 2016. "Lottery Security Director Hacked Random Number Generator to Rig Lotteries." *Security Affairs*. April 17. Available at www.securityaffairs.co/wordpress/64600. Accessed December 15, 2016.

Virilio, Paul. 1986. *Speed and Politics: An Essay on Dromology*. Paris: Semiotexte.

Thus, it is important to understand computer ethics and the principles which underlie them. You cannot merely obey the laws or go with the flow – since every practitioner will be asked at some point to decide independently about which files to keep, where materials should be stored, who can access them, what credentials will be required to access materials and so forth. There are not merely technical issues. They are also ethical issues.

Box 1.7 Application: the ethics of plagiarism

When you began this class, you probably thought that you were not a philosopher or ethicist. However, you have already encountered common ethical problems and you have used some basic philosophical and ethical principles to decide what you should do.

One issue you have experience with involves your own education. Every student has probably struggled with whether to lie to a teacher or professor to get an extension on a paper (perhaps claiming to have an emergency or a death in the family), whether to cheat on an exam or help someone else cheat or whether to take credit for someone else's work in doing a group assignment. If your university has an honor code you may even have spoken extensively with your professors and fellow students about this topic.

These are all problems in practical or applied ethics. A philosopher might ask a **normative** question in **applied ethics** like "What should students (or professors) do in regard to cheating at the university?" But he or she might also ask a more abstract question like "Why is plagiarism wrong?" or "What values are being violated when plagiarism occurs?"

Why is plagiarism wrong?

You may have heard that **plagiarism** is lazy or dishonest, that it is a form of stealing or even that old line "You're only cheating yourself when you plagiarize because you're robbing yourself of an opportunity to learn." But ethics gives us several frameworks for thinking about this issue:

1 In a university which subscribes to an honor code, plagiarism violates the **trust** the university places in its students and therefore erodes the community and familial relationships among students and students and staff.
2 In a school where students hear a lot about values like duty and honor, plagiarism may be seen as an act which violates a student's **integrity** or sense of self as a person with strong values.

    Still others argue that plagiarism is a type of lie since the student engages in **deception** through presenting himself as someone whom he is not. This argument relies on a **virtue ethics** framework (which we will examine more closely in Chapter 2 of this textbook). This ethical stance assumes that individuals should strive to engage in the behavior which most closely aligns with their personal values. Living out one's personal values should thus be one's ethical objective, regardless of the surroundings in which one finds oneself.
3 If you cheat on a licensing or credentialing exam for a professional qualification (such as a software expert badge or nursing license) then it is a **breach of contract** since you are paying to be recognized as an expert in the field and cheating on the test prevents this. It is also a waste of resources since you might gain more in the short term through acing the test but would lose in the long run if you fail to acquire the skills you need to work in your field. This stance most closely aligns with the **utilitarian** view which states that the most ethical choice is the one that provides the most utility or good generated through one's actions.

    An ethicist might also ask if plagiarism is always wrong, if all acts are equally wrong or if they should be viewed as occurring along a scale and if one should consider whether the student is committing a first offense or is a serial plagiarist. An ethicist might also ask if certain types of climates are structured in ways which can either discourage or encourage plagiarism.

You may find that you already have strong stances on many of these questions and that you have thought them through at length. In that case, you are well on your way to thinking ethically.

Chapter summary

- Ethics is a branch of philosophy concerned with "the good."
- **Normative ethics** considers what one 'ought to' do, while descriptive ethics is concerned with observing and understanding ethical behaviors in different places, times and cultures.
- Computer ethics are normative ethics. They are a branch of both practical and professional ethics.
- Moral philosophers can be either **moral relativists** or **objectivists**. Moral relativists argue that what is morally right or wrong can depend on someone's individual disposition or on the conventions of a particular historical era or culture. Objectivists believe that it is possible to find out what the right thing to do is objectively, and that values and value commitments are universal in scope.

Discussion questions

1. Consider your own experiences in the area of computer science. Can you think of any ethical dilemmas which you have encountered in your own work? What were they and how did you resolve them?
2. Can you think of an example of an unjust law or policy which you have encountered? Think about Kohlberg's levels of moral reasoning. How did you think through your decision to follow or not follow the policy?
3. What are some issues that you have encountered in either your work or leisure online for which there is not a consensus regarding what is the right thing to do?
4. Reflect on the inset on 'Does the Internet have Embedded Values?' Which view do you most agree with – in terms of how the internet derived its values?

Recommended resources

Barlow, John Perry. 1996. "The Declaration of Independence of Cyberspace." Available at www.eff.org/cyberspace-independence. Accessed March 12, 2017.

Leiner, Barry, Cerf, Vinton, Clark, David, Kahn, Robert, Kleinrock, Leonard, Lynch, Daniel, Postel, Jon, Roberts, Larry, and Wolff, Stephen. No Date. "Brief History of the Internet." Available at www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet. Accessed March 12, 2017.

Spinello, Richard A. "Information and Computer Ethics: A Brief History." *Journal of Information Ethics* 21(2): 17–32.

Tavani, Herman. 2002. "The Uniqueness Debate in Computer Ethics: What Exactly Is at Issue and Why Does It Matter?" *Ethics and Information Technology* 4: 37–51.

Chapter 1 sources

Audi, Robert. 1995. *The Cambridge Dictionary of Philosophy*, Second Edition. New York: Cambridge University Press.

Austin, Michael. No Date. "Divine Command Theory." In *Internet Encyclopedia of Philosophy*. Available at www.iep.utm.edu/divine-c/ Accessed January 2, 2017.

Brackman, Levi. No Date. "Where Do Ethics Come From?" *Chabad.org*. Available at www.chabad.org/library/article_cdo/aid/342501/jewish/Where-Do-Ethics-Come-From.htm. Accessed June 12, 2016.

Brey, Philip. 2007. "Ethical Aspects of Information Security and Privacy." In N.M. Petkovic and W. Jonker, eds. *Security, Privacy and Trust in Modern Data Management*. Heidelberg: Springer Berlin: 21–36.

Burley, Diana, Bishop, Matt, Kaza, Siddharth, Gibson, David, Hawthorne, Elizabeth, and Buck, Scott. 2017. "ACM Joint Task Force on Cybersecurity Education." *SIGCSE '17 Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*. March 8–11, 2017. ACM: Seattle, Washington: 683–684.

Bynum, Terrell. 2000. "A Very Short History of Computer Ethics." *American Philosophical Association Newsletter on Philosophy and Computing*. Available at www.cs.utexas.edu/~ear/cs349/Bynum_Short_History.html Accessed February 8, 2017.

Bynum, Terrell. 2015. "Computer and Information Ethics." In *Stanford Encyclopedia of Philosophy*. Available at https://plato.stanford.edu/entries/ethics-computer. Accessed February 7, 2017.

Calman, Kenneth C. 2004. "Evolutionary Ethics: Can Values Change?" *Journal of Medical Ethics* 30(4): 366–370.

Chang, Christina Ling-Hsing. 2012. "How to Build an Appropriate Information Ethics Code for Enterprises in Chinese Cultural Society." *Computers in Human Behavior* 28(2): 420–433.

Chasi, Colin. 2014. "*Ubuntu* and Freedom of Expression." *Ethics and Behavior* 24(6): 495–509.

Chatterjee, Sutirtha, Sarker, Suprateek, and Valacich, Joseph S. 2015. "The Behavioral Roots of Information Systems Security: Exploring Key Factors

Related to Unethical IT Use." *Journal of Management Information Systems* 31(4): 49–87.

D'Arcy, John., and Sarv Deveraj. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model." *Decision Sciences* 43(6): 1091–1124.

Didier, Christelle. 2010. "Professional Ethics Without a Profession: A French View on Engineering Ethics." In Ibo van de Poel and David E. Goldberg, eds. *Philosophy and Engineering, Philosophy of Engineering and Tech*. Berlin: Springer Science+Business Media B.V: 161–173.

Falk, Courtney. 2005. "The Ethics of Cryptography." C*ERIAS Tech Report 2005–37*. (Thesis) West Lafayette, IN: Purdue University.

Floridi, Luciano. 1998. "Information Ethics: On the Philosophical Foundation of Computer Ethics." Remarks at ETHICOMP98: The Fourth International Conference on Ethical Issues of Information Technology (Erasmus University, Rotterdam, Netherlands, 25–27 March 1998). Available at www.philosophyofinformation.net/talks/ Accessed June 6, 2016.

Floridi, Luciano. 2013. *The Ethics of Information*. Oxford: Oxford University Press.

Gotterbarn, Donald. [No Date.] "An Evolution of Computing's Code of Ethics and Professional Conduct." [Unpublished paper.] Available at http://csciwww.etsu.edu/gotterbarn/artge1.htm.

Inacio, Chris. 1999. *Ethics*. Pittsburgh, PA: Carnegie Mellon University. Available at https://users.ece.cmu.edu/~koopman/des_s99/ethics/ Accessed February 7, 2017.

Koller, Peter. 2014. "On the Nature of Norms." *Ratio Juris* 27(2): 155–175.

Levy, Stephen. 1984. *Hackers: Heroes of the Computer Revolution*. New York: Penguin Group.

MacDonald, Euan. 2011. *International Law and Ethics: After the Critical Challenge – Framing the Legal Within the Post-Foundational*. Boston, MA: Brill.

Manjikian, Mary. 2010. "From Global Village to Virtual Battlespace: The Colonization of the Internet and the Rise of Realpolitik." *International Studies Quarterly* 54 (2): 381–401.

Moor, James. 1985. "What Is Computer Ethics?" *Metaphilosophy* 16 (4): 266–275.

Morozov, Evgeny. 2010. "In Defense of DDoS." *Slate Magazine*. December 13. Available at www.slate.com/articles/technology/technology/2010/12/in_defense_of_DDoS. Accessed November 15, 2016.

Myskja, Bjorn K. 2008. "The Categorical Imperative and the Ethics of Trust." *Ethics and Information Technology* 10(4): 213–220.

Nissenbaum, Helen. 2005. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7(2): 61–75.

Pereira, Roberto, and Baranauskas, Maria Calani Cecilia. 2015. "A Value-Oriented and Culturally Informed Approach to the Design of Interactive Systems." *International Journal of Human-Computer Studies* 80: 66–82.

Raicu, Irina. 2016. "Virtue Ethics on the Cusp of Virtual Reality." *Markkula Center for Applied Ethics*. Available at www.scu.edu/ethics/internet-ethics-blog/virtue-ethics-on-the-cusp-of-virtual-reality/. May 25. Accessed June 17, 2016.

Ross, Alec. 2016. *Industries of the Future*. New York: Simon and Schuster.

Scharff, Robert, and Sudek, Val. 2013. "Introduction." In Robert Scharff and Val Dusek, eds. *Philosophy of Technology: The Technological Condition--An Anthology*. Oxford: Blackwell.

Sellen, Abigail, Rogers, Yvonne, Harper, Richard, and Rodden, Tom. 2009. "Reflecting Human Values in the Digital Age." *Communications of the ACM* 52(3): 58–66.

Turilli, Matteo, Vaccaro, Antonino, and Taddeo, Mariarosaria. 2012. "Internet Neutrality: Ethical Issues in the Internet Environment." *Philosophy of Technology* 25(2): 135–151.

Whitehouse, Diane, Duquenoy, Penny, Kimppa, Kai, Burmeister, Oliver, Gotterbarn, Don, Kreps, David, and Patrignani, Norberto. 2015. "Twenty-Five Years of ICT and Society: Codes of Ethics and Cloud Computing." *SIGCAS Computers and Society* 45(3): 18–24.

2 Three ethical frameworks

Learning objectives

At the end of this chapter, students will be able to:

1. Articulate assumptions of each of the three major frameworks – virtue ethics, utilitarian ethics and deontological ethics
2. Compare and contrast major ethical stances – including virtue ethics, utilitarian ethics and deontological ethics
3. List criticisms of each of the three ethical lenses
4. Apply the three different ethical stances in thinking through the ethical consequences of a particular problem or action

In this chapter, we examine three ethical stances developed for considering this question: virtue ethics; utilitarian ethics; and deontological ethics.

Why use an ethical framework?

Every day we make hundreds of decisions: Should I walk to work, drive or take public transportation? Should I bring my lunch from home or purchase it? Should I apply for that promotion or decide that I am happy in my current job?

Academics in many fields – including business, leadership, economics and psychology – think about how people make decisions. In doing so, they build **models** – or simplified pictures of reality – to understand decision making. In building a model, the researcher specifies his assumptions about how the model works, the conditions under which it works, and any restrictions or constraints which might affect the model's working. In considering decision making, researchers make several assumptions. First, they assume that in any situation, we can clearly identify an individual or group as the decision maker. (That is, we assume that decisions don't just evolve in an organization and that they are not made by consensus.) Furthermore, we assume that the decision maker is aware that s/he is deciding, that s/he has the authority to make decisions and that s/he has agency or

control over the choice of actions being considered. S/he is not being coerced by a supervisor to act in a certain way but acts independently. Furthermore, we assume that decisions are made in isolation, that one decision does not necessarily affect and is not affected by any previous decisions, and that the decider is aware of the constraints under which s/he is making the decision. (For example, if one is considering making a choice to violate company policy, we assume that the individual knows what the policies are and what the consequences of choosing to violate them will be.)

In this text we apply three models of decision making – virtue ethics, utilitarian ethics and deontological ethics – to asking questions about cybersecurity. Should you send spam e-mail and what is the consequence of doing so? Should you engage in cyberwarfare against your own country on behalf of another country who is paying for your expertise? How should you treat potentially embarrassing or incriminating information you find out about an employee while carrying out computer system monitoring? In each case, we assume that the individual is the decider, that he is aware of his position as decider and that his decision is independent of previous and subsequent decisions.

The different lenses emphasize different concepts – such as identity and utility – depending on the model chosen. Sometimes the model's recommendations will contradict one another, while in other instances they might overlap. The models can disagree about the badness or goodness of a proposed action or attitude, about the moral or ethical significance of a proposed action or why it matters. Sometimes all three lenses might yield the result that an action – like pirating copyrighted content and redistributing it to make a profit – is wrong, but they may disagree about why it is wrong. In other instances, all three models might suggest taking a certain action but they may disagree about the why, or what makes something necessary. For example, both a virtue ethics and a deontological ethic might value the achievement of equity and nondiscrimination in a situation but they might disagree about why equity is necessary and what choosing equity means. In brief, a virtue ethics argument rests on a claim that "I am the kind of person who" while a deontological ethic considers those who might be the subjects of any sort of ethical rule which is formulated.

In addition to using the models, philosophers use **thought experiments**. In deciding what the correct decision is in a particular situation, ethical philosophers often begin by telling a story about a situation. The situation may be outlandish, far-fetched or unlikely (i.e. Jim is informed that this evening at seven o'clock, he will be required to kill one of his family members). Clearly, such a hypothetical situation is unlikely to happen in real life. However, the story can then be used by philosophers to explore the motives and consequences of an ethical choice.

Computer ethicists may use stories drawn from science fiction to allow individuals to think through the consequences of emerging technologies. For example, in 2000, law professor Lawrence Lessig (2000, 99) posed a thought experiment on his blog, asking "Could architects ever build a building which was so safe and secure that no one could ever break into it?" He then went on to explore the consequences for society, for criminality and for law enforcement of the existence of such a building. More than ten years later, we saw these concerns reflected in discussions about whether the Federal Bureau of Investigation could order the Apple Corporation to decrypt or unlock users' cell phones if they were implicated in terrorist events, like the ones in San Bernardino in fall 2015.

Philosophers in many fields of applied ethics use a variation of what has come to be known as the **Trolley Problem**, developed in 1978 by Phillipa Foot. In this thought experiment, a group of children are playing on the trolley tracks unaware that a trolley is speeding towards them. An observer stands on a bridge. From this vantage point, he sees the events as they are about to occur and has the ability to influence them. He stands next to a very large man. This man's mass is great enough that were the observer to throw him down onto the tracks, his body could stop the trolley. The man, however, would die. Thus, the observer needs to decide if it is moral to sacrifice the life of the one fat man in order to save the lives of the children on the tracks. Today, ethicists point out that automobile drivers may sometimes be called upon to make a similar sort of decision. If they are about to hit an oncoming car, should they swerve to avoid it, saving the life of that car's occupants but possibly endangering the occupants of their own vehicle? To whom is their ethical duty greater – that of the stranger or that of their own family or friends? Robot ethicists note that we will soon have self-driving vehicles and ask how computers can learn to think about similar ethical scenarios when they react to unanticipated situations and road obstacles (Jaipuria, 2015).

However, some academics have criticized philosophers' reliance on models and thought experiments. Walsh (2011) notes that neither models nor thought experiments reflect the real world, where we seldom act in isolation and where our choices are often not discrete or made in isolation, and where we often do not conceptualize of ourselves as being at a decision point at the time when we do act.

Nonetheless, we rely upon these models for both pedagogical and research reasons. The three lenses provide you as students with a clear way of thinking about ethical decision making, and of thinking through ethical decisions. And as you will see in Chapter 7, these same models are often used by policymakers, including those in the United States military, as they think through the consequences of ethical decision making in relation to issues including the use of autonomous weapons and the rights and responsibilities of soldiers engaged in cyberwar.

What are virtue ethics?

The first model is Virtue Ethics. We can trace this approach to ethical thinking back to the days of ancient Greece and in particular back to **Aristotle** (384–322 BC). Aristotle believed that everything that exists in nature does so for a purpose. This includes man, whose purpose in life is to act well as a human being (Afthanassoulis, 2012, 55). If he does this, Aristotle counsels, he will have a good life. This principle has sometimes been referred to as the cultivation of human flourishing. Aristotle himself describes acting in this way as the equivalent of being healthy. One is ethically healthy if one cultivates certain attitudes, characteristics and ways of being which are then expressed appropriately (Gottlieb, 2009, 21). Koller (2007, 31) writes, "The concept of virtue refers to the character traits of persons, their practical attitudes or dispositions which have some motivating force for their conduct."

In Aristotle's ethics it is the acts which matter, along with the attitudes which lead an individual to carry out these acts. It is referred to as **agent-centered ethics**, since it emphasizes the decision-maker's agency or free will to make choices, and because it focuses on the decision maker and his character as the main consideration in determining whether an action is ethical. An ethical individual, in Aristotle's view, is someone who does and feels "the right things at the right time in the right way and for the right reasons" (EN#6 1106b21 in Gottlieb, 2009, 21). In his work, Aristotle counsels people to find the spot in the middle or the mean when thinking about character. Each virtue exists along a spectrum and neither an excess nor an absence of a quality is good. Indeed, displaying either too much or too little of something is regarded as a vice. For example, we can think of a spectrum which runs from timidity to courage to foolhardiness. Aristotle would counsel against having too much courage if it leads to making stupid decisions, as well as against having too little. He also acknowledges that the right amount of a virtue might vary depending on the context as well as on one's own limitations. For example, deciding not to rescue a drowning man would be wise if you were a poor swimmer but would be wrong if you were a good swimmer. The good swimmer is being timid here while the poor swimmer is being wise (Gottlieb, 2009, 30). Similarly, in a culture like the United States where taking risks is often regarded as praiseworthy, quitting your job to start your own business might be regarded as courageous while in another culture it might be regarded as foolish (Walker and Ivanhoe, 2007).

Virtuous does not mean saintly

Although we use the word virtue, Aristotle's ethics is aimed at teaching people how to live well in keeping with their human nature. It does not merely apply rules but considers people's psychology and emotions. It tells people how to 'succeed' at life (or

flourish) through acting sensibly and in keeping with their human nature. It does not counsel taking unnecessary risks nor does it suggest that you must always sacrifice yourself for others – though it does suggest that one should strive to treat others well if possible. Aristotle does not say you should never get angry (as a saint might) but says you should be appropriately angry at the right time for the right reasons (Gottlieb, 2009, 21). And as we will see in Chapter 7 on cyberwarfare, virtue ethics counsels that killing one's enemy may be the right action and the right attitude, depending on the situation and the place, as well as the conditions under which the decision is made. It doesn't merely say that killing is wrong.

Many of the virtues which Aristotle addresses overlap with the character traits (or theological virtues) stressed in many of the world's major religions. The ancient Greeks acknowledged Four Cardinal Virtues – prudence, courage, moderation and justice (Gottlieb, 2009). Other analysts have added additional character traits which individuals should strive to develop – including reasonableness, truthfulness, honesty or sincerity, goodness or benevolence, helpfulness, friendliness, generosity, humility and modesty (Koller, 2007).

Ali (2014, 10) identifies virtue ethics (along with a utilitarian ethics) in Islamic thought. He notes that both the Koran and the Hadith stress the importance of intent. He notes that the Prophet Muhammed stated that "God examines your intentions and actions," arguing that honest or bad intentions determines a work's outcome. He also identifies ten Koranic virtues – "forbearance, generosity, adherence to accepted custom, righteousness, patience, thankfulness, flexibility, reason, sound faith and knowledge." Jewish scholars point to the emphasis throughout the Old Testament on wisdom. A wise person also has the tools to learn about and acquire other virtues, and to solve all sorts of issues which arise (Borowitz and Schwartz, 1999).

Virtue ethics also assumes that one's character develops over time – through one's experiences and exposure to people and ideas. One can practice ethical behaviors and grow in virtue. In writing about the development of a virtue ethic within a military community, Vallor defines virtues as "habituated states of a person's character that reliably dispose their holders to excel in specific contexts of action and to live well generally" (2013, 473).

Contemporary virtue ethics

Today analysts cite two modern texts in describing more recent developments in virtue ethics – Elizabeth Anscombe's 1958 essay, "Modern Moral Philosophy" and the work of Alasdair Macintyre. These texts argued that the previous philosophical emphasis on rights and duties in figuring out what people should do was insufficient and unduly focused on applying rules and finding laws for behavior. Furthermore, it focused too

much on thinking about specific values like equity and justice, to the detriment of considering issues like generosity, friendship and charity (Walker and Ivanhoe, 2007).

These theorists liked virtue ethics' emphasis on **intent** (or what Aristotle would have described as right thinking). In Aristotelean virtue ethics, an action is considered virtuous if it is performed correctly, at the right place and at the right time, but also with the right intent. Here, we can consider activities which individuals can perform that might seem virtuous but in fact are not because of the intentions behind them. In the first example, John saves a man from drowning in a lake – but only because he wants to impress the girl he is with by behaving heroically in front of her. In the second example, Kate accidentally donates to charity by pushing the wrong button on her computer while online shopping (she meant to purchase a sweater!). In each instance, the individual did not actually behave morally because the individual did not behave with moral intent (Afthanassoulis, No date).

Therefore, virtue ethics is useful for carrying out applied ethical thinking since it can help us to know what it is to do good versus merely knowing what good is in the abstract. For this reason, virtue ethics is also very useful in framing a professional ethic and in building professionalism (Walker and Ivanhoe, 2007). Indeed, we will see in Chapter 3 that many aspects of the hacker ethic can be seen as stemming from virtue ethics.

Critiques of virtue ethics

However, there are those who do not like the virtue ethics model. We can identity three different types of critiques: First, some scholars oppose using a model to 'do ethics,' arguing that models are by definition simplifications of the real world. Here analysts point out that often in the real world, people may be coerced or compelled into making decisions – through peer or social pressures or threats.

Next, some analysts suggest that the individual level is not the most appropriate level of analysis for thinking about the development of good in society. Some analysts prefer pragmatic ethics. **Pragmatic ethics** is a subfield of ethics which focuses on society, rather than on lone individuals as the entity which achieves morality. John Dewey, a theorist of pragmatic ethics, argued that a moral judgment may be appropriate in one age in a given society but that it may cease to be appropriate as a society progresses. Pragmatic ethics thus acknowledges that ethical values may be dynamic and changing.

Still other scholars critique the specific model of Aristotelian virtue ethics, rather than the idea of relying on models itself. Voicing what is commonly known as the 'situationist critique,' a number of scholars have utilized psychological research to argue that one cannot truly speak of one's moral character or personality as a fixed and unchanging entity. These scholars note that people behave differently in different situations – even at

different times of day (Kouchaki and Smith 2014) – while virtue ethics assumes that one's notion of the self is relatively stable and fixed (Slingerland, 2011; Ellithorpe et al., 2015). Others call Aristotelian virtue ethics Western-centric, since it recommends pursuing characteristics and attributes which may be prized in some societies more than others, or more highly prized amongst men than amongst women (Barriga et al., 2001). For example, does every society and gender equally prize courage as a value? In some societies, members might see courage as belligerence and prefer cultivating peacefulness. Finally, some scholars describe virtue ethics as based on circular reasoning: One acts in a certain way in order to show one's character which is a function of one's actions. It is unclear whether actions cause character or character causes action.

Some scholars dislike virtue ethics' emphasis on individual moral reasoning, suggesting that it is selfish for the decision maker to care more about his own flourishing than the overall outcome of the decision. For example, if someone decided not to lie to an authority figure because he prized truthfulness, then he might feel virtuous in telling a Nazi officer who amongst his neighbors was hiding Jewish citizens in his home. Here his personal virtues might lead to a lack of compassion towards others.

The virtue ethics approach has also been criticized because it is theoretically possible for someone to be wholeheartedly committed to a value but to still be an objectively evil person. Consider the Islamic terrorists who perpetrated the bombings of September 11, 2001. In the context of their religious assumptions, they were virtuous in carrying out what they saw as an obligation to conduct jihad or religious war against unbelievers. This problem suggests that merely choosing to commit to the service of a particular value or virtue may not be sufficient to guarantee that one is behaving in what a majority of people would consider to be moral and ethical behavior.

A final critique of the virtue ethics lens is that it is outdated and not relevant to the real world. To some degree, this criticism comes from individuals who are misinformed about the model, hearing the word virtue and assuming that it is a "preachy" religious model. However, scholars are currently debating whether it makes sense to talk about virtue ethics in cyberspace.

Virtue ethics in cyberspace

In Chapter 1, we encountered the uniqueness debate – the dispute about whether cyberspace is an alien environment in which traditional ways of thinking about ethics are irrelevant – or whether cyberspace is an extension of real space (or meat space), where humans behave in the same way that they do in the real world. Philosopher Bert Olivier (2017, 1) feels that virtue ethics apply to cyberspace. He asks:

> Why would one's virtual presence in cyberspace give you license to behave any way morally than under the concrete conditions of the human, social-life world? In ordinary social and interpersonal interactions we expect people to behave in a morally "decent" manner; in cyberspace there should be no difference.

Indeed, studies show that individuals can import their values from real world interactions into cyberspace. Harrison describes students who chose not to engage in online cyberbullying, noting that many of these students described the values which led them to make this decision. Among those values, they listed care for others, individual self-discipline or restraint, compassion, humility and trust. As we see in this text, many interactions among individuals and groups in cyberspace rest on core values of virtue ethics – such as the establishment of trust, the building of relationships and a desire to speak honestly and avoid deception.

Vallor (2013, 120) identifies twelve 'techno-moral virtues' which she believes can serve individuals as a guide to making ethical and moral decisions about their conduct in cyberspace. She lists "honesty, self-control, humility, justice, courage, empathy, care, civility, flexibility, perspective, magnanimity and wisdom." She suggests that individuals in technological fields can practice these virtues in their daily lives.

Some analysts, however, argue that cyberspace's distinct architecture facilitates certain types of actions and practices – including deception. And other analysts say that we cannot conflate respecting people's data or digital identities with respecting human persons – especially because the nature of the internet itself makes certain data collection, retrieval, storage and sharing practices more likely and more desirable. These analysts do not believe that a person who aggregates data sets and accidentally or on purpose learns information about an individual which may be seen to violate their privacy and personal boundaries, has somewhat made an ethical misstep, by failing to respect that person. While it may violate one's individual values to harm a person, they argue, harming one's reputation in cyberspace by publishing private data is not an equivalent act (Burnham, 2016). Rather, in our current age, people should expect that their data will likely be collected and shared by utilities like Spokeo. The one who does so is thus not a thief or person of poor moral character; instead, he may be a businessman, an analyst or an investor who is following standard protocols and expectations.

Box 2.1 Application: the ethics of trolling

Trolling, which has been around since the earliest days of the internet, refers to the act of "intentionally disrupting an online community" through posting something which is facetious and often intentionally inflammatory (Malwebolence, 2008). A troll attempts to increase tensions in an online discussion and sometimes attempts to divert the conversation through posing a query or making a remark, often acting anonymously or even posing as someone else. Trolling is deceptive and disruptive, but is it unethical?

Some individuals make a **utilitarian argument** in which they state that trolling imposes costs and poses the risk of disrupting an online community. However, they argue that overall, trolling can improve a conversation online by making it more lively and forcing people to think a bit harder about their assertions. These individuals argue that trolling is an art form and that when done correctly it is a great way of calling attention to other respondents who may be behaving inappropriately or responding in a knee-jerk simplistic fashion (Anderson, 2016). These respondents distinguish between ethical trolling and other activities like cyberbullying. They state that the costs of a few bad eggs are insufficient to shut it down, since often it is useful and helpful.

Others, however, refer to Garrett Hardin's "**tragedy of the commons**." Hardin asserts that people are self-interested and they don't treat communal resources the same way as their own resources. Farmers, for example, are more likely to overgraze on farmland which is communal in order to realize an individual short-term gain by selling healthy, well-fed cattle and less likely to care about the long-run good of the communal land (Hardin, 1968). This is why people seldom cooperate to preserve an environment, whether it is real or virtual (theconversation.com, 2012). Similarly, one can argue that trolling degrades the internet environment by increasing tension and outrage. In addition, what begins as trolling may quickly devolve into online harassment or bullying (dailybeast.com, 2015).

One can also reference **virtue ethics** and the ethic (again) of diversity and equity. A virtue ethicist might argue on behalf of outlawing anonymous conversations which might lead to trolling – noting that trolling isn't an equal opportunity activity. Instead, they note that trolls often seek to silence particular viewpoints, leading to internet conversations which are less accepting of diverse viewpoints. For example, respondents have noted that trolling is often misogynistic and aimed particularly at silencing the voices of women and minorities, including the transgendered, on the internet (dailybeast.com, 2015).

Currently, legislation exists which carries stiff penalties for activities like cyberbullying. In addition, in some nations legislation exists which requires

individuals to use their real names or to register in order to participate in a conversation. However, government regulation of trolling raises additional ethical issues, as requiring all participants to register as users or as members of particular sites may silence some views or cause fewer participants overall.

Sources

Anderson, Jon. 2016. "Trolling Etiquette – Art of Ethical trolling, Provoking for LOLS." November 16. *Hubpages.com*. Available at https://hubpages.com/art/Trolling-Etiquette-Art-of-Ethical-Trolling-Provoking-for-LOLs. Accessed March 2, 2017.

Dailybeast.com . 2015. "Cover-Ups and Concern Trolls: Actually, It's About Ethics in Suicide Journalism." October 31. Available at http://thedailybeast.com/articles/2015/10/03/cover-ups-and-con. Accessed November 8, 2015.

Schwartz, Mattatias. 2008. "Malwebolence – the World of Web Trolling." *New York Times*. August 3. Available at www.nytimes.com/2008/08/03/magazine/03trolls. Accessed December 2, 2015.

Theconversation.com . 2012. "Troll Watch: The Internet Needs Ethical Standards." *The Conversation*. September 18. http://theconversation.com/trollwatch-the-internet-needs-ethical-standards. Accessed March 2, 2017.

How do professional codes of conduct reflect virtue ethics?

Virtue ethics often form the basis of a **professional code of ethics**. For example, all medical personnel subscribe to the **Hippocratic Oath** (see Box 1.3), which describes the responsibility a physician or health care provider should feel towards a patient. In applying virtue ethics, professionals might ask: "What does it mean to be a benevolent doctor, teacher, lawyer or soldier? What characteristics, values and habits should a member of my profession cultivate and represent?" We can also see virtue ethics approaches applied to human services fields like psychology, social work and nursing. In each case, writers make a link between someone's vocation or calling to practice a particular profession, the individual's values and identity as a person.

What are deontological ethics?

The second model is deontological ethics. We commonly point to **Immanuel Kant** as the father of deontological ethics. Immanuel Kant (1724–1804) was a German philosopher who believed that humans have a privileged place in the universe due to their ability to reason. Writing during the Enlightenment, Kant felt that humans could use reason to derive normative or ethical stances. Kant suggested that you could be moral even without believing in God or natural law because you could calculate the appropriate

moral action or set of duties. Kantian ethics is also referred to as **deontological ethics**, or an ethics of **duty** or **obligation**.

Unlike Aristotle, Kant was not focused on the agent's state of mind or character. And unlike utilitarian ethics, Kant did not focus on the outcome of the agent's decision. Instead, deontological ethics defines certain behaviors as moral duties or obligations which all humans have to one another – these duties exist independently of any good or bad consequences that they might create (Brey, 2007). A deontological approach deems an action moral or ethical if the duty has been complied with. This approach does not promise that the individual who makes the decision to fulfill his duty will necessarily be happy as a result of doing so, nor that it will necessarily lead to the best possible outcome. Rather, it is simply the right thing to do.

Deontological ethics suggests that humans can utilize their reason to solve an ethical problem through searching for the **categorical imperative**, which can be expressed as "always act on the maxim or principle which can be universally binding, without exception, for all humans." His ethics thus assumes that it is not moral to have a different set of ethical or moral laws for one individual than would be appropriate for everyone. That is, it suggests that everyone should define and agree to adhere to the same set of standards, rather than identifying, for example, one set of standards for CEO's or wealthy nations and a different set of standards for employees or poorer nations.

A second principle of Kantian ethics is the notion of **reversibility** or the Golden Rule. In contemplating taking an action, the actor needs to ask himself "Would I be harmed if someone took the same action against me? How might I be harmed?" Thus, he would conclude that theft is bad since he would be harmed if someone stole from him. Trust is a fundamental component of ethics, and that Kantian ethics help to establish a foundation where people can trust one another – since individuals recognize that they have a duty not to deceive, coerce or exploit their fellow humans (Myskja, 2008). Kant's emphasis was on identifying principles that would be universally true, always and everywhere. In a study of Chinese enterprises, Chang (2012, 427) found that many Chinese people saw the Golden Rule as similar to a principle that exists in Confucian ethics. She quotes a worker at a factory who says, "People should respect each other. This is a human principle." Thus, she argues that the "general moral imperatives" section of the Association of Computing Machinery (ACM) code (which includes the ideas that one should contribute to society and human well-being, avoid harm to others, promote honesty and trustworthiness and promote fairness and nondiscrimination) is universal in its scope and its appeal, due to its overlap with Chinese values including loyalty and the Golden Rule (referred to as 'the silver rule' in Chinese culture).

A related principle in Kantian ethics states that everyone should treat others as an end in themselves, as people who deserve respect and dignity, rather than merely as means to

an end.

Box 2.2 Going deeper: Immanuel Kant

Immanuel Kant (1724–1804) was a German philosopher who believed that humans have a privileged place in the universe due to their ability to reason. Writing during the Enlightenment, Kant's *Critique of Pure Reason* (1781) laid out the proposition that humans should be able to use their reason to derive normative or ethical stances. Kantian ethics thus suggest that one could be a moral person even in the absence of a belief in God or natural law because one could calculate the appropriate moral action or set of duties to himself and his fellow man. Morality thus did not inherently reside in people, but rather was derived by them using their intellectual powers of reasoning. Kant has been described as a revolutionary figure in philosophy due to the new emphasis on reasoning which he brought to philosophical study.

He is also seen as a key figure in the development of philosophy of mind, which deals with the question "How does the mind receive and make sense of or structure information which comes from outside itself, from the physical world?"

Kant's influence, however, extends far beyond the field of academic philosophy. He is also considered an important figure in political science where his idea of 'perpetual peace' is referenced in describing views of the international system and methods for conflict resolution. Today, scholars in international relations still debate whether the international system is best understood through a Hobbesian or a Kantian lens. In a Hobbesian world, states do not trust other states and view them through an adversarial lens, while in a Kantian world, states view other states as basically good and rational and seek to cooperate with one another to eliminate or preempt conflicts. Many view Kant's idea of perpetual peace as the foundation upon which US President Woodrow Wilson decided to build the League of Nations in 1917. This institution went on to become today's United Nations. In addition, John Rawls, the 20th century American political philosopher, was influenced by Kant in his thinking about justice and equity (Kant 1993).

Today, analysts such as Floridi (2010) have attempted to apply Kantian principles like perpetual peace to thinking about conflicts in cyberspace.

Sources

Floridi, Luciano. 2010. *The Philosophy of Information.* Oxford, UK: University of Oxford Press.

Floridi, Luciano, and Taddeo, Mariarosario. 2014. *The Ethics of Information Warfare*. New York: Springer.

Kant, Immanuel. 1781. *Critique of Pure Reason*. Cambridge, UK: University of Cambridge Press.

Kant, Immanuel. 1993. *Grounding for the Metaphysics of Morals*. Translated by James Ellington. 3rd Edition. Indianapolis, IN: Hackett.

Guthrie uses deontology – and the reversibility principle – in describing the ethical responsibilities of technology's designers. He argues that "designers should not be attempting to persuade others of something they would not consent to" (Guthrie, 2013, 57). If you would be uncomfortable with a technology which reads your mail, stores your mail or monitors your activity online, then you should not be building them or installing them. If you would be uncomfortable with a technology which 'prompts' you to do things (not speeding, not leaving the baby in the car on a hot day, not driving without a seatbelt), then you should extend the same courtesy and respect to other would-be users of this technology.

In the 20th century, another philosopher (who was not a moral philosopher but a political philosopher) took up many of Kant's ideas about the categorical imperative. Like Kant, **John Rawls** believed that people could reason their way to an ethical solution, and that they should seek to identify universal rules for behavior which could apply to all people equally. In other words, the value he prized the most was justice or distributive justice, since he believed that humans had the obligation to seek a just or fair solution to ethical dilemmas. However, he argued that in deciding an ethical solution, none of us is really objective. When we think about situations and what we should do, we cannot separate out our identities as men or women, as Americans or other nationals or as rich or poor people and we are tempted to choose the solution which is in our own self-interest. We may believe that we have earned or are entitled to certain advantages. However, Rawls argued that no one should have the right to have more goods or opportunities simply because of any particular character traits he or she has, or any advantages which one might have through the circumstances of one's birth.

Thus, he argued that as people reasoned their way to an ethical position or rule, they should engage in a thought experiment in order to seek what he called "**the original position**." Here, they should ask themselves "If I was blind to my own position – i.e. I didn't know my gender, my race, my social class, my nationality – what rule would I then be willing to adopt as universal in this situation?" He referred to this position of not knowing who you were in the scenario as "**the veil of ignorance**" (Smith, 2016). He suggested that in reasoning behind the veil of ignorance, people would have to consider the position of the person who was least favored by any proposed hypothetical rule (what he refers to as the d**ifference** p**rinciple)**, and that in this way, people's regard for

those at the bottom of our sociopolitical hierarchy would be strengthened (Douglas, 2015).

Rawls' ideas have been influential not only in the field of philosophy but also in the field of politics. Bagnoli argues that Rawls' original position allows for people of diverse cultures, religions and value systems to come together to conclude agreements which would be ethically acceptable to all. Today, much thinking about international governance, the role of foreign aid, and the duty of the developed world towards the developing world are influenced by his thinking (Douglas, 2015).

We can contrast Rawls' theory with utilitarianism. Both aim to find the 'best' outcome to a dilemma, but utilitarianism is concerned with maximizing utility in the aggregate or finding the most utility – regardless of how that utility is distributed. In other words, a solution could potentially be unfair in that some people benefitted significantly more than others, or some people benefitted while others lost out. However, if that solution produced the greatest amount of utility, then it would be considered the best solution by a utilitarian. In contrast, Rawls' theory would only allow an inequitable solution in the event that the inequitable solution gave maximum benefit to the least advantaged. It considers not just aggregate utility but also the distribution of that utility (Schejter and Yemini, 2007, 146).

Box 2.3 Critical issues: ethics of Wikipedia

Most students today grew up with Wikipedia. The online encyclopedia, created by its users, was launched in 2001 by its founders Jimmy Wales and Larry Sangers.

The site is in many ways a living embodiment of many of the **communitarian principles** which the internet's earliest founders espoused. Wikipedia is a collaborative project where people volunteer to write articles, to check the accuracy of other's work and to suggest changes and amendments. Wikipedia can be seen as a site where knowledge is produced collectively as a collective good, through the voluntary contributions of its users. De Laat (2015) refers to participating in Wikipedia as "a gesture of friendship."

However, a look at some of the controversies which have emerged over Wikipedia's short history helps us to understand the issues which communitarian social spaces face, and why many analysts believe that Wikipedia's utopian vision is unrealistic. From an ethical perspective, there are two major issues.

The first issue concerns the **politics of equity and representation**. Although communitarians want to create spaces in which all will have equal representation and rights, Wikipedia does not actually achieve this. Simonite (2013) points to the

fact that Wikipedia offers more coverage of technical topics, Western-oriented topics and male-oriented topics. He notes that 84 percent of articles about places provide information about either North America or Europe.

Paling (2015) suggests that Wikipedia is not merely biased but is actively hostile to some groups, including women. She faults the decision-making body of 12 individuals who referee controversies which arise in the space, noting that between 84 and 91 percent of editors are male, and that of the super contributors (who have contributed to 500 or more articles by furnishing information or making edits), only 6 percent are female. She points to a lack of pages about prominent women scientists, and a tendency to dismiss certain types of knowledge or achievements, such as featuring American female novelists in a list of 'women novelists' but not in a list of 'American novelists.'

Over time, other analysts have pointed to the increasingly high barriers to entry for participation in Wikipedia as the process for suggesting edits and adding information has become more bureaucratic, requiring a greater investment of time and a greater overall level of skill. Thus, Wikipedia is merely reflecting some of the access and equity problems which exist in the real world, rather than creating a new space where these problems do not exist.

A second set of ethical concerns deals with the **problem of harm**. Wikipedia states that a good article meets the following six criteria: it is well-written; verifiable through links to other resources, but without original research; broad in its coverage; neutral, without editorializing or being biased; stable or unchanging from day to day and illustrated with images if possible (Wikipedia, No date).

However, while Wikipedia checks the credibility of its information, most of Wikipedia's contributors do so anonymously. Thus, Wood and Santana (2009) ask how users can know that the authors are being truthful and what, if any, incentives authors have to be truthful. Not surprisingly, some individuals and corporations have public relations firms write articles about their own individual or corporate accomplishments which reflect them in a positive light. Others engage in 'revenge writing,' in which case they may include negative information about another individual or group. Revenge writing may include slander, libel or racism, or it may reflect ongoing nationalist or political disputes.

Santana and Wood (2009) argue that most users are unaware of these controversies and that they frequently do not 'click through' to the original articles, nor do they verify that the Wikipedia article is accurate. They do not know that Wikipedia receives up to 9000 malicious or disruptive edits per day (de Laat, 2015). Santana and Wood (2009) write, therefore, that "users may act upon information

that is incomplete, misrepresented or untrue; these actions may result in unintended harms to users to other others."

A related ethical issue is the problem of **guilt or culpability**. In the event that a user is somehow harmed by relying on information (such as medical information) on Wikipedia, who should be held liable – the reader who was insufficiently wary of the source? The source itself? The author who furnished the false information, or the technology which somehow enabled the incident to take place? Ethicists have taken a variety of positions in relation to this issue.

Sources

de Laat, Paul B. 2015. "The Use of Software Tools and Autonomous Bots Against Vandalism: Eroding Wikipedia's Moral Order?" *Ethics of Information Technology* 17: 175–188.

Kleeman, Jenny. 2007. "Wiki Wars," The Guardian. March 25, 2007. Available at https://www.theguardian.com/technology/2007/mar/25/wikipedia.web20. Accessed November 1, 2015.

Paling, Emma. 2015. "How Wikipedia Is Hostile to Women." *Atlantic Monthly*. October 10. Available at www.theatlantic.com/technology/archive/2015/10/how-wikipedia-is-hostile-to-women/411619/. Accessed December 10, 2016.

Santana, Adele, and Wood, Donna J. 2009. "Transparency and Social Responsibility Issues for Wikipedia." *Ethics of Information Technology* 11: 133–144.

Simonite, Tom. 2013. "The Decline of Wikipedia." *MIT Technology Review*. October 22. Available at www.technologyreview.com/s/520446/the-decline-of-wikipedia/. Accessed December 2, 2016.

Wikipedia. No Date. "Good Article Criteria." Available at https://en.wikipedia.org/wiki/Wikipedia:Good_article_criteria. Accessed September 2, 2016.

Critiques of deontological ethics

There are many critiques of Kantian ethics. Some analysts suggest that Kant's notions of universal duties in all situations are too idealistic and ultimately unachievable. For example, Kant suggests that humans have a duty to engage in peaceful relations with each other and to assume that the other is trustworthy.

Others have dismissed Kantian ethics because they see it as inflexible. The rule or duty to be truthful, they suggest, should not be absolute. Shouldn't you have the ability to lie to a Nazi official who asked you if you were sheltering Jews during World War Two, they ask? Should one tell the truth to someone else whose own intentions are impure and inclined to do ill to you? Others describe this as a misreading of the categorical imperative, noting that in his later writings, Kant did distinguish between lying to someone who might harm you (like a criminal) versus lying to someone else (Falk, 2005).

Critiques of Rawls

Some of Rawls' critics object to the assumptions which he builds into his model. In particular, they disagree with his assumption that the overriding value which deciders should wish to pursue is justice. Here some misread Rawls, believing that his emphasis on providing an equitable solution means that he would never countenance a solution in which some people benefitted more and some people benefitted less from a situation. However, he does acknowledge that a just solution might be one where the wealthy benefitted more, provided that the poor also benefitted, and did not lose in any proposed settlement. (Thus, for example, he might find a public building project equitable if it created an infrastructure that allowed everyone to have clean water, even if the project benefitted the wealthy more than it benefitted the poor.)

Writing in *Liberalism and Its Limits*, philosopher Michael Sandel has objected to Rawls' emphasis on acquiring individual goods rather than collective goods. In deciding what the equitable solution to a dilemma is, Rawls believed that everyone had the right to "equal basic liberties" including the right to vote, to run for office, to have freedom of speech and assembly and freedom to own private property. He also believed that individuals should have equality of opportunity to pursue goods and actions in their society (Douglas, 2015). Sandel also takes issue with Rawls' notion that one can think of an autonomous person who is somehow completely separate from the circumstances of his upbringing, culture or birth. He goes on to argue that in suggesting that the most well-off should somehow be asked to apply their talents and resources for the benefit of the least well off rather than for their own benefit – in accepting a solution which benefits those at the bottom more than those at the top – Rawls is actually treating these individuals as 'a means to an end' rather than an end in themselves – which violates the rules which Kant established earlier (Baker, 1985).

Some utilitarian philosophers fault Rawls' use of the veil of ignorance as a deciding mechanism because they feel that choosing the solution which does the least harm to the weakest member is too cautious or risk-averse an approach. Such analysts argue that sometimes one has to take a risk or a gamble in implementing a just solution, and that even if one group suffers in the short-term, the good created by a particular policy might be best in the long-run. In response, Rawls has argued that it is not rational to gamble with liberties and opportunities (Schroeder, 2007).

Box 2.4 Application: is Tor unethical?

Tor, which stands for 'the onion router,' is a software program that allows people to disguise their IP addresses so they can browse, e-mail and chat anonymously. More

than 5000 computers throughout the world voluntarily serve as relays and messages 'jump' from one computer to another in random patterns, breaking the link between the user's identity and his activities as a result (Lawrence, 2014).

Tor's origins

The US government originally funded Tor's development in order to help people in authoritarian countries use the internet to engage in pro-democracy activities (Nicol, 2016). Today, social service agencies use it to aid victims of domestic violence in the US and abroad.

However, US government officials now believe that Tor is dangerous, since it allows all sorts of anti-government activists, including terrorists, to organize online free from government surveillance or law enforcement. Today, many actors on the dark web use software like Tor. Tor has been implicated in various types of organized crime where it acts as a force multiplier, making criminal syndicates more effective and efficient through allowing them to pass information anonymously. Individuals can download criminal materials like child pornography with less risk of being caught.

Ethics: the problem of complicity

For an ethicist, Tor's existence poses a quandary: Can a technology be evil? And can a technology help create evil? Mellema defines complicity as the enabling of harm. For example, if someone wishes to commit murder but is unable to purchase a weapon because he is mentally ill or has a criminal record and he asks another person to purchase the weapon for him, the person who purchased the weapon might be found to be complicit or an accessory to murder, even if he himself never pulled the trigger (Manjikian, 2015). Using this reason, we might describe Tor as a utility which enables harm – such as the purchase of drugs, conventional weapons or cyber weapons.

However, as we learned in Chapter 1, social constructivists believe that technology is neither good nor bad. Rather, what matters is how people use it. These analysts would consider Tor merely as a utility, and ask what specific uses of this utility would be ethical or unethical. Using this approach, we can use our models – virtue ethics, utilitarian ethics and deontological ethics to ask what uses of Tor are ethical.

Here, a virtue ethics approach would look to the virtues of integrity and self-restraint in arguing that Tor is incompatible with the practice of those two virtues.

Integrity suggests that individuals should have the courage of their convictions and be willing to accept the consequences for behaviors in which they engage. Self-restraint suggests that people should be willing to inhibit certain behaviors, while Tor allows individuals to act without inhibitions.

Similarly, a **utilitarian** argument might stress that Tor reduces risks associated with anti-social and anti-state behaviors, thereby making it more likely that such behaviors would increase in the system. That is, Tor could be said to enable anti-social activities – like the purchase of pornography, illicit drugs and stolen credit card numbers. Furthermore, Tor could be a very effective weapon in the hands of terrorists. For this reason, France's Ministry of the Interior considered two proposals in the aftermath of the 2016 Paris Massacres – a ban on free and shared wi-fi during states of emergency, as well as measures to ban Tor in France (Anthony, 2015). A utilitarian might argue that these risks outweigh any social utility that might be created through allowing individuals in authoritarian nations to freely engage in online transactions and interactions.

A deontologist would ask what sort of universal rule could be found regarding access to anonymizing technologies. Would you support an absolute ban on citizen (versus military or government) access to this technology in order to prevent terrorist outbreaks? Such a ban might mean that terrorists could not use the technology, but neither could you.

Tor's future

It is unlikely that Tor will shut down. However, scientists are always working to find ways to break anonymity and there are promising new steps in this direction. The FBI's Remote Operations Unit is reported to have developed malware known as "Cornhusker" or "Torsploit" which allows it to unmask and identify Tor users. This has allowed them to prosecute individuals for criminal and intelligence matters through using materials sent through Tor (O'Neill, 2016). This technology was used in the FBI's take-downs of the illegal drugs website Silk Road (Vaas, 2015).

Sources

Anthony, Sebastian. 2015. "France Looking at Banning Tor, Blocking Public Wi-Fi." *Arstechnica.co.uk*. December 7. Available at https://arstechnica.com/tech-policy/2015/12/france-looking-at-banning-tor-blocking-public-wi-fi/. Accessed December 2, 2016.

Lawrence, Dune. 2014. "The Inside Story of Tor: The Best Internet Anonymity Tool the Government Ever Built." *Bloomberg Businessweek*. January 23. Available at www.bloomberg.com. Accessed June 8, 2016.

Manjikian, Mary. 2015. "But My Hands Are Clean: The Ethics of Intelligence Sharing and the Problem of Complicity." *International Journal of Intelligence and Counterintelligence* 28(4): 692–709.

Nicol, Will. 2016. "A Beginner's Guide to Tor: How to Navigate Through the Underground Internet." January 19. Available at www.digitaltrends.com. Accessed June 8, 2016.

O'Neill, Patrick Howell. 2016. "Former Tor Developer Created Malware for the FBI to Hack Tor Users." The Daily Dot. Available at: https://www.dailydot.com/layer8/government-contractor-tor-malware/. April 27, 2016.

Tor Project. Available at www.torproject.org

Vaas, Lisa. 2015. "FBI Again Thwarts Tor to Unmask Visitors to a Dark Web Child Sex Abuse Site." *Sophos.com*. May 7. https://nakedsecurity.sophos.com/2015/05/07/22fib-again-thwarts-tor

Deontological ethics in cyberspace

Some analysts make deontological arguments about duties in cyberspace. These arguments assume that there is nothing unique about cyberspace and that individuals have the same obligations and duties to their fellow man that they would have in real space. Spinello and Tavani (2005) suggest that individuals are obligated to respect intellectual property regimes since not doing so is a form of theft. He applies the rule of reversibility here, noting that we would not like it if others did not respect our intellectual property and so therefore we should respect the intellectual property of others. And Fisher and Pappu (2006) have suggested that certain practices that occur in cyberspace – such as using bots to generate artificially high numbers of clicks or likes – are actually forms of deception that should be avoided. They argue that the duty not to lie or practice deception holds in cyberspace just as it does in the real world.

In recent years, analysts have also begun asking questions about attribution, trust and deception in cyberspace using deontological ethics, including the ideas of John Rawls. Douglas suggests that in thinking about how internet governance might be used to structure a more equitable and just internet for all users – or stakeholders – one might take the original position. How might you feel about issues like net neutrality, surveillance or rights like anonymity in cyberspace if you did not know if you would be a corporation, an individual user, a person in the developing world, or even someone who did not have access to any internet connected devices? You might be less motivated to make decisions that were only in your own self-interest or the interests of your company (Douglas, 2015). In her work, Smith has asked who would and would not be helped by a requirement that engineers redesign the internet so that it is significantly easier to attribute an action (like a cyberattack) to a specific player. In other words, she asks "What would a just and equitable internet look like?" Here she references Bishop et al.'s (2009) conception of the multiple stakeholders who will be affected by any rule related to attribution: the message sender, the message sender's organization, the

sender's government, the ISP the sender uses, the network backbone providers, the government of intermediate nations through which the message passes, the government of the recipient's country, the organization associated with the recipient and the recipient himself. Thus, they ask what sort of rule might be adopted governing the process of attribution which would not unfairly either privilege or penalize any of the stakeholders (Bishop et al., 2009). Others have suggested that internet access or access to information should be added to the "equal basic liberties" that Rawls listed (Van den Hoven and Weckert, 2008).

Deontological ethics has also affected thinking in robot ethics. As Yu (2012) points out, duty-based ethics requires that the decider have the ability to reflect back upon his or her own actions, in order to ask "What would happen if everyone was able to behave in the way in which I am behaving in every circumstance," and to ask "Am I treating the others in this situation as merely a means to an end?" Thus, he asks whether machines could ever be taught to think morally through the use of deontological ethics, since they are not capable of reflecting back upon their own actions in the same way that humans can. For this reason, analysts such as Arkin (2009) and Wallach and Colin (2010) have suggested that if one believes that machines can be taught to think ethically, it is more likely that they can be taught to calculate the utility of a particular decision with an eye towards maximizing this outcome. That is, machines could eventually learn to think morally using utilitarian ethics, but they are unlikely to become virtuous or to comprehend their moral duties using deontological ethics.

What are utilitarian ethics?

The third lens is utilitarianism. Utilitarianism is sometimes referred to as a teleological or consequentialist theory since it is concerned with the end point or the decision's consequences, rather than the decision maker's attitude or intent. Utilitarianism is newer than virtue ethics. We can trace it back to the ideas of **Jeremy Bentham (1748–1832)**, an 18th century British social reformer. The utilitarian framework arose out of the **Enlightenment**, a period in European history in which society was captivated by the notion that reason or logic could provide a guide to social behavior in the world. Reason was often explicitly described as the opposite of a religious sensibility. Authors thus stated that while religion often told people what to do based on scriptures, religious teachings and centuries of moral practices in society, reason allowed individuals to choose for themselves what the best course of action might be based on more scientific principles. In particular, Jeremy Bentham (1789) argued for a decision-making calculus based on hedonism, or the pursuit of pleasure. He argued that one should always seek to achieve pleasure and to avoid pain. These rules could then be used to govern what we

ought to do. He argued that we can arrive at an ethical decision based on reason and law, rather than looking to religion or any form of higher order. For this reason, we often use the phrase 'utilitarian calculus' to refer to a process of decision making in which individuals weigh up the possible costs and benefits associated with a particular choice.

John Stuart Mill (1806–1873) built upon Bentham's ideas in his own essay, entitled "Utilitarianism." Here he claimed that he wasn't inventing a theory which people would then set out to use in decision making. Instead, he offered a historical look in which he argued that people already unconsciously act like utilitarians, totaling up the possible costs and benefits of undertaking one course of action rather than another. He traces this line of thinking back to the ancient Greeks. He also argues that the 'rules' which Kant identifies in his **deontological ethics** such as "act in the same way that you would want others to act towards you" are in reality based on utility theorizing, since it would make little sense for us to treat our opponents badly if we knew that someday we might be in a situation where they would do the same towards us.

Comparing virtue ethics and utilitarianism

Thus, we can explicitly contrast utilitarianism with virtue ethics, since virtue ethics assumes that the outcome alone is not the most important determinant in deciding what the moral choice would be. Virtue ethics states that one's orientation towards a subject is important, and that it is as important to wish to do good as it is to have a good outcome. Virtue ethics also suggests that an individual's ethical obligations – to act well and with good intent – are largely unchanging since one's character is regarded as unchanging.

Utilitarianism, in contrast, also allows for the possibility of **situational ethics**. Situational ethics suggests that in some circumstances you might need to violate a society's or your own moral code in order to provide the most moral outcome. In utilitarian ethics, the 'best' decision is the one with the highest payoff – or the one that creates the most utility or happiness. Utilitarian ethics also acknowledges that there will be trade-offs. In order to create utility for the many it may be necessary to create disutility or to sacrifice the needs of one or more individuals. Here we can think back to the Trolley Problem. The utilitarian would agree that sometimes it is necessary to push the fat man off the bridge in order to stop the trolley from injuring the children playing on the tracks. The utility derived from saving several children is in this case greater than the loss incurred through the death of the fat man.

Pros and cons of utilitarian ethics

Utilitarian ethics have much to recommend them. When compared to other ethical lenses, the utilitarian model is **parsimonious** – it explains a lot of things while using a fairly simple mechanism. It is also seen as morally neutral since it can be applied

objectively, without regard to one's underlying beliefs or culture. It could be seen as universally valid across cultures and time periods. Here Mill shows that utilitarianism does however, usually line up with conventional morality.

Indeed, Bonnefon et al. (2016) believe utilitarian ethics could be programmed into the driving programs for a self-driving autonomous vehicle (AV). They argue that it is possible to create "moral algorithms that align with human moral attitudes." For example, a programmer could instruct a vehicle to minimize the death toll in the event that a vehicle crash is likely. That is, while an AV cannot monitor its intent (as a human is expected to in practicing virtue ethics), it could calculate likely outcomes using a decision tree and arrive at a 'moral choice' using a utilitarian calculus. Even a self-driving car has the potential to calculate which is the 'lesser of two evils.'

However, there are critics of the theory. First, ethicists have asked if maximizing utility is actually the same thing as doing what is good or what is right. Here, we can imagine actions which a utilitarian approach might prescribe which nonetheless might seem morally or ethically troublesome. For example, imagine a situation where a man who is single and has no dependents is an exact match for an organ donation to a man who has a large family and several people depending on him. One could argue that the greatest amount of happiness would be achieved if the family with many children was allowed to continue to have a healthy father; therefore, the moral thing to do would be to force the single man to donate his organs, even if doing so would kill him. One could also argue that it is moral to force everyone who earns a certain amount of money to donate to charity, since this would maximize happiness for the greatest number of people who would likely receive benefits. In each instance, the rights of the individual are subordinated to the rights of the group, and the proposed solution can be seen as authoritarian (West, 2004, 23).

Military ethicist Edward Barrett (2013, 4) takes this approach, arguing that utilitarian thinking is inappropriate for considering the ethics of cyberwarfare. He argues that individual rights to liberty and dignity "cannot be overridden by a consequence-derived utilitarian calculation," and thus recommends a **Just War** perspective be applied to thinking about ethics in cyberspace. (The Just War perspective takes virtue ethics as its starting point and is explored more thoroughly in Chapter 7 on cyberwarfare.)

Utilitarian ethics in cyberspace

In applying utilitarianism in computer ethics, we again encounter the **uniqueness debate**. Should we have different norms and morals for dealing with one another in cyberspace than we have for dealing with one another in real space? And finally, how do we define 'the good' in cyberspace? Is the same as 'the good' in meat space, or is it somehow different?

Among computer ethicists, Moor (1998, 1999), one of the original framers of the ACM Code of Ethics, strongly promotes a "just consequentialism". He argues that only a universal set of computer ethics is useful and cautions against framing a culturally specific or relative set of ethics. Instead, he feels that we can identify core ideas in computer ethics on which to frame a universal ethical theory. Moor introduces the acronym ASK FOR. He states that "no matter what goals humans seek they need ability, security, knowledge, freedom, opportunity and resources in order to accomplish their projects. There are the kinds of goods that permit each of us to do whatever we want to" (1999, 66). Thus, he suggests that decision makers should embrace policies which allow individuals to have these goods and to avoid the 'bads' described above (death, pain, disability, etc.) Here he also cautions against choosing a policy which appears to provide maximum good in the short-run but which may create unpleasant consequences in the long-run. He asks the reader to imagine a situation where a marketing corporation has the ability to buy a database with vast amounts of detailed personal information about everyone in a country. The good is clear, he argues. The company can sell more products. But in the long-run, people will have less autonomy and freedom as more details about their lives are known (1999, 67).

In their work, Tuffley and Antonio (2016) grapple with the question of how we define 'the good' in regard to information technology. They conclude that:

> In the broadest sense, technology is ethical when it is life affirming, when it helps people grow towards their full potential, when it allows them to accomplish what they might otherwise not be able to.
>
> (Tuffley and Antonio 2016, 20)

Here the claim is that technology's goal is to produce human flourishing and that is the standard by which it ought to be measured. Using this yardstick, a computer engineer can ask "What is the likelihood that more or greater human flourishing would be produced through choosing this action over another?" Here, intent or psychological attitude does not matter and the outcome is primary, as prescribed by the utilitarian ethics approach.

Box 2.5 Application: the ethics of net neutrality

The debate about so-called net neutrality has been ongoing in both the US and abroad for over 20 years. The phrase refers to the ways in which data currently travels across the networks that make up the internet. **Net neutrality** is shorthand for a system that would not discriminate between the users of data or the types of

data which currently travel across the internet. A nation practicing net neutrality would not allow internet service providers (ISPs) to create a system where some people or corporations paid for tiered-service allowing them faster data access and allowing data which they generated to load faster at user sites. Under net neutrality then, all data would travel at the same speed – regardless of whether it was created by an individual blogger, a hospital, a company like Coca-Cola or a Hollywood film company.

Some ISPs argued that they should be able to discriminate among users, since higher fees would discipline users who routinely use more than their fair share of data. They argue that people are routinely disciplined for misusing other public resources (like polluting the air or water). Other analysts argue that some data uses actually are more important and worthy of prioritization. For example, a hospital using data to share images of an operation or medical records should not have to wait because others are watching TV.

However, both the US federal government and many user groups support maintaining net neutrality. And in 2012, the Federal Communications Commission (FCC) adopted new rules aimed at maintaining net neutrality (Turilli and Floridi, 2009, 134). So what are the ethical arguments in favor of net neutrality and how do they fit into the frameworks we are using in this course?

A deontological argument would consider how the people involved were impacted. Are they being treated as important in themselves rather than as a means to an end? The deontological approach also asks about the solution which would be accepted as a universal rule. How would I feel if I were subjected to a two-tiered system of internet access? Would I feel that it was just or equitable? As Grabowski (2014) notes, 83 percent of users believe that internet access is a basic human right which people need in order to fully participate in society (1). Thus, a deontologist would argue that individuals should be given equal access to a resource and that their rights should be supported. Grabowski also makes a **duty argument** in stating the corporations need to consider corporate social responsibility. Here their ethical obligation as ISPs should override any monetary incentives which cause them to provide a tiered pricing model (2).

Another argument rests on the value of community. Here, Bollman argues that "a non-neutral internet could likely spark a new kind of **digital divide** among users" (Bollman, 2010, 1). Our internet community would change if there were two kinds of users – the fully enfranchised and the not fully enfranchised. Some people might have laptops and internet but they could not be full participants in the community in the same way as others might be. The organization

Savetheinternet.com is a group of individuals and groups who are committed to the vision of a "free and open internet" as a community (Turilli and Floridi, 2009, 135).

Google's founders, Larry Page and Sergey Brin, offer a different argument. They put forward a **utilitarian argument, s**tating that perhaps the 'next big idea' will be unable to emerge if entrepreneurs can't access the internet freely and fully without discrimination (Bollman, 2010, 2). They feel that the potential costs of not pursuing internet neutrality will be too great and the benefits from doing so are potentially great. They argue that it is up to government to provide a level playing field for all entrepreneurs.

Sources

Bollman, Melissa. 2010. "Net Neutrality, Google and Internet Ethics." *The Humanist.com*. December 10. Available at https://thehumanist.com/magazine/november-december-2010/up-front/net-neutrality-google-and-internet-ethics. Accessed February 9, 2017.

Grabowski, M. 2014. "Commentary: Telecoms Have Ethical Obligation for 'Net Neutrality'." *Media Ethics* 6(1). Available at www.mediaethicsmagazine.com/index.php/browse-back-issues/193-fall-2014-vol-26-no-1-new/3999037-commentary-telecoms-have-ethical-obligation-for-net-neutrality. Accessed February 7, 2017.

Turilli, Matteo, and Floridi, Luciano. 2009. "The Ethics of Information Transparency." *Ethics of Information Technology* 11: 105–112.

Comparing and contrasting the models

In this chapter, we encountered three models for thinking about computer ethics. The agent-centered virtue ethics model assumes that individuals make decisions and that the most ethical solution is the one that helps an individual to develop his or her character, leading to human flourishing. This model is the oldest one and it is rooted in history and tradition, including religious traditions. It is attractive to individuals today because of its emphasis on the inherent rights and dignity of each individual and because of its requirement that decisions be made and applied consistently. That is, 'the right thing to do' does not vary according to the place or position in which one finds oneself.

The utilitarian model, in contrast, advocates a type of situational ethics where 'the right thing to do' is highly affected by the environment in which decisions are being made. While murdering another human being is seldom 'the right thing to do', a utilitarian might argue that if the person is a future tyrant like Hitler or Mussolini, then it might be ethically appropriate to destroy the one individual in order to achieve an outcome which is better for all. This model purports to be highly rational and universal –

in the sense that one can perform calculations regarding utility in any nation or any culture simply by adding up the costs and benefits of particular courses of action. In this model, as noted, the decision maker's intent is not important. Rather, what counts is the outcome.

Finally, the deontological model considers who might be affected by an ethical decision. Which choice allows the most humane treatment of the participants, not treating them as means to an end but as ends themselves? This model helps us think about technology's effects on people, and how people are affected by technological decision making. This model acknowledges that humans have moral duties and that their duties are to one another.

As we have seen the models require the decision maker to ask a different series of questions before making a decision. Figure 2.1 lays out the decision-making calculus for each approach to 'doing ethics':

In the following chapters, we apply the frameworks to thinking through problems in cybersecurity ethics. We consider privacy, surveillance, military ethics and intellectual property, using the frameworks. As Figure 2.2 indicates, each model or lens highlights certain facets of the issue being considered while downplaying others. Each has strengths and weaknesses, as we shall see in the following chapters.

Model	*Questions to Ask in Ethical Decision Making*
Virtue Ethics Approach	• Which position is in line with or best expresses my values and character? • If I choose this, can I live with myself? • Will it contribute to my own human flourishing/character development?
Utilitarian Ethics Approach	• Which position will give the greatest positive utility and produce the fewest negative consequences? • What costs are associated with each outcome? • What potential benefits are associated with each outcome?
Deontological	• Who will be affected by this decision? • Am I treating others as a means or an end in themselves? • If my actions became a rule and I myself was subject to that rule, would I accept it and view it as ethical?

Figure 2.1 Applying the models

	Pros	*Cons*
Virtue Ethics	• Creates consistent ethical positions across issues • Allows for solutions to new and novel ethical dilemmas • Emphasizes character of decision making	• Compassion problem • Problem of evil • 'Traditional' – and therefore perhaps outdated in new environments
Utilitarian Ethics	• Calculations are clean and often value-free • Can be taught • Used in AI, with robots • Is universally valid, rather than idiosyncratic or based on the values of a particular culture	• There ARE no absolute moral imperatives • Forcing adopting an instrumental view of human beings, as means to an end – rather than valuable, sacred or important in their own right
Deontological	• Focus on those affected by decisions • Reciprocal – forces agent to see himself as both decider and subject of decision	• Overemphasizes duty to individuals over duty to produce the best possible outcome • Can be inflexible in insistence on universal rules • Can be stodgy and risk-averse (Rawls)

Figure 2.2 Comparison of ethical frameworks

Chapter summary

- Over time, different ways of evaluating the ethical aspects of actions have emerged, based on developments in religion and philosophy.
- The three frames considered here (virtue ethics, utilitarianism and deontological ethics) differ in terms of what constitutes ethical behavior – is it acting in line with one's values? Achieving a particular ethical outcome, or acting in line with moral standards?
- **Virtue ethicists** believe that there is some objective list of virtues that, when cultivated, maximize a person's chance of living a good life.
- **Utilitarianism** assumes that one can measure the utility of particular choices and decide rationally which action will yield the most utility. In seeking a particular end, it is possible that other values will need to be compromised, and it assumes that what is 'best' in one situation might not be best in another.
- **Deontological ethicists** believe that humans can use their reasoning abilities to derive an ethical position through asking a series of questions including "What would be the outcome if everyone acted this way?" And "Would I approve of this type of behavior having the status of a universal law?"
- Each framework allows us to make a particular type of ethical argument. The frameworks might not all agree on what the best choice is in a particular situation.

Discussion questions

1. Think about the obligations of a computer security professional. To whom are you ethically obligated in the course of doing your job? Only to your particular client? Or to others who might be impacted by your actions? Do you have a duty to society?
2. Do you think that you ever behave differently online than you do in person? In what ways? Have you ever been tempted to behave less ethically in cyberspace?
3. Many corporations have produced values statements or codes. Consider the "Community Values" of the online retailer eBay:

    i. "We believe people are basically good.
    ii. "We believe everyone has something to contribute.
    iii. "We believe that an honest, open environment can bring out the best in people.
    iv. "We recognize and respect everyone as a unique individual.

v "We encourage you to treat others the way you want to be treated." (eBay "Community Values" at http://pages.ebay.ie/help/community/values.html)

Consider each of these values in turn.

- Which ones fit in with virtue ethics, with utilitarian ethics, and with deontological ethics?
- Do any of these strike you as universal principles or are they all unique to Ebay?
- How do these principles contribute to the sustainability of Ebay as a community in the short term and long term?

Recommended resources

Douglas, David M. 2015. "Towards a Just and Fair Internet: Applying Rawls' Principles of Justice to Internet Regulation." *Ethics of Information Technology* 17: 57–64.

Edmonds, David. 2015. *Would You Kill the Fat Man? The Trolley Problem and What Your Answer Tells Us About Right and Wrong*. Princeton, NJ: Princeton University Press.

Jaipuria, Tanay. 2015. "Self-driving Cars and the Trolley Problem." *Medium.com*. May 23. Available at https://medium.com/@tanayj/self-driving-cars-and-the-trolley-problem-5363b86cb82d. Accessed June 3, 2016.

MacDougall, Robert. 2011. "E-Bay Ethics: Simulating Civility in One of the New Digital Democracies." In Bruce Drushel and Kathleen German, eds. *The Ethics of Emerging Media: Information, Social Norms and New Media Technology*, London: Bloomsbury Academic: 13–34.

Chapter 2 sources

Afthanassoulis, Nafsika. 2012. *Virtue Ethics*. London: Bloomsbury.

Afthanassoulis, Nafsika. No Date. "Virtue Ethics." In *Internet Encyclopedia of Philosophy*. Available at www.iep.utm.edu/virtue/. Accessed June 14, 2016.

Ali, Abbas. 2014. *Business Ethics in Islam*. London: Edward Elgar.

Anscombe, Elizabeth. 1958. "Modern Moral Philosophy." *Philosophy* 33(124). Available at www.pitt.edu/~mthompso/readings/mmp.pdf. Accessed February 1, 2017.

Arkin, Ronald. 2009. *Governing Lethal Behavior in Autonomous Robots*. New York: Chapman & Hall.

Bagnoli, Carla. "Constructivism in Metaethics." In Edward N. Zalta, ed. *The Stanford Encyclopedia of Philosophy*, Spring 2017 Edition. Available at https://plato.stanford.edu/archives/spr2017/entries/constructivism-metaethics/. Accessed April 4, 2017.

Baker, C. Edwin. 1985. "Sandel on Rawls." *University of Pennsylvania Law Review* 133: 895–910.

Barrett, Edward. 2013. "Warfare in a New Domain: The Ethics of Military Cyber operations." *Journal of Military Ethics* 12(1): 4–17.

Barriga, Alvero Q., Morrison, Elizabeth M., Liau, Albert K., and Gibbs, John C. 2001. "Moral Cognition: Explaining the Gender Difference in Antisocial Behavior." *Merrill-Palmer Quarterly* 47: 532–562.

Bentham, Jeremy. 1789. *An Introduction to the Principles of Morals and Legislation*. London: T. Payne & Sons.

Bishop, Matt, Gates, Carrie, and Hunker, Jeffrey. 2009. "The Sisterhood of the Traveling Packets." *Oxford, UK: NSPW Proceedings of the 2009 Workshop on New Security Paradigms*: 59–70.

Bonnefon, Jean-François, Shariff, Azim, and Rahwan, Iyad. 2016. "The social dilemma of autonomous vehicles." *Science* 352(6293): 1573–1576. Available at http://science.sciencemag.org/content/352/6293/1573.

Borowitz, Eugene, and Schwartz, Frances. 1999. *The Jewish Moral Virtues*. Philadelphia, PA: The Jewish Publication Society.

Brey, Philip. 2007. "Ethical Aspects of Information Security and Privacy." In N.M. Petkovic and W. Jonker, eds. *Security, Privacy and Trust in Modern Data Management*. Heidelberg: Springer Berlin: 21–36.

Burnham, Michael. 2016. "Ethical Implications of Data Aggregation." Available at www.scu.edu/ethics/focus-areas/internet-ethics/resources. Accessed June 2, 2016.

Chang, Christina Ling-Hsing. 2012. "How to Build an Appropriate Information Ethics Code for Enterprises in Chinese Cultural Society." *Computers in Human Behavior* 28(2): 420–433.

Douglas, David M. 2015. "Towards a Just and Fair Internet: Applying Rawls' Principles of Justice to Internet Regulation." *Ethics of Information Technology* 17(1): 57–64.

Ellithorpe, Morgan, Cruz, Carlos, Velez, John, Ewoldsen, David, and Boerg, Adam. 2015. "Moral License in Video Games: When Being Right Can Mean Doing Wrong." *Cyberpsychology, Behavior and Social Networks* 18(45): 203–207.

Falk, Courtney. 2005. "The Ethics of Cryptography." *CERIAS Tech Report 2005–37*. (Thesis) West Lafayette, IN: Purdue University.

Fisher, Josie, and Pappu, Ravi. 2006. "Cyber-Rigging Click-Through Rates: Exploring the Ethical Dimensions." *International Journal of Internet Marketing and Advertising* 3(1): 48–59.

Foot, Philippa. 1978. *Virtues and Vices and Other Essays in Moral Philosophy*. Oxford: Clarendon Press.

Gottlieb, Paula. 2009. *The Virtue of Aristotle's Ethics*. Cambridge: Cambridge University Press.

Guthrie, Clifton F. 2013. "Smart Technology and the Moral Life." *Ethics and Behavior* 23(4): 324–337.

Hardin, Garrett. 1968. "The Tragedy of the Commons," *Science*. December 13, 1968. 162, (3859): 1243–1248. Available at: http://www.garretthardinsociety.org/articles/art_tragedy_of_the_commons.html

Harrison, Tom. 2015. "Virtuous Reality: Moral Theory and Research Into Cyber-Bullying." *Ethics of Information Technology* 17: 275–283.

Jaipuria, Tanay. 2015. "Self-driving Cars and the Trolley Problem." *Medium.com*. May 23. Available at https://medium.com/@tanayj/self-driving-cars-and-the-trolley-problem-5363b86cb82d. Accessed June 3, 2016.

Koller, Peter. 2007. "Law, Morality and Virtue." In Rebecca Walker and Philip Ivanhoe, eds. *Working Virtue*. Oxford: Clarendon Press: 191–200.

Kouchaki, Maryam, and Smith, Isaac H. 2014. "The Morning Morality Effect: The Influence of Time of Day on Unethical Behavior." *Psychological Science* 25 (1): 95–102.

Lessig, Lawrence. 2000. *Code: And Other Laws of Cyberspace*, Version 2.0. New York: Basic Books.

Moor, James H. 1998. "Reason, Relativity and Responsibility in Computer Ethics." *Computers and Society* 28(1): 1–16.

Moor, James H. 1999. "Just Consequentialism and Computing." *Ethics and Information Technology* 1(1): 65–69.

Myskja, Bjorn K. 2008. "The Categorical Imperative and the Ethics of Trust." *Ethics and Information Technology* 10(4): 213–220.

Olivier, Bert. 2013. "Is There a Need for Cyber Ethics?" *Thought Leader*. July 28. Available at http://thoughtleader.co.za/bertolivier/2013/07/28/is-there-a-need-for-cyber-ethics/. Accessed February 2, 2017.

Sandel, Michael. 1998. *Liberalism and the Limits of Justice*. Cambridge, MA: Cambridge University Press.

Schejter, Amit, and Yemini, Moran. 2007. "Justice, and Only Justice, You Shall Pursue: Network Neutrality, the First Amendment and John Rawls's Theory of Justice." *Michigan Telecommunications and Law Review* 14(1): 137–174.

Schroeder, Drew. 2007. "Rawls and Risk Aversion." Unpublished Manuscript. Available at www1.cmc.edu/pages/faculty/ASchroeder/docs/RawlsMaximin.pdf. Accessed February 8, 2017.

Slingerland, Edward. 2011. "The Situationist Critique and Early Confucian Virtue Ethics." *Ethics* 121: 390–419.

Smith, Jessica. 2016. "Attribution From Behind the Veil of Ignorance." *The National Interest*, November 14. Available at http://nationalinterest.org/feature/the-great-cybersecurity-attribution-problem-18385. Accessed April 9, 2017.

Spinello, Richard A., and Herman T. Tavani. 2005. "Intellectual Property Rights: From Theory to Practical Implementation" In Richard A. Spinello and Herman T. Tavani, eds. *Intellectual Property Rights in a Networked World: Theory & Practice*. New York: IGI Global: 1–6.

Tuffley, David, and Antonio, Amy. 2016. "Ethics in the Information Age." *Australian Quarterly* January–March: 19–24.

Vallor, Shannon. 2013. The Future of Military Virtue. In: Karlis Podins, Jan Stinissen, and Markus Maybaum, eds. *5th International Conference on Cyber Conflict*. Tallinn, Estonia: NATO CCD COE Publications.

Van den Hoven, Jeroen. 2008. "Information Technology, Privacy, and the Protection of Personal Data." In: Jeroen van den Hoven and John Weckert, eds. *Information Technology and Moral Philosophy*. New York: Cambridge University Press.

Van den Hoven, Jeroen, and Weckert, John, eds. Information Technology and Moral Philosophy. New York: Cambridge University Press.

Walker, Rebecca, and Ivanhoe, Philip. 2007. *Working Virtue*. Oxford: Clarendon Press.

Wallach, Wendell, and Colin, Allen. 2010. *Moral Machines: Teaching Robots Right from Wrong*. Oxford: Oxford University Press.

Walsh, Adrian. 2011. "A Moderate Defense of the Use of Thought Experiments in Applied Ethics." *Ethical Theory and Moral Practice* 14(4): 467–481.

West, Henry. 2004. *An Introduction to Mill's Utilitarian Ethics*. Cambridge: Cambridge University Press.

Yu, Sherwin. 2012. "Machine Morality: Computing Right and Wrong." May 10. Available at http://www.yalescientific.org/2012/05/machine-morality-computing-right-and-wrong/. Accessed December 3, 2016.

3 The ethical hacker

Learning objectives

At the end of this chapter, students will be able to:

1. Define hacking and describe how computer hacking has changed and evolved since its inception
2. List at least five reasons why hackers engage in hacking activities and describe types of hackers
3. Compare and contrast the conditions and approaches of white hat, grey hat and black hat hackers
4. Describe the licensing mechanisms currently used for certifying an ethical hacker
5. Provide an evaluation of the ethics of hacking and penetration testing using a virtue ethics, a utilitarian and a deontological framework

    - In considering the ethics of hacking, we need to consider several factors – including who the hack targets, the intents of the hacker, and the conditions under which the hack takes place.

As we consider the ethical problem of hacking in this chapter, we can consider five real-life situations involving the use of hacking by a computer specialist or an amateur:

- In spring 2011, Britain's government investigated journalistic culture, practice and ethics. The investigation began when it became clear that journalists for several leading British newspapers had hired a private investigator who had used technology to eavesdrop on cell phone communications of celebrities and other newspapers in order to gather additional information. Individuals whose communications were alleged to have been hacked included the British Royal

Family, singer Paul McCartney and author J.K. Rowling. The public was particularly disturbed to hear that journalists had accessed the cell phone account of a missing British school girl, Milly Dowling, and downloaded her voice mail messages. When Milly's family and the police saw that her messages had been downloaded, they thought she might still be alive, rather than assuming that her phone had been tampered with. This scandal led to the shutdown of a newspaper (*News of the World*), the resignation of several figures in British journalism and politics, jail terms for some participants and the payment of damages to victims of these crimes (Carlson and Berkowitz, 2014).

- In spring 2016, the US Federal Bureau of Investigation paid a professional hacker 1 million dollars to bypass security protocols to gain access to the cell phones of Tashfeen Malik and Syed Rizwan Farook. In December 2015, Malik and Farook carried out a terror attack at Farook's workplace which killed 14 and injured 21. The FBI first asked the Apple Corporation for help in accessing the phones but they refused. Then the FBI hired a hacker. They argued that the hacker actually helped Apple through identifying a security flaw in the iPhone which could then be addressed (Nakashima, 2016).
- Self-identified geek Jay Garmon tells the story of the "Konami Code," a sequence of commands that video gamers use to cheat the system, making it easier and faster to complete a video game. Using the code, you can program your avatar to begin the game with 30 lives instead of one, for example. Garmon describes the Konami code as a beloved part of geek culture. He argues that programmers who put surprises like secret commands and graphics (known as "Easter Eggs") in their games actually want users to hack the games to find the rewards. Thus, he suggests that users and creators are often ethically complicit in the cheating which occurs (Garmon, 2007).
- In spring 2015, a group of University of Virginia researchers showed how a hacker could take control of a self-driving car and issue commands to interfere with the car's braking and steering mechanisms, potentially injuring the car's passengers as well as pedestrians and occupants of other vehicles (Pell, 2015).
- In spring 2016, the CEO of a hospital in Texas showed how hospitals are vulnerable to hacking of medical devices like pacemakers, insulin pumps and automated medication dispensers. Such hacks could have fatal consequences (Mace, 2016).

What do these stories have in common? Each involves the use of a 'hack' and each presents an ethical dilemma. In some ways, the stories are similar: In each instance,

someone with specialized knowledge was able to gain access to a system, outsmarting and outwitting any defenses which had been created against entry. But the stories are also very different: In four of the instances, someone could potentially be harmed or damaged as a result of the hack, even fatally. In some of the instances, the hack was clearly illegal while in other instances, the hacker actually worked with law enforcement! These stories allow us to consider who the hacker is, what his intent is, who his target is, and the actions which he carries out. As the examples show, not all hackers are malicious, and hacking can have a variety of repercussions – emotional and social, financial, legal and political.

In this chapter, we consider what hacking is and is not, the ways in which the so-called hacker ethic has changed and developed over time as computer security has become more professionalized and the differences between white hat, gray hat and black hat hacking.

What is a hacker?

A **hack** refers to an unconventional way of doing something. Hacking a program thus might mean using code written to accomplish one task and modifying it so that it can be used to carry out a different task. When the term originated in the 1980s, it was often applied to individuals like Steve Jobs and Bill Gates, who were seen as engaging in heroic and creative endeavors which produced new technological resources which enriched society.

However, today hacking has both a negative and a positive meaning. A hacker can be someone who wants to show off, to do things more efficiently or to aid his community by making a resource more widely available. At the same time, a hacker might be someone who is committing criminal acts, injuring others and causing social disruption. Today, the term is often used to denote someone who wishes to gain *unauthorized access* to a system (for example, if an individual working in one section of a corporation looked at files belonging to another section of the corporation for which he had not been given permission) or it might mean gaining *illegal access* to a system (through utilizing stolen passwords, impersonating another user or simply using an algorithm to guess a password).

While hacking may have initially begun in the early days of the computer revolution as merely a type of game or joke, today hacking is often viewed as a type of **cybercrime**. Technopedia defines a cybercrime as "a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes) (Technopedia.com, 2017)." Hobbyist

hackers may offer their skills to the highest bidder and those skills may often be purchased by syndicates run by cybercriminals. Today's hackers may engage in acts which are considered vandalism, destruction of property and theft. Here, some analysts, like Brey (2007, 27) distinguish between **hacking** and **cracking**, reserving the term cracking for malicious activities intended to harm systems or data. Today, most analysts agree that certain activities which fall broadly under the umbrella of hacking can also be described as variants of cybercrime. Here, Tavani (2004, 121) includes:

Cybertrespass – the use of information technology to gain unauthorized access to computer systems or password-protected sites

Cybervandalism – the use of information technology to unleash programs that disrupt the operations of computer networks or corrupt data

Computer fraud – the use of deception for personal gain in online business transactions by assuming a false online identity or by altering or misrepresenting data

Cyberterrorism – the execution of politically motivated hacking operations intended to cause grave harm that is, resulting in either loss of life or severe economic loss or both.

Returning to the definition of cybercrime, we see that cybercrimes may include attacks specifically upon hardware or software with the intention of damaging a system or data, but that cybercrime might also include 'regular crimes' which are carried out through relying on technology to achieve their effect. (That is, one can either steal a physical credit card, or one can steal someone's credit card data in cyberspace. Both represent a type of theft, but the second instance is also a cybercrime, since a computer was used as a means of carrying out the theft.) Hacking and the use of technology can thus be used to carry out additional crimes like cyberstalking and cyberbullying. Here, information gathered through the internet might enable an attacker to know where to find a victim or to identify the victim's vulnerabilities.

Thus, hacking is often unlawful. Certain hacks violate a variety of federal and state laws. In the United States, the **Computer Fraud and Abuse Act (CFAA)** spells out the federal punishments related to hacking which includes and imprisonment of up to 20 years. Additional US federal laws include the Wiretap Act, the Unlawful Access to Stored Communications Law, the Identity Theft and Aggravated Identity Theft Laws, the Access Device Fraud Law, the CAN-SPAM Act and the Communication Interference Act.

In addition, hacking is mentioned in the **US Patriot Act**, legislation on US national security which was passed in the aftermath of the 9-11 terrorist attacks. The Patriot Act notes that breaking into federal computers may fall under definitions of terrorism and cyberhackers can be prosecuted as terrorists (Young et al., 2007, 281). On a state level, hacking behaviors may also be in violation of laws regarding phishing and the use of spyware (Hackerlaw.org). Similarly, in Great Britain, the Terrorism Act of 2000 listed engaging in computer hacking or threatening to engage in computer hacking a potential terrorist act. If the hacker was doing so in support of a political, religious or ideological cause, or because s/he wanted to influence the government or intimidate the public or some segment of the public, then it is considered terrorism (Inbrief.co.uk). Hackers in the UK can also be prosecuted according to the Criminal Damage Act 1971 and the Computer Misuse Act (www.inbrief.co.uk/offences/hacking-of-computers).

Is hacking always wrong?

It is too simplistic, however, to say merely that all hacking is always ethically wrong, or that all hacking can be ethically justified. Similarly, not all hacking is illegal. Instead, as we will see in this chapter, there are several factors that we need to consider – from who the hack targets, to the intents of the hacker, to the conditions under which the hack takes place.

In their work, Bratus et al. (2010) suggest that hacking is actually ethically neutral. They define 'hacking' as merely a package of skills which computer experts can develop, arguing that "Hacking is the skill to question trust and control assumptions expressed in software and hardware, as well as in processes that involve human(s)-in-the-loop (a.k.a. 'Social Engineering.')." Thus, hackers acquire and use skills like the ability to encrypt and decrypt data, the ability to create and transmit viruses and the ability to identify and diagnose security vulnerabilities within a computer system. They argue that just like doctors, locksmiths or martial artists could use their skills either to aid humans or to harm them, hackers are not constrained to act either ethically or unethically. It is moral reasoning, they argue, in the last analysis that will determine how hackers use the skills that they have developed.

Box 3.1 Application: sharing passwords

An article in *Consumer Reports* (2015) presents the following scenario: Hans has spent the last several years watching free Home Box Office movies and television series using a log-in which belongs to his sister's ex-boyfriend. Should Hans feel guilty about this action? And is it unethical? Why or why not? We will use our three frameworks – virtue ethics, utilitarian ethics and deontological ethics – to consider this question.

Virtue ethics

Virtue ethics considers how one's decision to share a password reflects upon one's identity as a moral person. Key values to consider are sharing, altruism, generosity, theft and integrity. Biddle (2013) feels that "sharing" a password is an act of altruism or generosity. However, a generous person donates his own resources while the password sharer donates someone else's resources (e.g., Netflix's or HBO's resources). And a generous person decides to give even doing so involves a sacrifice.

Furthermore, Aristotelian virtue ethics acknowledge that charity and giving are good, but still place some conditions on the particular act of giving. Charity should be towards a worthy end, like giving money to construct a beautiful building, not so that someone can watch Game of Thrones without paying. In addition, Aristotle explicitly notes that a virtuous act of accepting charity would not include taking the fruits of either theft or gambling (Gottlieb, 2009, 83).

Utilitarian

Utilitarians would consider the outcomes generated by the decision to share, rather than focusing on the intent of the user. In looking at outcomes, we can make a utilitarian argument for and against sharing passwords. Clearly, the most expeditious outcome is one where the maximum number of people allowed or permitted enjoy the programming. Thus, since Netflix allows four users to be enrolled and HBO Go allows up to six streams, it would be ethical to share up to these maximums. Here, a utilitarian would also note that the total sum of resources is not deleted by the fact that an additional person has access to them. In this way, adding an additional watcher to a streaming movie is different from downloading a product and keeping it, both because the watcher does not receive a tangible item (as he would in theft) and because one person's ability to view something does not keep others from viewing it at the same time or later.

Utilitarians might also suggest that sharing creates an additional good like security, since sharing passwords allows you to monitor the behavior of others (Fleischmann, 2015). Thus, a parent could care for their child's moral and spiritual growth through monitoring what they watch.

However, Margaret Sullivan, an editor at the *New York Times*, argues that many content providers today – including newspapers and magazines – face economic woes when free riders use services without paying. If sharing could ultimately bankrupt Netflix, Amazon and others, then this is an additional cost for utilitarians to consider.

Deontological ethics

A deontologist would consider two factors: the ways in which we might react if a similar action was taken against us, and the question of whether one could format a universal law in which such behavior might be either allowed or disallowed. How would you feel if you lent someone an item and found that they subsequently shared it with others without your consent or knowledge? What if you hired a house sitter to tend your house while you were away and later found out that s/he had a party at your house without your knowledge or consent. You might feel violated or harmed. Thus, we should conclude that the service provider is also harmed by such actions.

We also find that it is impossible to format a universal law which states that "It is always appropriate for the recipient or purchaser of an item to share it and distribute it widely without the provider's knowledge or consent," since such a law would allow for sharing a computer password, but not for physical items such as a house or a car.

Sources

Biddle, Sam. 2013. "It's Time to Stop Sharing Your Netflix Password." *Gizmodo*. March 13. Available at http://gizmodo.com/5990315/its-time-to-stop-sharing-your-netflix-password. Accessed March 12, 2017.

Cauterucci, Christina. 2015. "Ex Flix: Do Couples Need Prenups for Their Shared Streaming Passwords?" *Slate*. October 26. Available at www.slate.com. Accessed June 13, 2016.

Consumer Reports. 2015. "IS It OK to Share Log-Ins for Amazon Prime, HBO Go, Hulu Plus or Netflix?" *Consumer Reports*. January 28. Available at www.consumerreports.org/cro/magazine/2015/01/share-logins-streaming-services/index.htm. Accessed March 2, 2017.

Fleischmann, Glenn. 2015. "Family Sharing Is Convenient But Comes With Its Own Risks." *MacWorld* 32(2). February. Available at www.macworld.com/article/2861024/family-sharing-is-convenient-but-comes-with-its-own-risks.html. Accessed March 12, 2017.

Gottlieb, Paula. 2009. *The Virtue of Aristotle's Ethics*. Cambridge, UK: Cambridge University Press.

Sullivan, Margaret. 2013. "Times' Writer Tangles With the Ethics of Password Sharing." *New York Times*. April 10. Available at http://publiceditor.blogs.nytimes.com. Accessed March 3, 2017.

Technopedia.com. 2017. "Cybercrime (definition)". Available at: https://www.techopedia.com/search?q=cybercrime&section=terms. Accessed August 20, 2017.

Van Allen, Fox. 2015. "Is It OK to Share Your Netflix and Hulu Passwords." *Techlicious*. January 30. Available at www.techlicious.com. Accessed June 13, 2016.

Whitty, Monica, Doodson, James, Creese, Sadie, and Hodges, Duncan. 2015. "Individual Differences in Cyber Security Passwords: An Examination of Who Is Sharing Passwords." *Cyberpsychology, Behavior and Social Networking* 18(1): 3–7.

Wortham, Jenna. 2013. "No TV? No Subscription? No Problem." *New York Times*. April 6. Available at www.nytimes.com/2013/04/07/business/streaming-sites-and-the-rise-of-shared-accounts.html. Accessed March 3, 2017.

At the same time, many hackers argue that running a system which is poorly protected – through choosing a common password; using open source code as part of your systems' internal programs; or being careless about corporate security – is the equivalent of leaving your door open and being surprised when your house is robbed. They argue that users are responsible for having strong security and that users are therefore responsible when their systems are hacked, and not the hackers. Indeed, some hackers argue that they are performing a public service in letting companies know that their systems are vulnerable.

However, Xu et al. (2013) caution that while hackers might start off innocently they may over time be drawn into engaging in less ethical pursuits. These authors stress that the best predictor of whether someone will continue to engage in mischief or move on to more harmful pursuits is their own ability to engage in moral reasoning. Students who understand that their actions have ethical consequences can, they argue, set limits regarding what behaviors cross an ethical line.

Why do people hack?

In considering the five cases encountered in this chapter's beginning, we see that hacking is a very broad term, covering everything from mischievous activities to

those which are illegal and possibly life-threatening. The five cases differ in three ways. First, not all of these hackers had the same intentions. Those who aided the FBI wanted to help law enforcement respond to a terrorist incident, those who cheated on the video game wanted to win the game, and those who hack into cars and medical devices may actually want to kill or injure others. Next, we see that hacking has a variety of consequences – a hacker can cause an airplane to fall out of the sky, or he can change the score on a video game. Finally, these examples show that ethics and law do not always line up neatly. Some actions are both illegal and unethical (i.e. the cell phone hacks in Britain), some are arguably illegal yet ethical (i.e. "breaking into" a cell phone that does not belong to you as the hackers did when they aided the FBI) and some might be legal but still unethical (i.e. perhaps "cheating" on a video game).

In one case, we can identify specific individuals victimized by a hacker (the family of Milly Dowling). However, in other cases, the situation is more complicated. In the case of the San Bernardino i-Phone, the federal government served the Apple Corporation with a warrant, allowing them to search the device on the grounds that the individuals constituted a threat to national security. Here, the understanding is that the two individuals had a right to not be the subject of unreasonable search and seizure under the Fourth Amendment to the United States Constitution. However, that right was revoked when they engaged in a terrorist activity. In this case – in comparison to the British case – the search was thus legal and arguably ethical as well. In the case of the Konami Code, many hackers argue that finding and using cheat codes is half the fun of playing a video game. They argue that no one else is hurt through one player's use of a cheat code, and that in fact, some games can only be completed through the use of cheat codes.

In considering the types of hacking behavior, then, we can place acts on a spectrum, ranging from least to most harmful. As we move along the line from least to most severe, we can see that the type of person liable to engage in the activity changes, as do the types of attacks, the level of organization of the groups, and the overall destructiveness of the acts themselves. Figure 3.1 illustrates the various types of hacks which are possible today, in increasing order of severity.

Type of Attack	*Includes*	*Motivation*	*Target*	*Type of Attacker*
Nuisance	• Cheating on a video game • Playing pranks	• Demonstrate skill • Enhance reputation • Learning	• Individuals – either general or selected	• Least well organized – might be students or youth
Activist	• Attempts to change the outcome of political events – including leaking information, tampering with elections, political doxing	• Ideological	• Public figures • Corporations	• May be small or large organization • Either spontaneous or more permanent in nature
Crime	• Identity theft • Theft of assets • Installation of spyware, malware & ransomware	• Money • Profit	• Individuals • Rival corporations	• May be individual or criminal syndicate • Ties to organized crime
Acts of War	• Attacks on critical infrastructure Changing of coordinates for military targeting • Acts of a terrorist nature.	• Supplement conventional warfare • Cripple opponent • May be ideological (cyberterrorism)	• States • Nonstate actors	• States including military units (Cybercommand) • Nonstate actors

Figure 3.1 Types of hacks

(Based on information provided in Khalilzad and White, 1999; Fry, 2013)

As the chart indicates, hackers may have more than one motive, and a hacking attempt may be a 'one off' event, or related to a larger strategy. In particular, it is becoming more difficult to distinguish between those hacks like **political doxing** which might include the release of embarrassing information about a political official, and acts of war. As we saw in the case of the 2016 United States presidential elections, activist hacks which target the integrity of a political process may be as serious a threat to a nation as a traditional military cyber strike. As Schneier (2016, 1) argued in the Schneier on Security Blog, attacks which are aimed at calling into question the legitimacy of an election can threaten the "very core of our democratic process." When actors, including activist groups or other nations, interfere in domestic political events in another country, it may go beyond simple activism to actually constituting a crime according to international law.

The professionalization of hacking

In considering where our ethics regarding hacking come from today, we can consider how the earliest computer hackers, working at MIT in the 1950s and 1960s, conceptualized their activities. Here, Brey (2007, 27) defines a **hacker ethic** as "as "a

set of (usually implicit) principles that guide the activity of many hackers." He notes that for early hackers, these principles included a conviction that information should be free and that access to computers should be unlimited.

However, the principles identified by early hackers did not constitute an ethical system or set of professional ethics as we conceptualize them today. Today, groups like the Association of Computer Machinery have formally drawn up codes of ethics and professional standards based on a common understanding of the project of computer science and computing. Such standards help practitioners to understand their role in this project, the mission of computer science, and the standards of behavior and values which practitioners should adopt in order to participate in this project. In contrast, in the earliest days of the internet, hacking was not yet a profession, with the hallmarks which describe a profession. There were no clear standards by which one trained as a hacker, including professional credentials which one could obtain. There were no licensing standards for entering the hacking profession, and most importantly, there was not a unified understanding of what it meant to be a hacker, or what the mission of hacking was. Rather, a large number of individuals used the term hacker to refer to themselves, and they came from a variety of backgrounds, with some possessing academic credentials as computer scientists, while others were largely self-taught. Finally, today, professional organizations may point to ethical codes and standards as a way of policing the behavior of their members, ensuring that they meet and uphold professional standards. In contrast, the old hacker ethic was unenforceable and lacked a formal organization with a commitment to enforcement.

We can thus describe the old hacker ethic as an ideal, a policy statement or an aspirational set of ethics – a statement of what hackers saw their activity as at present and what they imagined it could be in the future – rather than a code of ethics. Furthermore, this early hacker ethic evolved not from a shared project which hackers subscribed to, but instead was derived from what early hackers saw as inherent properties of the internet as they then understood it. Thus, it was **technologically deterministic**, since the technology itself was seen as driving and setting the rules for what it should be. In this rendering of ethics, ethical values were not derived from individual character (as they are in virtue ethics) or even based upon the possible consequences of actions in cyberspace (as they are in utilitarian ethics); instead, the values and ethics of cyberspace were seen as coming out of facets of the technology itself. This ethic described what technology 'wants to be,' or the ways in which technology could and should fulfill its own destiny.

The hacker ethic – as articulated by Levy (1984) – had three parts: Hackers were committed to the free and open access to information (expressed in the phrase "information wants to be free"). In this ethic, individuals who worked to reveal information, including that which was password protected or encrypted, were heroes, since information brought freedom. Here, a high emphasis was placed on information sharing, and hackers strived to violate boundaries which individuals, groups or governments placed around information, viewing them as a challenge to be surmounted. This 'ethic,' then, favored transparency over secrecy. Next, hackers were committed to a hands-on orientation towards the internet, wanting not to be mere consumers, but instead to actively create this new medium. They prided themselves on building the internet and its structures from the ground up, and distrusted top-down authority. Finally, hackers were "techno-utopians", who had an overwhelmingly positive orientation towards this new technology, believing that it could be harnessed to solve social problems as well as to create truth and beauty (Levy, 1984).

The old hacker ethic was thus **libertarian** in orientation, in favor of limited government intervention in this new medium. This ethic was expressed in arguments made by people like Paul Barlow in his **Declaration of the Independence of Cyberspace**, in which he stated that nations should not have sovereignty over what internet is, but that instead, the internet should be ungoverned, free of government interference and a place where everything should be allowed.

In addition, the old hacker ethic rested on an understanding that information was not merely something to be used by people but rather something which existed, to some degree, independently of the users. Information was seen as having agency or independent self-will; there were clearly right and wrong ways of using information, according to this view, and these rules came from inherent properties of the technology itself. This old hacker ethic suggested that individuals should use their skills to uncover information on the internet, without letting barriers like privacy concerns or copyright stand in their way. Such exercises were seen as a way of exercising creativity, rather than intrusions upon individual or corporate rights.

New and old hacker ethics

By the mid-2000s, however, some analysts declared the old hacker ethic no longer relevant, seeing its values and behaviors as at odds with new developing notions of what it meant to be an ethical participant on the internet. Tavani (2004) argued that 'information should be free' had been superseded by new ideas regarding intellectual property in cyberspace, and that while values like sharing and creating shareware had been important, an emphasis on open source code and shareware did not mean that

developers and creators never had a claim to ownership of their property, or that they should be obligated to share all of their work. Hacker began to be used as a pejorative term to label individuals whose behavior would – in other environments outside of a virtual world – be seen as anti-social, deviant or criminal. Some analysts argued that the so-called 'hacker ethic' was mostly a justification that these individuals had come up with to excuse behavior that they knew was criminal (Young et al., 2007, 286).

Furthermore, analysts rejected the idea that the internet itself had values which should provide the basis for an ethics in cyberspace. They did not accept technologically deterministic and utopian arguments which suggest that the internet is necessarily associated with freedom and democracy, and that left to its own devices, the internet will necessarily develop into a medium which brings democracy. Indeed, analysts like Evgeny Morozov have begun to argue the reverse – that the internet is just as capable of becoming an instrument for surveillance and depriving citizens of rights. Here he argues that the technology acts differently depending on whose hands it winds up in. An authoritarian government can and will use the internet differently than a democratic government will. That is, humans are seen to have agency or free will in setting and enforcing the parameters and ground rules for hacking and other behaviors in cyberspace.

Box 3.2 Going deeper: the Electronic Frontier Foundation

The Electronic Frontier Foundation (EFF) is a US-based nonprofit organization which began in San Francisco in 1990, with the mission of championing civil liberties in cyberspace. In the past 25 years, the organization has expanded its reach worldwide. With a staff of technologists, lawyers and policy experts, the EFF has weighed in on many of the most controversial issue which have arisen as the internet has expanded in scope and reach.

EFF leaders have testified in the US Congress on issues as diverse as: unwarranted surveillance of US persons by the US National Security Agency; the matter of net neutrality, on privacy issues related to users' medical and legal data; and whether legislation is needed to stop online trolling. They have also defended the rights of bloggers to be treated as journalists and to enjoy the same rights to freedom of speech that journalists enjoy.

The EFF also carries out research in regard to many political, legal and ethical issues which arise in cyberspace. Recently they have examined a situation in which Facebook and other social media providers have taken down or removed content in response to user complaints, and have weighed in on the matter of so-called 'fake news' (i.e. manufactured stories placed in social media for political or ideological purposes).

Throughout their history, the EFF has been at the forefront of addressing how issues regarding First Amendment rights (i.e. the right to free speech, freedom of the press and freedom to assemble) and Fourth Amendment rights (the right not to be subject to illegal search and seizure) should be interpreted and protected in cyberspace.

Source

The Electronic Frontier Foundation. 2016. www.eff.org

As Figure 3.2 shows then, some old hacker ethics directly violate some current conventional understandings of cybermorality. Many of the behaviors supported by the old hacker ethic – such as seeking out information which had been protected behind a firewall, or using and sharing information which was copyrighted – are considered unethical and illegal in our present environment. In particular, Floridi's work on information ethics suggests that invading the privacy of individuals through improperly sharing information may upset the information environment (termed the 'info sphere') and thus should be avoided. Furthermore, he suggests (2005, 182) that information is not merely 'information', but that information about particular people is an important aspect of who they are; when that information is taken, shared or used without their knowledge or consent, he argues, it is as though something has been stolen from them. Since doing so harms an individual, he thus argues that it is an ethical breach and something that should be avoided.

	Old Hacker Ethic (1970s, 1980s)	*New Hacker Ethic (1990s –present)*	*Professional Hacker Ethic*
Source of Ethical Values	• Properties of the internet itself	• Hacker community defines values	• Professional organization sets behavior norms/ standards
Intellectual Property/ Ownership	• Does not exist • "Information wants to be free" • Internet users have an obligation to share their work	• Share code, don't freeload	• Respects intellectual property and rules governing IP and IP theft in cyberspace
Privacy	• Transparency and openness are more important than privacy • No inherent right to privacy in cyberspace	• People have right to privacy	• The theft of people's personal information is harmful to them – it is not ethically justifiable
Role of Government	• The internet is being built from the bottom up by individuals and groups • The internet can govern itself as a community	• Internet should be self-governing	• Nations can 'own' and regulate cyberspace (Russian cyberspace, Chinese cyberspace)
Relationship between Meat Space and Cyberspace	• Two entities are separate • Real world authorities and rules have no place in cyberspace	• The worlds are linked	• Virtual identity and real identity are linked • Nations, international organizations can govern and establish norms in cyberspace
Role of Laws	• Laws don't apply to cyberspace	• Community should govern itself	• Real world laws apply to cyberspace

Figure 3.2 Comparing and contrasting hacker ethics

While the old hacker ethics have been superseded by new ethics, it is nonetheless important to consider what these ethics were and the arguments behind them because they still resonate within the hacker community. Today, groups like **WikiLeaks (**a hacker collective committed to sharing information including classified information with users in cyberspace); **Anonymous** (a vigilante type group committed to enforcing behavioral norms in cyberspace); and individuals like **Edward Snowden** (the American citizen who leaked information in 2006 about the US National Security Agency's large-scale surveillance efforts against American citizens and others within the international system) all reference old hacker ethics to justify their behavior. WikiLeaks and Snowden have claimed that they do not recognize laws which make certain types of material classified and not readily available to the general public, while groups like Anonymous claim that they are enforcing norms in cyberspace. In addition, individuals reference old hacker norms in explaining why spaces for selling pirated and illegal items (like Pirate Bay) or systems for anonymizing activities in cyberspace (like Tor) should exist. Some criminologists suggest that as long as individuals are being socialized into these old hacker norms, law enforcement activities against illegal hacking and cracking are likely to fail – since some

cybercriminals do not actually view their behaviors as wrong or criminal, but instead defend them as virtuous – according to another set of ethics (Young et al., 2007, 286).

If, as Figure 3.2 suggests, many old hacker ethics no longer apply, what then are the new hacker ethics which have arisen to replace them? In the mid-1990s, Mizrach determined that there are ten core values associated with new hacker ethics. This new hacker ethics is not based on qualities of the technology, but rather on the notion of a community. In this new set of ethics, hackers are asked to see themselves as members of a community and to think about whether their actions help or harm the community of hackers and internet users. Thus, it considers the situations and the interests of those affected by hacking, rather than merely justifying the actions of the hackers themselves.

In the new hacker ethics, the first principle is expressed as "above else, do no harm," and it resembles the injunction which appears in the physician's Hippocratic Oath. This hacker code of conduct also includes cautions against engaging in certain behaviors – including hacking for profit and selling out; freeloading, or taking advantage of open source code without giving back; and trashing and crashing systems, doing damage, and destroying data. The new hacker code builds in a value of restraint, asking hackers to be aware of their capabilities but to use judgment in deciding when and under what circumstances to exercise these capabilities. In this new hacker code, pranking is okay but not doing expensive damage. Similarly, this ethical code states that one can borrow some things but not others – a piece of code but not a credit card number. This ethic also acknowledges the rights of others on the internet, acknowledging that spying and invading people's privacy is wrong.

However, the new hacker ethic, like the older hacker ethic, does not acknowledge the right of states and the police force to control cyberspace, instead arguing that it should be self-governing. Thus, even in the new hacker ethics, there appear to be prohibitions against turning other hackers in or working with police to capture other hackers. Many new hackers still have a libertarian leaning, arguing that hacking is necessary to defend users against a dystopian future of massive government interference. Other ethics include an injunction against wasting resources, which Mizrach describes as the 'joy rider's ethic.' Here he states that if something is just lying around (such as extra bandwidth, storage space for files on a server, etc.) then hackers can and should make use of it.

The new hacker ethics, like the old hacker ethics, emphasize creativity and the invention of new knowledge. Brown (2011, 2) states that:

> Hacking is often about exploring and demonstrating possibilities. Hacking is about exploring a possibility space and about discovering exploits. It may result in the release or theft of personal information or in the breakdown of a web service, but this is often a byproduct of an initial attempt to demonstrate possibility.

Certain aspects of the new hacker ethic are then explicitly utilitarian. Actions are defended by looking to the outcomes which they create. Brown thus argues that if one explores and ultimately finds a security vulnerability and notifies the company, then one has actually contributed something positive. He also implies that the hacker's motive is often one of creative exploration rather than wishing harm upon the target.

The new hacker ethic also includes what has been called the **communication imperative**. This ethic or value notes that people have the right to communicate and associate with their peers freely. Thus, hacking over a firewall if you live in an authoritarian country represents an ethical use of hacking. Here, the International Telecommunication Union (ITU) describes freedom of association/communication as a fundamental human right. Other hackers also include freedom of the press and freedom of information as laws and values which uphold the ethic of communication.

Development of a professional code

As we have noted, over time, computer security has become an established profession with its own professional organizations and licensing mechanisms. Today, we can also point to the professionalization of principles for hackers, including the possibility of becoming licensed as a Certified Ethical hacker. An **ethical hacker** or **white-hat hacker** works for or with a private corporation or government agency to test their system's security. He or she may run tests – including conducting attempts to penetrate the system or using social manipulation tactics like phishing – in order to identify system vulnerabilities. He or she then makes recommendations to the client regarding how to address these vulnerabilities. The ethical hacker thus doesn't seek to harm a corporation but rather impersonates a hacker (thinking like the enemy) in order to help the corporation to better protect itself.

Today, over 50,000 individuals have received the Certification in Ethical Hacking from the International Council of E-Commerce Consultants (EC Council). The certification is endorsed by the United States National Security Agency and the Department of Defense, and individuals throughout the world have taken the test to achieve the certification. In addition, the Certified Ethical Hacker Code of Ethics requires that certificate holders agree not to participate in any underground hacking community activities which involve black hat activities, and not to participate or

associate with black hat community activities which endanger networks (CEH Candidate Handbook v2.0). In addition to agreeing to work in an ethical manner for those who might employ them, white hat hackers often also contribute to the community of computer science professionals as well. Many participate in so-called "**bug bounty programs**," reporting on security vulnerabilities which they have found in corporate or government computer systems.

Box 3.3 Going deeper: bug bounty programs

For nearly 20 years, major corporations have been rewarding those who hack into their computer systems – provided they report any security flaws which they find to the system's owners. Many corporations offer a prize (to include cash, recognition or merchandise) to individuals who visit specified websites and report security vulnerabilities they have found. The programs recognize that hackers can help to create a safer cyberspace and provide a public good by testing systems and reporting their findings, and that often safety is created by having large numbers of tests by diverse groups of people.

The practice first began with the web browser Netscape in 1995. Since then, 451 corporations have established international bug bounty programs. In 2015, United Airlines became the first airline to offer such a program, after a computer programmer found several vulnerabilities in Boeing airliners used by the company. As reported in *Wired Magazine*, a computer scientist named Chris Roberts was able to access many features of the plane's navigation from the inflight entertainment system located in the back of his seat. Using this device alone, he was able to hack into code that would have allowed him to send commands to the plane's engines causing it to roll, and also to deploy the airline's oxygen masks. The United program offers those who report bugs additional airline miles.

In 2016, US Secretary of Defense Ash Carter launched an initiative called "Hack the Pentagon." This was the first 'bug bounty' program in which registered participants could legally hack into the federal government. Hackers ranging from students to professional computer scientists competed to find security flaws in five government websites: defense.gov, dodlive.mil, dvidshub.net, myafn.net and dimoc.mil. Participants received from 100 to 15,000 dollars for their services.

Those wishing to participate in such programs can find a current listing of companies offering a bug bounty at www.bugcrwod.com.

Sources

No Author. 2015. "Hack the Pentagon." *Hacker One*. Available at https://hackerone.com/resources/hack-the-pentagon. Accessed October 16, 2016.

No Author. 2015. "United Will Reward People Who Flag Security Flaws – Sort Of." *Wired Magazine*. May 14. Available at www.wired.com/2015/05/united-will-reward-people-flag-security. Accessed October 3, 2016.

Similarly, students must agree to adhere to the ISC Code of Ethics in order to receive Certified Information Systems Security Professional (CISSP) certification. This code includes two rules that are relevant here: a systems security professional should "protect society, the common good, necessary public trust and confidence, and the infrastructure" and "act honorably, honesty, justly, responsibly and legally" (ISC^2, (2) 2016, 1).

Other ethical codes of conduct for computer professionals which address hacking behaviors include the Association of Computing Machinery's ethical code (found in Appendix A) which also refers to "causing no harm." In addition, the International Information Systems Security Certification Consortium, Inc. (ISC) provides a code of ethics, as does the Information Systems Audit and Control Association (ISACA). Finally, the Information Systems Security Association (ISSA) promotes a code of ethics which is similar to the ISC, ISACA and ACM codes of ethics.

Of course, some sceptics like to point out that Edward Snowden, the individual who exposed the surveillance techniques of the National Security Agency, is also a Certified Ethical Hacker. Any of the techniques taught in the course can be used both in service of one's state and also against one's state or employer. Ultimately, it is up to the individual to use the skills developed in the course appropriately and in an ethical manner.

White hat, black hat and grey hat hackers

In contrast to white hat hackers, **black hat hackers** attempt to breach internet security and gain unauthorized access to a system. They seek to destroy or harm the systems they penetrate, often by releasing viruses or destroying files. A black hat hacker could also engage in **cyber hostage taking** through holding files for ransom, or accessing personal information which the individual considered to be confidential (including educational information like test scores or medical information) and release it or threaten to do so. Thus, black hat hacking could harm a specific individual, a class of individuals (such as hospital patients) or a corporation, agency or nation. Black hat

hackers' activities are frequently illegal, and they may work on their own or in collaboration with a criminal organization.

Box 3.4 Application: ransomware

What is ransomware? It is malware which can be surreptitiously loaded onto a computer. It has the ability to encrypt all of a user's files. Once that is done, a message pops up informing the user that unless they pay a 'ransom' to a specific address by a particular deadline, all of their data will be destroyed. Those who pay the ransom are given a key which can be used to decrypt the data. A new variant, the Chimera Crypto-Ransomware acts slightly differently; this ransomware encrypts your files and then delivers a demand for payment or else your data will be released to the internet. In this way, this particular type of malware creates a threat not to destroy data but to publicly embarrass the recipient of the malware (Gamer, 2016).

Reacting to ransomware

Ransomware presents several legal and ethical dilemmas. For law enforcement agencies, it is often difficult to identify the agent who sent the malware, and it is unclear how the sender might be prosecuted, even if he or she could be identified and caught, since attacks often come from other countries where different laws and procedures apply. Furthermore, paying a ransom or negotiating with a terrorist group is both not advised and illegal under US law and international law.

For those who are attacked, a different ethical dilemma is presented. Should you ever pay a kidnapper a ransom? Currently, many targets have indeed 'paid up.' A British study suggests that 40 percent of the victims of the Cryptolocker malware attack in Britain paid up. And in October 2015, Joseph Bonavolonta, Assistant Special Agent in Charge of the Cyber and Counterintelligence Program in the Federal Bureau of Investigation's Boston office, was publicly criticized when he admitted that even the FBI sometimes simply advises clients to pay the ransom (Zorabedian, 2015).

Ethics of paying a ransom

Ethicists give several reasons why you should never pay a ransom. First, while an individual or corporation benefits by paying a ransom and avoiding consequences against themselves, they may harm others in the future – since paying up may encourage a group to carry out more attacks in the future. And a group might use the proceeds it gathers from *your* ransom to carry out research and development activities to make better weapons in the future. Paying your ransom and saving your data is thus viewed as selfish, since it does nothing to protect others from future attacks and perhaps even makes them more likely (Zorabedian, 2015).

However, McLachlan (2014) argues that people have a 'duty of care' which requires them to consider the needs of their dependents over a more general duty to all of humanity. A parent, for example, should defend his child. And McLachlan argues that a state should act to protect its citizens. Thus, the French government has 'bought back' kidnapped individuals from ISIS, as well as looked the other way when French corporations buy back their people, including individuals kidnapped by Al Qaeda in Niger – though both the United States and United Kingdom refuse to do so.

In cyberspace, one could argue that the hospitals' duty is to its patients. Allowing their medical duty to be destroyed would breach the relationship between the hospital and its patients. In a Chimera attack, a law firm or a psychologist should thus guard client privacy and protect them from the embarrassment of having their private details released to the public.

However, the ethicist Peter Singer (2014) cautions against what he calls the 'rule of rescue'. He argues that we always want to save an identifiable victim but that we are less likely to spend resources on an unidentified victim. He argues that we can imagine the consequences of not performing a particular action – like not paying a ransom – more clearly than we can picture other types of failure to act. He argues that "we ought to use our resources to save the most lives; and, overall, paying ransoms is likely to lead to more lives being lost" (Singer, 2014) Here we can adapt Singer's argument to frame the following response to the 'ethic of care.' If paying a ransom for malware ultimately strengthens terrorists and the Islamic State, then in saving our clients, we endanger many others – the refugees, women and children who are currently being victimized by that group. In this view, paying a ransom is not selfless, generous or caring but is rather a selfish act of privileging one's own members over the good of the group.

In this area, there appears to be no clear ethical consensus and perhaps no good solution.

Sources

Gamer, Noah. 2016. "Ransomware one of the biggest threats in 2016." *Trend Micro Simply Security*. January 8. Available at http://blog.trendmicro.com/ransomware-one-of-the-biggest=-threats-in

ISC^2. 2016. ISC^2 Code of Ethics. Available at www.ISC2.org/ethics

McLachlan, Hugh. 2014. "Paying Ransom for Hostages Is Sometimes the Right Thing to Do – Here's Why." *The Conversation*. October 3, 2014. Available at http://theconversation.com/paying-ransom-for-hostages-is-sometimes-the-right-thing-to-do-heres-why-32460

Singer, Peter. 2014. "The Ransom Dilemma." Project Syndicate. December 9. Available at https://www.project-syndicate.org/commentary/islamic-state-hostages-ransom-by-peter-singer-2014-12

Zorabedian, John. 2015. "Did the FBI Really Say 'pay up' for Ransomware? Here's What to Do … " *Naked Security*. October 28. Available at http://nakedsecurity.sophos.com/2015/10/28/did-the-fbi-really-say-pay

In contrast, white hat hackers receive training and agree to adhere to explicit rules regarding who they will target in conducting penetration tests of a system, the sorts of warnings which they will provide to the target before commencing their attack, and the responsibility which they accept in conducting the attack. In addition, white hat hackers seek and are granted permission before attempting to access a system, place self-imposed limits on the damage they will create in conducting attacks, keep detailed logs of the activities which they engage in while attempting to 'own' a system, and conduct legal tests of a system which are spelled out in an explicit contract before attempts are made.

	White Hat	*Black Hat*
Target	• Ground rules are established with defender regarding targets, what is off-limits	• May choose target as the result of a grudge, or for profit • No mutual decision with defender about what targets are off limits
Warning?	• Attacker and Defender agree on when attack will begin, employees may be warned in advance	• No warning that attack is imminent
Responsibility for Attack	• Attacker is known to defender and takes responsibility for attack	• Attacker is not known to defender, and defender may be unable to trace attack back to attacker (attribution)
Access	• Defender is PROVIDED with an 'invitation' to attempt to gain access	• Access is illegal, representing a trespass or invasion
Damages	• Attacker takes 'trophies' (compromising information) only for purposes of raising defender awareness of vulnerabilities • Treats compromising information carefully and with respect • Attacker takes steps to preserve access to information by defender so that it can be restored	• Trophies may be taken and used for profit or public embarrassment • Information or systems may be permanently destroyed
Intent	• Attacker seeks to 'own' the system, in order to demonstrate to defender that it is possible	• Attacker seeks to own the system in order to exploit it for his own purposes (economic, political, ideological, etc.)
Record of Activity?	• Attacker does not cover tracks by destroying logs – so that defender can learn what transpired and take steps to fix/correct access problems	• Attacker covers tracks, making it difficult for defender to identify exactly what weaknesses and vulnerabilities were exploited
Legal?	• Penetration testing is legal if it is spelled out in a contract between defender and attacker	• May violate United States Criminal Code statutes on fraud, wire and electronic communications interception • May violate Digital Millennium Copyright Act • May violate Cyber Security Enhancement Act of 2002

Figure 3.3 White Hat vs. Black hat hacking activities

Source: Harper et al., 2011. *Grey Hat Hacking: The Ethical Hacker's Handbook* provided the basis for reasoning in this chart, pp. 8–9

Both white hat and black hat attackers thus use similar techniques in attempting to access and own a system, but do so under very different ground rules. Figure 3.3 compares and contrasts the two sets of assumptions under which each group operates.

In identifying a hacker as a white hat or black hat hacker, then, the most important question is whether or not they gained unauthorized access to a system, rather than the type or amount of damage sustained, whether the damage was intentional or unintentional or who specifically they were working for. (However, this situation is complicated during activities like warfare, since one might legitimately claim to be acting ethically even if they are 'cracking' a system – if they are doing so on behalf of

their state against an enemy state in wartime, or if they are acting on behalf of an intelligence agency. We will explore this issue more in Chapter 7 on cyberwarfare.)

The final type of hacker to be considered is the grey hat hacker. The ethical 'code' of the grey hat hacker is spelled out in **Grey Hat Hacking: An Ethical Hacker's Handbook**. Here, the authors argue that

> If an individual uncovers a vulnerability and illegally exploits it and/or tells others how to carry out this activity, he is considered a black hat. If an individual uncovers a vulnerability and exploits it with authorization, she is considered a white hat. If a different person uncovers a vulnerability, does not illegally exploit it or tell others how to do so, and works with a vendor to fix it, this person is considered a gray hat.
>
> (Harper et al., 2011, 18)

In essence, a grey hat hacker is someone who is self-employed, working to collect bug bounties through testing systems without authorization but not seeking to damage the systems but rather to enrich himself through collecting rewards for identifying system vulnerabilities. This behavior can be justified on ethical grounds through arguing that hacking produces a public good, through identifying security vulnerabilities.

Ethics of pen testing

Penetration testing has been described as "the (sanctioned) illegitimate acquisition of legitimate authority" (Pierce, 2006). Pen testing is a set of practices carried out usually by an outside company hired by a corporation to attempt to access their systems. Pen testers utilize both traditional hacking and social engineering techniques to break into the client's system in order to identify and aid in the fixing of any security vulnerabilities which are found. **Social engineering** is defined as "the practice of obtaining computer information by manipulating legitimate users" (Gupta, 2008, 482). It is a form of deception in which testers might impersonate legitimate users and make inquiries about passwords or send e-mails inviting a user to click on a link. It relies less on technology and more on the human element in getting access to a system (Allen, 2006). Because social engineering involves deception, it raises ethical issues.

Despite the ethical issues, penetration testing is effective in increasing system security and is widely used today. A recent survey indicated that 34 percent of companies conduct external penetration tests and 41 percent conduct internal

penetration tests. (Trustwave, 2016) Penetration testing is the most widely outsourced security activity among corporations. Indeed, in April 2016, the Pentagon, headquarters of the United States Department of Defense, launched its own Hackathon, encouraging users to attempt to access the over 200 sites associated with the Department of Defense (Krishnan, 2016). But penetration testing practices contain potential legal and ethical pitfalls. How can corporations and personnel conduct activities that are lawful and ethical?

Ensuring the legality of penetration testing

Currently, analysts recommend that all parties conducting penetration testing create well-documented, written agreements. Many companies specify that those hired to carry out penetration testing have specific certifications (such as Certified Ethical Hacker; Information Assurance Certification Review Board Certified Penetration Tester; or the Council of Registered Ethical Security Testers certification [CREST]). To get certified, testers often undergo specific ethics training and furnish evidence that they have a clean criminal record (Karakasiliotis, Furnell, and Papadaki, 2007). Testers often also sign a nondisclosure agreement (NDA) spelling out their responsibilities to protect company secrets, as well as their agreement to comply with the laws of the country where work is being done. It is still illegal for pen testers to impersonate law enforcement, to threaten to harm someone in order to get information or to unlawfully obtain federal documents in order to access social security numbers. Companies will often ask testers to sign very specific contracts spelling out what sorts of behaviors are authorized. For example, if testers go through dumpsters looking for information that might aid in penetrating a system they should have permission to do so, as well as for incidents like stealing an employee's computer.

Ethics models

However, even if you follow all the rules, ethics issues will still arise. We can apply the three lenses – virtue ethics, utilitarian ethics and deontological ethics – in considering these issues.

Virtue ethics

A virtue ethics approach rests on the assumption that one's actions are a function of one's character. It does not allow for a division of actions into, for example, those which are carried out in public life and those which are carried out in private life. It

also does not focus merely on the outcome of actions but asks the actor to consider what is motivating his action and what that says about his character.

Pen testing presents an ethical issue from a virtue ethics approach for three reasons:

- A pen tester employs deceptive practices ('lies') including misrepresenting himself and his desires in order to achieve his target.
- A pen tester often adopts an instrumental approach towards other human beings which violates the principle of respect for others. To get access to data, he may treat his target group not as individual's worthy of inherent respect and dignity but rather as sources of information which he needs to access.
- A pen tester may display behaviors that don't appear to be morally consistent – for example, allowing deception in carrying out social engineering practices, but not elsewhere in a person's life.

Two virtues which can guide the pen tester who wishes to behave ethically are self-restraint and empathy.

The virtue of self-restraint

In history, there are many examples of individuals who have cultivated discipline or self-restraint as a virtue. Today, we look up to athletes who wake up early, engage in punishing workouts and delay gratification. A hacker who cultivated restraint would accept that an open door to a system does not necessarily mean that he or she has the right to enter. Rather, in situations where entering that system would be destructive or harmful, the hacker might decide to forgo this opportunity and the rewards that might accompany it. Here, Faily et al. argues that a pen tester should "not exploit the network for the sake of exploiting the network." In other words, he should refrain from accessing information he might find in a system (like personal records or e-mail) if he is not required to do so as part of his contract … like reading personal e-mail (2015, 239).

However, Hu et al. (2012) suggest that most hackers, by virtue of their youth, do not possess the necessary skills of delayed gratification or self-restraint. Rather, they point to research that suggests that young people are more likely to become addicted to the internet, more likely to commit piracy and data misuse. Here they rely on scientific research which purports to show that the structures within the brain that help people to reason their way through problems and delay gratification are actually the last set of structures to mature. They argue that since these structures are often not fully mature until the age of 21, then it may be developmentally inappropriate to

expect young people to display qualities like self-restraint and delayed gratification with respect to computer and data use (Yar, 2005).

The virtue of empathy

The next virtue which an ethical hacker might cultivate is one of empathy or respect for others. Here Brey (2007, 23) argues that hackers commit an ethical breach when they commit activities which compromise the ability of individuals to control the confidentiality, integrity and availability of their data. A hacker motivated by respect might thus decide not to release information like photographs or videotapes if doing so would hurt an individual.

So how might a virtuous pen tester behave? A virtue ethics approach thus suggests three cautions: first, the tester should treat everyone with respect in carrying out tests, not harming or embarrassing employees – but instead reporting the results of social engineering tests anonymously. Pierce et al. (2006) suggest reporting only percentages and statistical information (for example, noting that fully half of employees clicked on the link containing malware, rather than naming specific people who did so). An employee might be embarrassed or fired if linked to specific activities.

Second, the tester should include a representative of the Office of Human Resources in initial contract meetings. And he should avoid engaging in scenarios that employees would find upsetting, or actions which cause them embarrassment or jeopardize their employment or their reputation. Goodchild (2013) cautions against impersonating a real employee of the company in sending an e-mail that might get an employee to share a file, information or data. Instead, she recommends creating a fictional employee. She notes that it might be acceptable to lie and say you left your keys on your desk to get readmitted to a building, but you should not make up a story about a car accident that might traumatize some people. Pierce et al. also raise ethical concerns regarding the marketing of penetration testing services. They argue that sowing fear, uncertainty and doubt (FUD) to sell ethical hacking services is unethical, as is the use of crime statistics to promote these services. They suggest that pen testing companies need to walk a fine line between informing potential consumers of genuine risks that their companies may face and needlessly scaring or worrying potential clients (2006, 198).

Finally, pen testers can practice self-restraint and "not exploit the network for the sake of exploiting the network" (Failey, 239). In other words, the pen tester should refrain from accessing information they might find in a system (like personal records or e-mail) if they are not required to do so as part of their contract.

Utilitarian Ethics In contrast to the virtue ethics approach which considers what decisions about how to behave indicate about the hacker's character, a utilitarian ethics approach would consider only the consequences associated with the hacking offense. Who was hurt by the hacking and what sorts of damages occurred? This approach assumes that not all types of hacking are alike. Some are ethical while some are not. It also allows for the possibility of there being a spectrum of ethicality, with actions being somewhat unethical, mostly ethical or completely unethical.

Here, we can identify utilitarian arguments both supporting and condemning hacking. Defenders are that hacking produces social benefits which outweigh the costs and inconvenience that targets might incur (Raicu, 2012). They suggest that hacking increases transparency and accountability within the system of government and corporate actors using computers. However, as Raicu (2012) asks, if the outcome associated with hacking is that the scales of justice will somehow be righted and social wrongs will be rectified, is the hacker necessarily the best individual to be carrying out this righting of the scales – rather than some other type of regulatory actor, such as the government or a nongovernmental organization?

Brey (2007) uses a utilitarian framework to argue against the ethicality of hacking. In particular, he points to the economic consequences of hacking. And US government officials warn about the real dangers that could occur if hacking led to widespread **social disruption**. Hackers motivated by political, economic or ideological reasons could shut off supplies of natural gas to cold regions of the United States in the winter months, or access and shift navigation systems in airplanes and the air traffic control centers at airports. In addition, hackers can affect the operations of public transportation in urban areas and nationwide.

We can also consider the costs which individuals and corporations now pay as a result of the threat posed by hackers. Currently, the US government budget for cybersecurity is 14 billion dollars (whitehouse.gov)! While this budget might sound like good news to those contemplating careers in this field, spending on cybersecurity isn't free. Economists refer to **opportunity costs** to describe the choices that people make, forgoing spending in one area in order to fund something else desired or needed. Higher spending on cybersecurity means less money for social service programs like housing and food programs, education and student loans.

In many instances, legal restrictions on hacking reflect a utilitarian understanding, focusing on the target of hacking and the consequences of hacking. For example, Australian laws distinguish between four types of hacking offenses (Australian Institute of Criminology 2009):

1 Instances where an individual or corporation accessed data or impaired electronic communications with the intent to commit a serious offense (such as fraud or theft);
2 Instances where an individual or corporation accessed data or impaired electronic communications with the intent of causing harm or inconvenience (which might include mischief);
3 "Possession, control, production or supply of data with the intent to commit" an offense (which could include crimes like phishing or passing along a computer virus);
4 Accessing data which we would view as classified or related to critical infrastructure.

Australia's laws consider the intention of the individual or group engaged in hacking as well as the actual economic and physical consequences of the hack. The penalties for different types of hacking are thus different because the intent and consequences of hacking actions are not always the same.

Not surprisingly, utilitarian ethics favors pen testing as well as the attendant social engineering which occurs. The goods achieved through pen testing include the ability to gain awareness of weaknesses and vulnerabilities as well as an increased capability to address these vulnerabilities (Pierce et al., 2006). The only qualm a consequentialist might feel is due to an ethical concern, which Pierce et al raise. They note that some corporations may be too reassured if pen testing fails to find vulnerabilities in their companies. They argue that the failure to find vulnerabilities doesn't necessarily mean that there weren't any, merely that none were found. They thus warn that pen testing might provide false reassurance, ultimately harming a company through making it feel secure although it is vulnerable.

Deontology

Radziwill et al. (2016) note that deontological ethics would most likely not support hacking, regardless of the specifics of the situation. They note that the doctrine of reversibility would require a moral decision maker to ask "How would I feel if my site were hacked?" However, they then go on to state that since white hat hacking, including pointing out the flaws of one's system, *would* be appreciated, then it may be morally justifiable to help others out in the same way.

In considering penetration testing, a deontologist would start with the **categorical imperative**, asking if there was a principle which guides penetration testing which would still be valid were it to become a universal rule. It is difficult to see how

support for either deception or other types of social engineering activities could be upheld as a universal rule. Indeed, if one accepts the contention that lying to an employee for reasons of achieving a password or entry into a computer system is okay, then one would also need to accept that lying to an employee for other reasons at other times would also be morally acceptable – since the categorical imperative rule leaves no place for the application of circumstantial ethics. Applying deontological ethics would also require the pen tester to accept that he himself would be okay with any sorts of activities which he might carry out upon another person for the purposes of gaining entry into a system. In other words, if he found it morally acceptable to impersonate a fellow employee or supervisor in order to manipulate an employee into revealing a password, then he should also be accepting of a colleague or employer perpetrating the same hoax upon him.

A deontologist might also object to the fact that pen testing often requires an instrumental approach towards other human beings which violates the principle of respect for others. In order to get access to data, the tester may treat his target group not as individuals worthy of inherent respect and dignity but rather as sources of information which he needs to access. Indeed, Bok (1978) notes that lying in order to coerce someone to do something (such as giving up information) represents a form of violence against that subject.

However, if one decided to go ahead with pen testing anyway, a deontological ethics approach suggests three cautions: First, the tester should treat everyone with respect in carrying out tests, not harming or embarrassing employees – but instead reporting the results of social engineering tests anonymously. Pierce et al. (2006) suggest reporting only percentages and statistical information (for example, noting that fully half of employees clicked on the link containing malware, rather than naming specific people who did so). An employee might be embarrassed or fired if linked to specific activities.

Chapter summary

- As cybersecurity has evolved as a profession, hacking has moved from a casual, unregulated activity to one with clearly stated norms and standards of professional practice.
- Today we can distinguish between white hat and black hat hackers, with white hats often assisting government and groups in improving their security through running pen tests.
- Many types of hacks are illegal. The distinction between cyberterrorism and hacking is not always clear.
- Both technology developers and users share ethical responsibilities. Thus, it is possible to identify a duty not to hack as well as a duty to safeguard one's material so that one is not hacked.

Discussion questions

1 Some analysts argue that hacking contests are unethical since they might highlight security vulnerabilities or alternately make people feel too safe since they think their systems are impenetrable.

    Do you agree that hacking contests are unethical? Consider the hackathon against the Pentagon. Do you regard the Pentagon's decision to host a hackathon as unethical? Who might be harmed in this scenario?

2 Consider this scenario:

    Someone comes to you and asks you to set up a server for a business like prostitution or drug dealing. How do you describe your obligations as an ethical programmer? Who is your obligation to – your client, society? Are there other ethical issues to consider? What are they?

3 Consider this question:

    Bratus et al. (2010, 122) state that 'hacking' is merely a package of skills which computer experts can develop, arguing that "Hacking is the skill to question trust and control assumptions expressed in software

and hardware, as well as in processes that involve human(s)-in-the-loop (a.k.a. 'social Engineering')."

List the skills a hacker must develop in order to be successful. Think about how such skills could be used in both a society-enhancing and a socially detrimental way. Fill out the chart below. The first row has been filled in as an example:

Skill	*Society-enhancing*	*Socially detrimental*
Encryption	Provide security for banking and payroll transactions	Create ransomware and deploy for profit

Recommended resources

Faily, S., McAlaney, J., and Iacob, C. 2015. "Ethical Dilemmas and Dimensions in Penetration Testing." Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2015). Available at http://eprints.bournemouth.ac.uk/22014/. Accessed June 7, 2016.

Goodchild, Joan. 2013. "Social Engineering in Penetration Tests: Six Tips for Ethical (and Legal) Use." *Computer Security Online*. April 23. Available at www.csonline.com/article/2133330/social-engineering. Accessed June 7, 2016.

No Author. 2016. *Certified Ethical Hacker Candidate Handbook v2.0*. Available at www.eccouncil.org/wp-content/uploads/2016/06/CEH-Handbook-v2.0.pdf. Accessed October 12, 2016.

Raicu, Irina. 2012. "Unavoidable Ethical Questions About Hacking." *Markkula Center for Applied Ethics*. April 1. Available at www.scu.edu/ethics/. Accessed December 2, 2016.

Chapter 3 sources

Allen, Malcolm. 2006. "Social Engineering: A Means to Violate a Computer System." SANS Institute Reading Room. Available at www.sans.org/reading-room/whitepapers/. Accessed December 1, 2015.

Australian Institute of Criminology. 2009. *Hacking Offences*. Sydney, Australia: Australian High Tech Crime Centre. Available at www.aic.gov.au/publications/current%20series/htcb/1-20/htcb005.html. Accessed October 12, 2015.

Bok, Sisella. 1978. *Lying: Moral Choice in Public and Private Life*. New York: Pantheon Books.

Bratus, Sergey, Shubina, Anna, and Locasto, Michael. 2010. "Teaching the Principles of the Hacker Curriculum to Undergraduates." *SIGCSE'10*. March 10–13. Milwaukee, WI.

Brey, Philip. 2007. "Ethical Aspects of Information Security and Privacy." In N.M. Petkovic and W. Jonker, eds. *Security, Privacy and Trust in Modern Data Management*. Heidelberg: Springer Berlin: 21–36.

Brown, James J. 2011. "Exploits, Ethics and the 'Little Old Lady Problem'. " *Clinamen blog*. July 1. Available at http://clinamen.jamesjbrownjr.net/2011/07/01/exploits-ethic-and-the-little-old-lady-problem.htm. Accessed December 4, 2016.

Carlson, Matt, and Berkowitz, Dan. 2014. "'The Emperor Lost His Clothes': Rupert Murdoch, *News of the World* and Journalistic Boundary Work in the UK and USA." *Journalism* 15(4): 389–406.

Faily, Shamal., McAlaney, John., and Iacob, Claudia. 2015. "Ethical Dilemmas and Dimensions in Penetration Testing." *Proceedings of the Ninth International Symposium on Human Aspects of Information Security and Assurance (HAISA 2015)*. Available at http://eprints.bournemouth.ac.uk/22014/. Accessed June 7, 2016.

Floridi, Luciano. 2005. "The Ontological Interpretation of Informational Privacy." *Ethics and Information Technology* 7(4): 185–200.

Fry, Erika. 2013. "The 6 Worst Kinds of Computer Hackers." *Fortune.com*. Available at http://fortune.com/2013/02/the-6-worst-kinds-of-computer-hackers. Accessed December 2, 2016.

Garmon, Jay. 2007. "Geek Trivia: The Cheat Goes on." *Tech Republic*. March 5. Available at www.techrepublic.com/article/geek-trivia-the-cheat-goes-on/. Accessed October 11, 2016.

Goodchild, Joan. 2013. "Social Engineering in Penetration Tests: Six Tips for Ethical (and Legal) Use." Computer Security Online. April 23. Available at www.csonline.com/article/2133330/social-engineering. Accessed June 7, 2016.

Gupta, Jatinder, ed., 2008. *Handbook of Research on Information Security and Assurance*. New York: IGI Global.

Hackerlaw.org. 2017. "US Hacking Laws." Available at Hackerlaw.org/?page_id=55. Accessed March 14, 2017.

Harper, Allen, Harris, Shon, Ness, Jonathan, Eagle, Chris, Lenkey, Gideon, and Williams, Terron. 2011. *Grey Hat Hacking:* The *Ethical Hacker's Handbook*. New York: McGraw-Hill Osborne Media.

Hu, Qing, Zhang, Chenghong, and Xu, Zhengchaun. 2012. "Moral Beliefs, Self-Control and Sports: Effective Antidotes to the Youth Computer Hacking Epidemic." 45th Hawaii International Conference on System Sciences. Available at http://ieeexplore.ieee.org/document/6149196/. Accessed April 11, 2017.

Karakasiliotis, Athanasios, Furnell, Steven, and Papadaki, Maria. 2007. "User Security Awareness of Social Engineering and Phishing," *Advances in Network and Communication Engineering*, 4: 191–198.

Khalilzad, Zalmay M., and White, John P., eds. 1999. *The Changing Role of Information in Warfare: Strategic Appraisal*. Santa Monica, CA: RAND Project Air Force.

Krishnan, Rakesh. 2016. "Hack the Pentagon – United States Government Challenges Hackers to Break the Security." *Hacker News*. March 3. Available at http://thehackernews.com/2016/03/hack-the-pentagon.html. Accessed June 7, 2016.

Levy, Stephen. 1984. *Hackers: Heroes of the Computer Revolution*. New York: Penguin Group.

Mace, Scott. 2016. "For Real: Medical Devices Vulnerable to Hacking." *Medpage Today*. Available at www.medpagetoday.com/practicemanagement/informationtechnology/56566. Accessed September 12, 2016.

Mizrach, Steven. No Date. "Is There a Hacker Ethic for 90s Hackers?" Available at www2.fiu.edu/~mizrachs/hackethic.html. Accessed December 2, 2016.

Nakashima, Ellen. 2016. "FBI Paid Professional Hackers One-Time Fee to Crack San Bernardikno iPhone." *The Washington Post*, April 12.

No Author. 2016. "Certified Ethical Hacker Candidate Handbook v2.0." Available at www.eccouncil.org/wp-content/uploads/2016/06/CEH-Handbook-v2.0.pdf. Accessed October 12, 2016.

Pell, Rich. 2015. "Hacking Self-Driving Cars Easy, Say Firms." *EE Times*. June 10. Available at www.eetimes.com/document.asp?doc_id=1326838. Accessed May 10, 2017.

Pierce, Justin, Jones, Ashley, and Warren, Matthew. 2006. "Penetrating Testing Professional Ethics: A Conceptual Model and Taxonomy." *Australasian Journal of Information Systems* 13(2): 193–200.

Radziwill, Nicole, Jessica Romano, Diane Shorter, and Morgan Benton. 2016. "The Ethics of Hacking: Should It Be Taught?" *OALib Journal*. Available at www.oalib.com/paper1405941

Raicu, Irina. 2012. "Unavoidable Ethical Questions About Hacking." Markkula Center for Applied Ethics. April 1. Available at www.scu.edu/ethics/. Accessed December 2, 2016.

Schneier, Bruce. 2016. "The Security of Our Election Systems." *Schneier on Security Blog*. July 29. Available at www.schneier.com/blog/archives/2016/07/the_security_of_11.html. Accessed December 2, 2016.

Tavani, Herman. 2004. *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. Hoboken, NJ: Wiley Publishing.

Trustwave. 2016. "Security Testing Practices and Priorities: An Osterman Research Survey Report." Available at www2.trustwave.com/rs/815-RFM-693/images/Security%20Testing%20Practices%20and%20Priorities.pdf. Accessed May 2, 2017.

Xu, Zhengchuan, Hu, Qing, and Zhang, Chenghong. 2013. "Why Computer Talents Become Computer Hackers." *Communications of the ACM* 56(4): 64–74. Available at http://cacm.acm.org/magazines/2013/4/162513-why-coputer-talents. Accessed October 21, 2016.

Yar, Majid. 2005. "Computer Hacking: Just Another Case of Juvenile Delinquency?" *The Howard Journal of Crime and Justice* 44(4): 387–399.

Young, Randall, Zhang, Lixuan, and Prybutok, Victor. 2007. "Hacking Into the Minds of Hackers." *Information Systems Management* 24(4): 281–287. DOI:10/1081/10580530701585823

Part II

4 The problem of privacy

Learning objectives

At the end of this chapter, students will be able to:

1. Apply the three frameworks – virtue ethics, utilitarian ethics and deontological ethics – to describing the ethics of privacy
2. Describe privacy as both a universal and relative concept
3. Articulate ongoing legal issues in regard to regulating privacy in the United States
4. Argue on behalf of computer scientists' obligation to safeguard user data
5. Describe the ethical issues associated with anonymity in an online environment

As we consider the ethical problem of privacy in this chapter, we can consider five real-life situations involving the use of hacking by a computer specialist or an amateur:

- In December 2013, the massive US retailer Target Corporation revealed that as many as 70 million individuals who had shopped at Target during the holiday season may have had their credit card data stolen as a result of a hack into their database. In the following months, many individuals had problems with credit card fraud, and Target was required to pay damages to customers who had been harmed as a result of the data breach (Hirsch, 2014).
- In November 2014, the Sony Pictures Corporation was targeted by hackers believed to be operating in North Korea. The government of North Korea was angry that Sony had made a Hollywood movie which they believed demeaned the North Korean government and its leaders. Many private e-mails from Hollywood executives were released to the media and many Hollywood celebrities were embarrassed by the revelations (Haggard and Lindsay, 2015).
- In July 2015, the website for an American firm offering to match up individuals looking to have an extramarital affair, Ashley Madison, was hacked. The hackers, known as Impact Team, exposed names and e-mail addresses of some of the 37 million users of the site. It was later revealed that many individuals had used their work e-mails to browse the site, and the impacts of the revelations were felt at US agencies as diverse as the Department of Defense and the Central Intelligence Agency (Mansfield-Devine, 2015).
- In June 2016, many Twitter accounts believed to belong to supporters of the terrorist group ISIS were hacked by members of the vigilante group Anonymous. In a tribute to Gay Pride, the Anonymous hackers tweeted out photos and images from the suspected ISIS accounts which included rainbows and other symbols associated with gay rights (Colarik and Ball, 2016).
- In the summer and fall of 2016, hackers exposed personal e-mails sent by US Presidential Candidate Hillary Clinton, which contained details about her financial affairs, personal discussions related to the personalities and capabilities of other members of her team, and matters which were seen as relevant to the presidential campaign. Later, the head of the US Central Intelligence Agency stated that he believed

that the Russian government was behind the hacks, and suggested that Russian president Vladimir Putin may have been personally involved in this activity (Persily, 2017).

All of the examples above illustrate possible ways in which individuals, groups, corporations and states can be harmed as a result of privacy breaches in cyberspace. But the examples also raise a number of different ethical issues: What are the responsibilities of the corporations which collect our data, and what are our own personal responsibilities to practice good cyberhygiene and safeguard our own data? Should everyone have an equal right to be provided with privacy in regard to their online behavior, or should those whose actions are unethical, illegal or criminal expect that they would have less privacy? Should the actions which we carry out at work be regarded as automatically subject to our employer's surveillance and supervision? And should celebrities and politicians be granted the same sorts of privacy rights which ordinary people have?

In this chapter we ask: what is privacy and what rights do people have in regard to the privacy of their individual activities, their data and their digital identities? Are there universal rules regarding what it means to safeguard privacy, and how are new technologies changing our orientations towards questions of privacy? Will privacy even exist in the future?

What is privacy?

'Privacy' is a complex phenomenon encompassing issues including the integrity of our personal bodies, our reputations and our data. Issues related to privacy are of interest to academics and policymakers in many fields – including psychology, legal studies and political science. In addition, engineers and computer scientists today are interested in privacy issues, since they must often make decisions about the ways in which products can be created and configured in order to safeguard privacy or permit the sharing of personal information, images or data.

Privacy is often described as a cluster of rights – including how we are able to represent ourselves to others, the control we have over how we are perceived, monitored or represented by others, as well as the access which others have to our personal information about ourselves, and the degree to which we are able to control other's access to our persons and data. In a landmark essay entitled "The Right to Privacy," written by Samuel Warren and Louis Brandeis in 1890, they defined privacy as "a right to decide how you present yourself and how you are perceived" (Warren and Brandeis, 1890, no pagination). In other words, privacy is what allows an individual to keep information or data secret or confidential and to decide with whom to share secrets and under what conditions. A **secret** is something which is not known or intended to be shared with others.

The term 'privacy' thus includes rights to your own body, rights to your property and rights to your information or data which is generated by or about you. Floridi (2011) suggests that we distinguish between physical privacy (the right not to be observed or to be 'left alone'), decision privacy (the right to make decisions about your own life without interference by others), mental privacy (the ability to have our own thoughts) and information privacy (the right to control what others know about you and what information is collected and shared about you) (Tavani, 2008).

In 1965, the landmark US Supreme Court case **Clark vs. Griswold** extended thinking about privacy to questions of bodily autonomy in ruling that information about people's marriages and sexual relations was also protected as a privacy right (Stanford Encyclopedia of Philosophy, 2013, 4).

Privacy means that you as an individual have a claim to own your body and your image, as well as any information which you generate about yourself or any information which is generated about you. You are the person who ultimately controls that information – who gets to see it, and who doesn't, and under what circumstances (Al Saggaf and Islam, 2015). As the creator of that information and data, you get to decide who gets to be an intimate friend who knows everything about you, who gets to know some information about

you, and who should not be permitted to see you and your information (Marmor, 2015, 1). P**rivacy** also includes the idea of protection; privacy protects us from "unwanted access by others – either physical access, personal information or attention" (Wilkins and Christians, 2008, 10–11). Thus, privacy is related to **surveillance**. The right to privacy means that we have a right not to be surveilled – or watched or monitored – without our consent or knowledge; to be informed when we are under surveillance and to be able to establish private places in our own lives where we will not be under surveillance either by other individuals or by a group or agency, such as the government. Marmor (2015) describes privacy as a "cluster" of rights, many of which derive from the primary idea of privacy itself.

Many professions have developed explicit ethical codes which spell out how information (or secrets) which are shared with them should be treated, and the conditions under which such information should be shared or kept private. Historically, we can point to the institution of the parish priest in the Catholic Church, who keeps the confessions which citizens bring to him secret through the seal of the confessional. Catholic or Canon Law sets out the conditions under which a priest is bound to keep secrets revealed to him in confession. He is forbidden to reveal information to save his own life, to protect his reputation, to refute a false accusation or even to report a crime. He also cannot be compelled to testify in court nor can he be legally compelled to disclose this information (Saunders, No date). The American Bar Association Model Rule 1.5 states that lawyers cannot reveal information that their clients have shared with them without clients giving their informed consent. This rule helps to ensure that clients can trust those they have hired to represent them. Attorneys may only violate that privilege in rare circumstances (Michmerhuizen, 2007).

A violation of privacy occurs if "someone manipulates, without adequate justification, the environment in ways that significantly diminish your ability to control what aspects of yourself you reveal to others" (Marmor, 2015, 14). This may include, for example, a situation where the government tells citizens to assume they are being monitored all the time, or a situation where a corporation changes people's privacy settings on social media without their authorization and consent.

Public space and private space

Philosophers often distinguish between public and private space, and public and private information. We can trace this idea back to Aristotle who distinguished between the public sphere of governance (the *polis*) and the private sphere of the household (the *oios*). He argued that people developed themselves through having a private space for contemplation (Moore and Unsworth, 2005, 16–17). Confucius also distinguished between the public activity of government and the private affairs of family life (Moore, 2013).

Nagel (1998) describes "concealment" as a necessary condition for civilization, arguing that society would be unruly and anarchic if everyone shared all of their thoughts and opinions all of the time. Instead, he says, over time we learn which thoughts not to voice in order to get along with others in a community. As humans, we provide privacy to others and safeguard our own privacy through engaging in restraint. We don't ask intrusive personal questions, seek to peek into private spaces or trespass upon them (Nissenbaum, 2005, 71).

Legally, this distinction still exists, and is upheld in legislation which safeguards private information and the rights of people to keep information private. **Private information** is defined as "information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place and information which has been provided for specific purposes by an individual and the individual can reasonably expect will not be made public (such as a medical record)" (United States Department of Health and Human Services, 2013, 9). **Public information** includes "any activity – textual, visual, and auditory – (that) is legally available to any internet user without specific permission or authorization from the individual being observed, or from the entity controlling access to the information" (United States Department of Health and Human Services, 2013, 9). In many areas of our lives – such as with regard to our medical information or our educational records – specific legislation has been established to

spell out the rights and responsibilities of users and providers (See insets on HIPAA and FERPA). American constitutional law describes an **expectation of privacy** meaning that individuals may expect to have their activities treated as private, particularly when they are in a private space like a home or when they are engaged in private, rather than public communications. That is, privacy allows individuals to restrict others from accessing and controlling information about us.

Why does privacy matter?

There are four major reasons why privacy is such a crucial value and goal for individuals and societies. First, privacy allows us to develop ourselves as unique individuals free from public scrutiny or judgment. Next, privacy allows us to develop relationships with other people through creating levels of trust and intimacy. Third, privacy helps to create equity through creating conditions where everyone is able to decide how much of himself or herself to reveal and under what conditions. Finally, privacy helps to establish places where people feel safe and protected, in order to carry out functions which are important in society.

Privacy and moral growth

In his work, Sandel describes "the liberal conception of the self," arguing that each of us have the right to be an unencumbered self, making our own choices about our identity "in splendid isolation," unaffected by fears of how our choices might be viewed or judged by others (Van den Hoven, 2008, 31). Sandel (1998) argues that people have to be able to exist freely in the world, to associate with whom they wish, to dress the way they want and to go where they want, as well as to be able to say things and try on ideas without fear that they will be watched, tracked, ridiculed, humiliated or even punished for doing so – in order to become the people they wish to be (Alterman, 2003).

In this view, privacy means that we are all allowed to decide what face we want to present to the world, without being identified or labelled in advance. It also means that we have a right to a private life – we cannot be compelled to reveal information about issues we might choose to keep private, such as our sexual identity or lifestyle. We can decide what we choose to tell about ourselves and what we keep secret.

It also means that we can have a private space where we are free from public scrutiny, and the ability to carry out activities without being tracked or watched in order to achieve other rights which we hold as important in American society – including the right to assemble freely and the right to engage in free speech. Thus, privacy is related to the notion of **anonymity**, an issue which we will return to in Chapter 5 on surveillance.

Privacy and the right to a private life are also related to the idea of **autonomy**, or freedom from external control and influence. Recent legislation in France, for example, enshrines the principle that an individual cannot be compelled to respond to work-related e-mails and queries during the hours reserved for his leisure. In describing the reason for the legislation, Myriam El Khomri, France's Minister of Labor described the importance of preserving a border between one's work life and one's home life, and between one's working hours and one's hours of leisure (Rubin, 2017). The 2017 legislation aims to preserve people's private lives by clearly distinguishing between paid employment and leisure time and space. One cannot enjoy complete autonomy or control over one's life during working hours, but one should have this autonomy when one is at home living one's private life.

Box 4.1 Critical issues: the Family Education Rights and Privacy Act

If you are a college student, you may have heard professors and administrators at your university use the term FERPA. But what is FERPA and what does it have to do with you?

The Family Education Rights and Privacy Act is a US federal law which regulates the privacy of student educational records. FERPA legislation applies to all university and colleges which receive funds from the US Department of Education whether they are public or private, profit or nonprofit. FERPA legislation establishes several key understandings in regards to educational records. FERPA:

- Acknowledges that all students 18 and over are legal adults.
- States that parents of minor children, as well as adult students, have the right to see their own educational records and to have inaccuracies corrected. If there is a dispute about the accuracy of these records they are entitled to a hearing.
- States that information cannot be released without student permission to outside parties. Thus, the law safeguards the confidentiality of student information – including medical information and information shared with a school-based counselor.

Cybersecurity professionals working in colleges and universities will likely be involved in conversations about FERPA since FERPA mandates that educational institutions safeguard student records. Universities and colleges are responsible for implementing privacy and security best practices including having a data breach response plan. However, FERPA does not include specific data breach notification requirements. Cybersecurity professionals thus may be involved in making sure that universities comply with these requirements, and may also be involved in drawing up data breach response plans.

FERPA also presents ethical concerns related to privacy and transparency. First, students and families may be unaware of how much data is being collected about the student, what data is being collected, who has access to it and where it is being kept or housed or for how long. Bathon (2013) argues that student data is kept by individual states at the state level – where there may not be clear policies regarding what to collect, how to store it and where to store it. Policies may not be enforced, and administration may lack strong knowledge of data security practices.

Finally, FERPA presents legal issues, since there is currently a debate about what specifically constitutes an educational record for purposes of respecting confidentiality and integrity: for example, do a series of texts between a teacher and a student constitute an educational record? What about e-mails sent from home accounts, chats which might take place through Facebook or postings on social media?

These are issues which cybersecurity professionals need to pay attention to as they advance in their careers.

Source

Bathon, Justin. 2013. "How Little Data Breaches Cause Big Problems for Schools." *Technological Horizons in Education (THE)*. November 5. Available at www.questia.com/library/journal/1G1-352751609/how-little-data-breaches-cause-big-problems. Accessed January 2, 2016.

The challenge: preserving privacy while providing security

Today, however, citizens and governments face a great ethical challenge in deciding whether and under what conditions to compromise or limit people's right to individual privacy in order to provide security for a community like a workplace, a city or a country. Here we recognize that no one has a perfect right to always be anonymous. Instead, individuals may be asked to provide information which allows security personnel to engage in **authentication**, defined as "a process that leads us to have a high degree of certainty or probability about the identification of an individual" (Chinchilla, 2012, 2). Today security personnel often use biometrics – defined as "authentication techniques relying on measurable physiological and individual human characteristics that can be verified using computers" – to identify individuals before allowing them access to

facilities like a work place, a government building or an airplane boarding lounge. Biometric markers are unique to an individual, and computer programs can match up an individual's identity with their identifying biological information through examining features like their fingerprints, their retinas, their facial geometry or behavioral characteristics like one's gait or voice. As Cavoukian et al. (2012, 3) point out, biometric data are "unique, permanent, and therefore, irrevocable."

Biometric identification technologies allow security personnel to identify who is present at a demonstration or event. Law enforcement officers can track individuals on closed circuit television surveillance cameras, following them as they go about their daily activities. RFID technologies and GPS tracking technologies in cell phones and other devices create information trails about us as we exist in society. At the same time, security personnel use analytic algorithms to predict people's future behavior based on educated guesses or heuristics related to ethnicity, age, socioeconomic status, gender and other variables. McFarland (No date, 1) describes how data aggregation technologies may pose a threat to citizen privacy. He writes:

> From a person's search queries, one could infer, rightly or wrongly, medical and psychological issues… . Sexual activities and preferences, relationships, fantasies, economic circumstances… . Taken together they can suggest a fairly comprehensive portrait of a person, including that person' most intimate problems and vulnerabilities

Cavoukian et al. (2012, 3) caution against the aggregation of databases containing biometric data in particular, arguing that such personal data should not be shared or aggregated without the individual's permission and knowledge.

Profiling techniques can be used for a variety of reasons, including identifying government or private sector employees who might constitute a security risk or even a criminal threat. The American Civil Liberties Union describes criminal **profiling** as "the reliance on a group of characteristics (which are) believed to be associated with crime" by law enforcement officers, who determine who to stop for traffic violations or whom to search based on characteristics such as race (www.aclu.org/other/racial-profiling-definition). These practices contradict Sandel's ideal of a person who conducts his life without being prejudged or labelled by others, and is responsible for creating his own identity through his own actions. Here McFarland (No date) writes that such technologies also dehumanize those who are being evaluated in this way, treating them as collections of attributes, rather than as unique individuals. We will return to this issue in greater depth in Chapter 5, on surveillance.

Privacy and relationships

In addition to letting us behave as free, autonomous individuals, privacy lets us establish relationships, participate in our communities and to carry out activities which we do not necessarily want to share with others. Nissenbaum argues that privacy allows us to build healthy relationships, stating that:

> Properly functioning, psychically healthy individuals need privacy… . Privacy assures (these) people a space in which they are free of public scrutiny, judgment and accountability in which they may unselfconsciously develop intimate relationships with others.
>
> (1997, 209)

In this way of thinking, privacy is important because it protects you against undesirable consequences coming from a breach of privacy – like being embarrassed or having things stolen from you (Tavani, 2008).

Box 4.2 Going deeper: the right to be forgotten

Have you ever Googled yourself and been surprised by the information you found online? Did you find a social media post, an embarrassing photo or evidence of a youthful transgression? Who owns the information found online about you and do you have any control over what that information looks like?

In 2014, the Court of Justice of the European Union (CJEU) heard a landmark case. A Spanish citizen requested that the Spanish Data Protection Authority remove information relating to his previous failed business ventures, since it was harming his present economic prospects. His request was denied, but Google was ordered to "delink" the requested information, so that it would no longer appear in a Google search. This case also established the precedent that European users could petition Google to delink information which they did not wish to appear in searches of their name.

But this case presents both ethical and legal issues. Luciano Floridi, a Professor of Philosophy at Oxford, outlines the basic problem: two fundamental rights are in conflict – the right to privacy and the right to free speech. Floridi asks whether an individual's information belongs to the user, the publisher, a search engine, or the greater online community. Some might consider it an invasion of their privacy for information pertaining to them to not be deleted at their request. Others might consider it censorship (Floridi, 2014a).

Legally, the case also presents problems of territoriality and jurisdiction since the internet is a network that transcends borders. If the CJEU were to hypothetically rule in the favor of the Spanish citizen, what are the limits of their power? If Google were to delink the information only in the Spanish version of their engine, it would still be available everywhere else in the world. But the CJEU does not have the sovereign ability to enforce its rulings outside of the European Union. Therefore, even if someone wishes to exercise the right to be forgotten, they can only operate within the narrow boundaries of their own national law. Anything more risks an encroachment on ideas of sovereignty (Floridi, 2014b).

If there is a right to be forgotten, it is an issue that is far from being appropriately defined and remains very much an open topic. The CJEU ruled in favor of the Spanish citizen, ordering Google to delink the requested information from across the entire EU's internet … but it still exists on the domain of the publisher and can be accessed elsewhere. The availability of the information has not been changed in the slightest, merely the accessibility (Floridi, 2015).

Sources

Floridi, Luciano. 2014a. "Right to Be Forgotten: Who May Exercise Power, Over Which Kind of Information?" *The Guardian*. October 21. Available at www.theguardian.com/technology/2014/oct/21/right-to-be-forgotten-who-may-exercise-power-information. Accessed January 2, 2016.

Floridi, Luciano. 2014b. "Right to Be Forgotten Poses More Questions Than Answers." *The Guardian*. November 11. Available at www.theguardian.com/technology/2014/nov/11/right-to-be-forgotten-more-questions-than-answers-google. Accessed December 2, 2016.

Floridi, Luciano. 2015. "The Right to Be Forgotten: A Philosophical View." *Annual Review of Law and Ethics* 1(18), 30-45. Available at http://s3.amazonaws.com/academia.edu.documents/39017085/00-Floridi.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1500566047&Signature=G9IveyRudfFqlrMvAyjrw9a4dt8%3D&response-content-disposition=inline%3B%20filename%3DThe_Right_to_Be_Forgotten_a_Philosophic.pdf.

Privacy and justice

Van den Hoven (2008, 31) argues that privacy is an important prerequisite in order for people to experience equity and justice in society. He believes that privacy needs to be a 'good' which everyone has equal access to, and that everyone should have an equal ability to decide what to keep secret and what to reveal, regardless of factors like socioeconomic class. Floridi describes privacy in terms of ownership. If we own our information

about ourselves, then we can decide whether and under what circumstances to give that information away. In an ethical world, then, everyone would have an equal ability to own their personal information (Tavani, 2008).

However, surveillance or spying often violates this principle of equality in which everyone has a right to keep their secrets private. Some people are more likely to be monitored, even if doing so robs them of their dignity and independence. Most people agree that young children should get less privacy since they need to be watched and monitored closely because they lack adult judgment. Those who are elderly or infirm may also have less privacy as they are taken care of in facilities, often by paid caretakers. In these instances, those in authority have made a judgment call that if there are trade-offs to be made between privacy and the provision of security, security should be paramount.

New technological developments also have ramifications for privacy in relation to equity. Today, we may engage in a decision-making process, deciding to trade away some of our privacy (for example, information about purchasing decisions) in return for a discount on groceries or some other product. Others may decide to spend more money to, for example, hire an online reputation management company, in order to more carefully manage what information strangers can find out about them through online searching (Van den Hoven, 2008, 31). This has been referred to as a '**privacy calculus**.' In thinking about these developments, we need to be vigilant against the development of a system of **tiered privacy** in which some individuals are monitored or surveilled more closely than others.

Privacy and trust

Finally, Moor describes how privacy provides people with security. He describes a situation in which you might be stalked by someone who wants to know everything about you and watches you all the time. He notes that your watcher never harms you in any way, but then asks whether you still feel violated. In his scenario, you have complete autonomy to behave as you wish, but you have no privacy. Moor writes, "The subject's security is being violated… . Even if no other harm befalls the person. People have a basic right to be protected, which from the point of view of our computerized culture, includes privacy protection" (1997, 29).

Privacy also helps to create trust. Individuals are more likely to invest with banks or to engage in relationships with institutions where they are assured that their information will be kept confidential, that it will not be compromised through a data breach, and that others will not have access, including the ability to copy and disseminate that information. In this way, Brey (2007) notes that privacy is also related to property rights, describing actions like copyright theft and information piracy as violations of user privacy.

Thus, as we have seen, privacy is a foundational value because so many other rights and values are in some way dependent upon the provision of privacy. Figure 4.1 depicts the cluster of related activities and values which are associated with privacy.

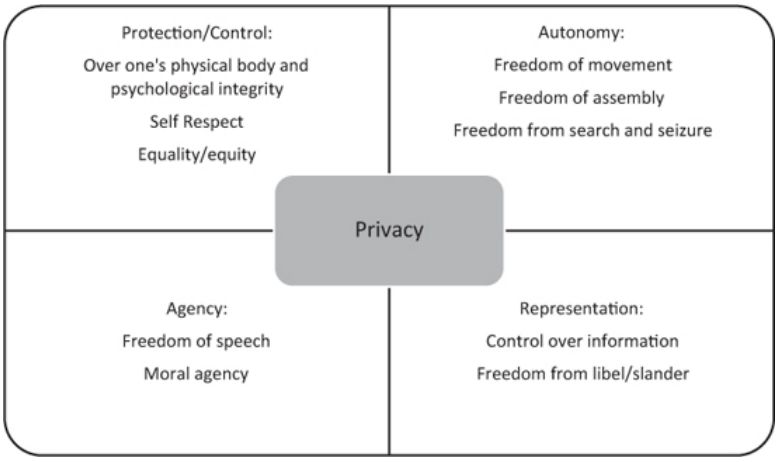

Figure 4.1 Values associated with privacy

Today, it is particularly difficult for governments and corporations to create and enforce regimes or sets of rules regarding what personal data about people will be captured and stored, and who may access it and under what circumstances given the prevalence of technologies like ubiquitous computing. **Ubiquitous computing** refers to the practice of embedding technology in everyday items such that they may collect information and transmit it to other objects, often without the user being aware of it. The Internet of Things relies on a ubiquitous computing to establish an environment in which the objects in your home can 'talk' to each other, with your thermostat, for example, talking to your smart phone.

In addition, it is sometimes hard to distinguish between public and private data, and public and private spaces. Finally, it is challenging for people to develop their moral selves 'in splendid isolation,' when we are often not anonymous, but rather identifiable through biometric identification regimes, as we walk down the street, appear in photographs or browse online. Marmor (2015, 3) notes that in order to secure people's privacy, it is necessary to create a "reasonably secure and predictable environment" in which individuals and groups understand how information is organized, how it flows and the consequences which might result from the release of information. Thus, individuals involved in information technology and in cybersecurity play a particularly important role in safeguarding privacy, through helping to build, establish, regulate and secure environments in which information flows.

Box 4.3 Application: privacy by design

What is privacy by design? A Canadian official, Ana Cavoukian (2011), defines it as "A proactive integration of technical privacy principles in a system's design – such as privacy default settings or end-to-end security of personal data – and the recognition of privacy in a company's risk management processes." In brief, privacy by design (PbD) means not waiting until after a system or technology is built and then thinking about how to protect data and provide privacy. Instead, as designers and engineers think about the goals which the new equipment should achieve, they should consider both technical goals (like processing speed and storage capacity) and nontechnical goals (such as creating trust, allowing users' agency to manage privacy, and providing transparency about how and under what conditions data should be shared).

As Spiekermann (2013) points out, PbD represents a revolutionary approach to regulating privacy because the responsibility rests not with legislators who develop laws or those who enforce regulations but rather with the creators of new technology products themselves. European Union officials are particularly keen to make PbD an important part of their strategy for enhancing consumer privacy in future technologies. Toward that end they have created a Privacy Impact Assessment framework which companies can use in defining, measuring and incorporating privacy goals in the design of new technologies. Just as companies assess other types of risks in designing new products, they can then assess the ways in which citizen privacy could be impacted by a new product, as well as laying out strategies for mitigating privacy risks which might arise.

However, as Yu and Cysneiros (2003) note, those who engineer new products often must negotiate a compromise between multiple competing sets of requirements. Users want privacy but often don't want to pay more for a product providing more privacy, nor will they settle, for example, for a more secure product that works more slowly or offers fewer options for how a product might be used.

Though challenges exist, privacy by design offers a possible way forward in thinking about the future of privacy as new products are created.

Sources

Cavoukian, Ana. 2011. "Privacy by Design Curriculum 2.0." Available at http://privacybydesign.ca/publications/. Accessed January 2, 2016.

Spiekermann, Sarah. 2013. "Challenges of Privacy by Design." *Communications of the Association of Computing Machinery* 56(7): 1–3.

Yu, Eric, and Cysneiros, Luiz Marcio. 2003. "Designing for Privacy in a Multi-Agent World." In *Trust, Reputation, and Security: Theories and Practice*, eds. Rino. Falcone, Suzanne Barber, Larry Korba, and Munindar Singh. Berlin, Germany: Springer, 209–223.

Privacy: can it evolve and change?

Some analysts describe privacy as a universal value, which all cultures recognize (Bok, 1989). However, others argue that privacy is a **social construct** which varies widely across time and across cultures (Boyd and Marwick, 2011; Tuffley and Antonio, 2016). These analysts describe it as a relatively modern phenomenon which emerged only the 1800s. Prior to that people lived communally without a great deal of privacy. In this view, an individual's need for privacy is not innate, but is rather the product of **social practices** which we engage in: As young children we learn that certain activities and information are private, and have expectations about what how our thoughts, selves and behaviors will be made public and under what circumstances. In this view, individual and group ideas about privacy might change over time, in response to social changes, or even in response to technological changes like the widespread availability of social media today. Danah Boyd (2011) has looked at the ways in which teenagers today think about privacy as the result of social media exposure, arguing that young people may no longer recognize the previously accepted clear distinction between the homes as a private space demarcated off from more public spaces.

We use the term **normative expectations of privacy** to refer to ideas about what is socially appropriate in terms of privacy, though normative expectations of privacy often line up with legal understandings as well. Because norms – or unwritten social expectations or rules – are often specific to a culture, norms regarding privacy may also differ from one society to another (Belloti, 1997; Etzioni, 2015). For example, in many Middle Eastern cultures, women may wear a hijab in order to control who may view their bodies. In other cultures, norms regarding the viewing of the female body may differ, and clothing choices will reflect this difference.

Operational definitions of privacy refer to the specific capabilities which may exist within a technology for providing the safeguarding of data. An operational definition of privacy might thus specify what sorts of privacy settings are available in a program, and who has the ability to administer these settings.

Currently, analysts disagree about the ethical responsibilities of data providers to guarantee data privacy, given technological limitations. Should a data provider be required to guarantee citizens that their data will completely safe, and is this even possible? Kligiene (2012) notes that currently there is no universal solution for guaranteeing data privacy to citizens in all forms of social media. Aicardi et al. (2016) suggest furthermore that just because at present there is not a technique for tracing all of the content which you create online back to you directly, this does not mean that there will not be a technique for doing so in the future. They suggest that the most a data provider can say is that "At present, your data is safe from intrusion and your anonymity is secure – but that does not mean that it will continue to be into the future."

Is there such a thing as too much privacy?

While thus far we have made the case that privacy is healthy, socially desirable and necessary, not everyone agrees with this view. Plato, whom we met in Chapter 1, saw privacy as an unnecessary counterproductive value in an ideal state. In *The Laws*, he wrote, "Friends have all things in common" (1967, Vol. 1, 5). Famously, the US president Woodrow Wilson argued that people who request privacy or secrecy are often hiding something, drawing upon the thoughts of the English philosopher Jeremy Bentham. Wilson equated secrecy

with impropriety, particularly in the case of governments seeking to keep secrets from citizens. He thus prized transparency or openness against secrecy as a value, running a 1912 presidential campaign where he spoke about openness, sunshine and fresh air, equating secrecy with corruption (Bok, 1989).

Today, legal rulings have established the understanding that privacy is a right which individuals have. However, corporations and government agencies cannot use privacy rights to disregard or ignore their obligation to share information with constituents about programs and policies. Here, the cooperative value or norm is one of **transparency** – or the obligation to share information with citizens. Citizens require that their governments and their elected officials practice transparency, and public figures therefore also have less expectation of privacy. In the United States, citizens can file Freedom of Information Act (FOIA) requests to get permission to see government documents (Ballotpedia, n.d.). Prospective voters may also feel entitled to see information about a candidate's health or finances as well. Today, local, state, and federal governments often participate in **Open Data Initiatives**, moving their public records online and making them searchable, so that citizens may see the salaries of their public officials, and how their tax dollars are being spent through examining budget documents.

While governments and public officials can expect less privacy, even individuals acknowledge that the right to privacy is not absolute. We might still be compelled to furnish information about our finances for functions like paying taxes, writing a will or negotiating a divorce. We also do not have an absolute right at all times to communicate anonymously, to engage in activities which are untraceable, or to maintain sites or carry out activities on the so-called Dark Web. While we might agree that in general 'your home is your castle,' where you can do what you like, this does not include the right to abuse family members, to use illegal narcotics, or to assemble weapons that might threaten the nation. And while we may wish to grant privacy to others, we may also find that we are required to violate their privacy if, for example, we find that they are planning to carry out violence against other people. Most individuals would not find calling the Department of Homeland Security to report suspected terrorism, or calling Child Protective Services to report suspected child abuse to be a violation of one's right to privacy. Thus, ethics related to privacy are often described as being dependent upon a particular situation (Tavani, 2008).

Indeed, some feminists critique the idea that "people have the right to do as they wish within the private space of their home." MacKinnon (1987) notes that providing people privacy in their homes may not be advisable in a situation such as child abuse or domestic violence. Similarly, we can ask whether the right to act anonymously is absolute today or whether it is appropriate to ask internet users to identify themselves in situations where there is a threat of cyber harassment or cyberbullying. Thus, one of the major issues regarding the ethics of privacy is how to reconcile the competing needs for privacy and the need for security.

The fields of **digital forensics** and **encryption** both rest on this assumption that privacy is not absolute and that we do not have an absolute right to keep secrets – since not all secrets are good secrets. Individuals with expertise in digital forensics assist law enforcement with retrieving data from captured digital devices. They might attempt to access data on a captured computer regarding drug transactions, look for evidence that an individual was engaged in the pornography trade, or look for evidence of illegal financial transactions such as embezzlement or money laundering. Digital forensics experts might testify in court regarding their findings and several companies and schools now offer certification in this growing field.

Other computer experts may work in the field of **encryption**, devising strong methods of encryption and decrypting data, assuring the safety of individual's and corporation's legitimate financial transactions, thus enabling the US and international economies to function routinely and without interruptions.

As Figure 4.2 indicates, today individuals and society must balance two competing sets of needs – the need to safeguard individuals' reputation and provide them with privacy, and the need to collect information and make information available, in order to enable society to function safely and efficiently.

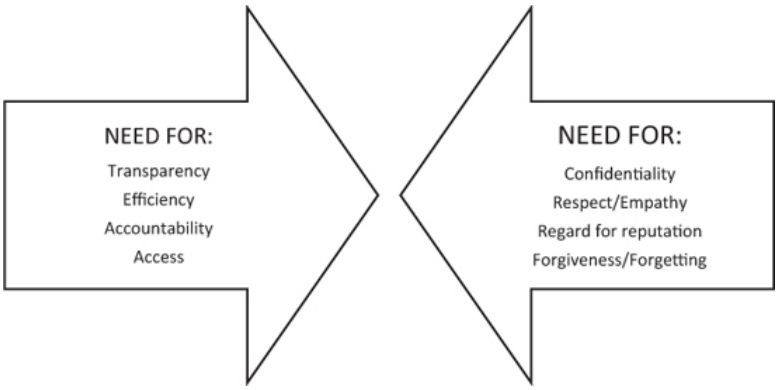

Figure 4.2 Competing social needs – privacy versus security

Protecting citizen privacy today

Today, we can identify several regulations which safeguard individual privacy, including privacy in relation to data provision. Regulations may be created by local, state and national bodies, as well as occupational bodies like the American Institute of Certified Public Accountants. In addition, the term '**fair information practices**' refers to principles adopted globally to ensure that individual's privacy rights are protected and that corporations take sufficient care to make sure that they do so (Culnan and Williams, 2009).

In US law, violating someone's privacy constitutes a type of harm and is thus the subject of tort law, a branch of civil law which deals with the actions of providing damages for a wrong. In the 1965 Supreme Court case **Griswold vs. Connecticut**, Justice Douglas stated that the legal right to privacy is implied in four amendments to the US Constitution: the First Amendment (providing freedom of speech and of the press), the Third Amendment (rights establishing the sanctity of one's home), the Fourth Amendment (rights against unlawful search and seizure) and the Fifth Amendment (right against having to incriminate oneself).

Today, many types of information are regarded as sensitive or private, and there exists specific legislation which lays out what information may be collected and stored, and who may have access to that information and under what conditions.

One area where privacy rights have become controversial in recent years is in hiring situations. In the United States, labor relations laws are very strict regarding what sorts of questions are off-limits in a job interview. Employers cannot ask about prior arrests, plans to get married or get pregnant or religious observance (Giang, 2013). However, using social media, employers can now investigate an applicant's private life quite thoroughly – finding out their age, race, gender and political views, viewing photographs and investigating their qualifications (careerbuilder.com, 2014). Legal cases have supported the finding that a prospective employee has a lower expectation of privacy from an employer than an actual employee, who has a relationship with the employer, would (Sloan et al., 2012, 6). In addition, employers have a fair amount of discretion regarding how they can monitor employee's social media use in the workplace once they are hired. For this reason, experts advise job candidates to sanitize their online profiles, and suggest that even once hired, employees should be careful about posting provocative photos, making off-color remarks or sharing information about their employers.

In the United States, the **Electronic Communications Privacy Act**, passed in 1986, spells out the circumstances under which an employer, government agency or an individual could engage in surveillance, wiretapping or eavesdropping – or the situations in which you could be surveilled without your knowledge or consent. The term Electronic Communications Privacy Act (ECPA) now serves as a type of shorthand for a variety of legislative initiatives which have been passed – of those addressing the issue of privacy in some way. Thus, the ECPA also includes the US Patriot Act, the Department of Homeland Security Act, the Foreign

Intelligence Surveillance Act of 1978 and subsequent amendments in 2008. The ECPA in particular outlaws wiretapping or gathering people's communications without court approval. Information gathered using these means (without consent) cannot be used in criminal proceedings; sharing this information is also illegal (Doyle, 2012, 8).

However, the ECPA states that there is a certain subset of situations, clearly defined, under which it is legal and appropriate for an individual to lose this absolute right to privacy. Thus, the law states that ECPA states that under certain circumstances, including for law enforcement, an individual, corporation or law enforcement agency can collect wire, oral and electronic communications. Eavesdropping is also legal if one party consents to the procedure (for example, if you were being blackmailed by another person and wished to have law enforcement help you out) and in some instances if it is being conducted by a spouse (who might, for example, suspect infidelity and is collecting evidence in case of a divorce). Thus an employer could listen in on your phone conversation if you were being investigated because they suspected that you were breaking the law but not simply because they were curious.

Figure 4.3 describes the types of information which are currently legislatively protected and the legislation or legal rulings which protect them.

Preserving privacy in a technological era

In one of the first textbooks on computer ethics, Johnson (1985) wrote that computers create new versions of the moral and ethical problems with which we are already familiar. She suggests that the challenge is to apply our existing moral thinking to this new "uncharted realm" (Kernaghan, 2014).

As we saw earlier in this chapter, each of us has a physical identity – a collection of **attributes** (such as citizenship and occupational grouping) and qualities which are linked to us – to which we can claim ownership and protection. However, today, we can also speak of a **digital identity** which belongs to each of us. A digital identity can be linked to our physical identity through a process called **authentication** where we might, for example, show documents to prove that we are who we say we are, and that our online activities belong to us. In this way, our real world and our virtual activities are linked (such as when we make a purchase in the online environment using our actual money) and we are often not anonymous online but rather functioning as our real selves, just as we would in the real world.

So do we have a right to the same sorts of privacy protections in our online activities that we have in our real-world activities, and do our digital selves have the same claim to protection that our physical selves do? Do we have a right to carry out the activities described in Chapter 4: to decide which digital face we will present to the world, to create private spaces online and to limit who has access to these spaces, to experience equality in terms of how much privacy we experience online, and to experience security in situations where we reveal something of ourselves online?

Type of Information	*Legislation*	*Summary*
Educational Information	Federal Education Rights and Privacy Act (FERPA, 1974)	• Gives families of children under 18 right to view and contest their children's educational records • Gives students over 18 right to control who views their educational records
Health Information	Health Insurance Portability and Accountability Act (HIPAA, 1996)	• Provides federal minimum standards for safeguarding privacy of medical records • Gives patients' rights in regard to disclosure of protected health information • Established penalties for violating patient privacy
Banking Information	Right to Financial Privacy Act (RFPA, 1978) Fair Credit Reporting Act, 1970	• RFPA gives US customers of financial institutions certain rights in relation to US government searches of a financial institutions' records and provides payment of damages to customers for violations • FCRA protects customers from inaccuracies in their credit information through regulating the collection, dissemination and use of consumer credit information
Genetic Information	Genetic Information Nondiscrimination Act (GINA, 2008)	• Limits ability of employers and health insurers to treat individuals differently based solely on tests that indicate a genetic predisposition to develop a medical condition in the future and provides for the privacy of this information
Journalistic Sources	Privacy Protection Act (1980)	• Protects journalistic sources and newsrooms from search from government officials without a subpoena
Information Generated by Telephone or Internet Communication	Electronic Communications Privacy Act (ECPA, 1986)	• Extends government restrictions on wire taps to include electronic data stored on a computer or while in transit
Biometric Information	State level legislation: i.e. Illinois Biometric Security Act	• Provides that citizens be informed before their biometric information is collected and that they are apprised in writing of conditions under which information will be stored, shared and destroyed
Information Related to a Job Candidate's Disability Status, Age, National Origin, Religious Beliefs, etc.	Legal cases involving Equal Employment Opportunity Commission, National Labor Relations Board	• New rulings forbid employers from 'Googling' potential job candidates to ascertain information about candidates' family status, sexual preference, race, etc. Social media should not be used to provide answers to questions which an employer is legally prohibited from posing during an interview.

Figure 4.3 Legal protection measures for citizen privacy

Box 4.4 Critical issues: what was the Silk Road?

The Silk Road was an illegal website which operated from 2010 until 2013, providing an international marketplace for trafficking in illicit goods and services – including drugs, computer viruses, malware and exploits, guns and assassination services. Users could access the site using the anonymizing software Tor, paying for their purchases with Bitcoin. At its height, it sold over 200 million dollars' worth of illegal products annually. Ross Ulbricht, the founder of Silk Road, was sentenced to life in prison for his activities. Authorities maintained that in operating the site he broke a number of federal and international laws, including those forbidding drug trafficking, money laundering and computer hacking.

While it is clear that Ulbricht's activities were illegal, how do we understand the ethics of a place like Silk Road? In his defense, Ulbricht has stated that he merely provided a site for people to carry out activities that they were going to do anyway. Indeed, one could make a utilitarian argument that he was providing a public service through allowing people who need drugs to obtain them without travelling to dangerous places late at night. Furthermore, in creating a marketplace for vendors to compete, it's possible that the resulting products will be more affordable and of better quality. The fact that what was being sold was illegal narcotics seems almost irrelevant, according to this argument.

Other defenders of the site have argued that most purchasers were not purchasing heroin or hard drugs, but were rather purchasing marijuana for recreational use. These individuals argued that ultimately the responsibility for policing one's use of drugs should fall to the individual user and not the

creator of the site. Blaming Ulrich for a heroin addict's death would be like blaming General Motors for someone's death from driving while intoxicated according to this logic.

However, one can also consider the ethics of complicity, in arguing that facilitating someone's death through heroin addiction is morally unethical. In this argument, Ulbricht failed to help someone who was addicted, instead encouraging that addiction. Indeed, six people are purported to have died from overdoses through using Silk Road

From a more pragmatic standpoint, analysts like Nelson (2015) have argued that once the technology for setting up a darknet market exists, it is perhaps inevitable that someone will invent one. He argues that even if Silk Road has been shut down, there will be others who will attempt to create similar marketplaces, either using Silk Road as a blueprint or going on to produce more elaborate markets as the technology evolves.

Sources

BBC News. 2015. "Silk Road Founder Ross Ulbricht Jailed." May 30. Available at www.bbc.com/news/world-us-canada-32941060. Accessed September 1, 2016.

Bertrand, Natasha. 2015. "Silk Road Wasn't Even Close to the Biggest Drug Market on the Internet." *Business Insider.com*. May 23. Available at www.businessinsider.com/silk-road-wasnt-even-close-to-the-biggest-drug-market-on-the-internet-2015–2016. Accessed March 12, 2017.

Nelson, Steven. 2015. "Buying Drugs Online Remains Easy, 2 Years After FBI Killed Silk Road." *USNEWS.com*. Available at www.usnews.com/news/articles/2015/10/02/buying-drugs-online-remains-easy-2-years-after-fbi-killed-silk-road. Accessed March 1, 2017.

Thinking about the ethics of privacy in a virtual environment is complicated, however, when we begin to ask not just about identities, including our digital identities, but when we begin to ask about our data as well. The term **digital footprint** refers to the data which we use and which we produce on all of our devices when we are online. As Kligiene explains:

> A digital footprint is a combination of activities and behavior when the entity under consideration (a person or something else) is acting in the digital environment. These may be log on or off records, address of visited web pages, open or developed files, e-mail or chat records.
>
> (Kligiene, 2012, 69)

In his work on information ethics, Floridi (2013) suggests that we own our digital footprint and that in a very real way, we *are* our digital footprints. He suggests that we feel harmed if our data is taken, shared or stored without our permission. We will feel equally violated by the thought of someone peeking at our data as we would if they physically peeked into our homes without our knowledge or consent. We would also feel equally violated if someone stole our virtual identity and proceeded to act in cyberspace as though they were us (Tavani, 2008).

But providing online and data privacy is challenging for three reasons: First, connectivity and networking has eroded the distinction between public and private space and public and private activities. In addition, our ability to store, share and aggregate data creates new problems of privacy. Finally, developments in the field of biometrics are eroding the distinction between our physical bodies and our digital bodies and identities, and creating new ethical challenges.

Problem one – connectivity and networking

Our information environment is characterized by **connectivity**, or the ability to make connections between points in a telecommunications system. We might furnish data to one particular website, but then it might be shared with other entities within a network, often without our knowledge or permission. And the distinction presented in part one of this chapter, between private and public space, does not map neatly onto cyberspace. Instead, activities today are characterized by a lack of clear demarcations between public and private spaces and public and private activities.

This distinction is particularly unclear in the area of social media. Sloan et al. define **social media** as "any electronic medium where users may create, share or view user-generated content which can include videos, photographs, speech or sound" (2012, 1). But does this social content which you generate – meant to be shared and viewed by others – belong to you alone, or does it also belong to other interested parties, like your employer or even to law enforcement agencies? Can we speak of a right to privacy in relation to social media?

This erosion of the public and private distinction poses a number of ethical and legal issues: Under what circumstances do we have a right to privacy online? Are there situations in which we should be required to relinquish this right to privacy and under what conditions? On the one hand, we may believe that as individuals we should have the right to say and do what we want online no matter where we are or what we are doing. But on the other hand, we also expect to feel and be safe in our workplaces and communities, to be protected from harassment and bullying, and for authorities to be aware of dangers and threats to our safety and perhaps even to act preemptively to protect us and keep us safe.

Problem two: privacy versus security

Clearly authorities – including employees – have the responsibility to police the safety of their environments, even if doing so means accepting that privacy violations will occur. Individuals and groups may need to monitor individual social media activities in order to safeguard individuals in the real world. In this view, the risks associated with allowing a disgruntled employee or even a terrorist to threaten individuals or carry out dangerous activities are so great that it is worth violating individual online privacy in order to secure the safety of those affected by an individual's online activities.

US legal developments support this ethical understanding that employers have a right and responsibility to monitor employee's personal social media posts – reacting to defamatory posts and those which show danger or disclose private or proprietary information. In the United States, the Electronic Communications Privacy Act establishes the principal that we do not have an absolute right to privacy online during working hours, whether we are physically or virtually located at a workplace. This law allows employers to monitor how their employees spend their time online during working hours – tracking the websites visited and the activities carried out. However, new laws are beginning to limit these rights. In Maryland, California and Tennessee, employers cannot ask employees for their names and passwords for social media accounts nor demand that they be added to accounts (Sloan et al., 2012) In Tennessee, employers are allowed to conduct activities which assure that employers are treating company data as confidential, which might include searching for postings in their name on social media. However, the legislation clearly specifies which employer activities would constitute an invasion of privacy and encroachment on a citizen's First Amendment rights to free speech. In addition, in Tennessee and in other states, some employee unions have written privacy clauses into their contracts, specifying exactly what employers may and may not ask for or monitor (workplacefairness.org, 2014).

The duty of individual users

In addition, many analysts today emphasize the principle that users of the internet now have a responsibility to proactively take steps to safeguard their own privacy and the integrity of their own data online. They

cannot simply expect that their internet service provider or the owner of a website which they use will take the necessary steps to safeguard their data, and thus need to be individually motivated to do so.

Floridi (2013) suggests that all information technology users should have a shared commitment to protecting the 'information infosphere.' In his work, he makes a similar sort of argument to that which environmentalists make – all of us should have a shared commitment to preserving the physical environment and should think about how our actions affect this environment. He argues that those who monitor the infosphere and those who use it have a responsibility to carry out practices which will preserve the internet as an entity which all can enjoy. This may mean making a decision not to engage in practices like spamming, harassment and trolling, and it may also mean taking a serious interest in practicing good cyberhygiene, from being aware of practices like phishing, to investing in a good firewall, to investigating and using Privacy Enhancing Technologies (PET) like authentication, biometrics and encryption.

Problem three – data storage and sharing

However, while individuals may be careful about privacy in their online interactions, they often don't think much about how their data is stored or shared. **Ubiquitous computing** refers to the practice of embedding technology within everyday objects so that they can store and collect data, sharing it with other objects within the Internet of Things to which they are connected. The technology in these objects is unobtrusive and users are often unaware that this data is being collected, stored and shared (Belloti, 1997).

Data mining refers to the practice of searching through databases in order to discover relationships and patterns (Tavani, 1999, 141). As Al-Saggaf notes, "Data mining can be used to classify and categorize, and to know more about a user and to make predictions about his future behavior – such as future purchasing behavior" (Al-Saggaf and Islam, 2015, 946). **Web usage mining** looks at the usage behavior of users – including what websites they visit, and what they are looking for online. These practices mean that if you visit the website for a university, the university's experts can tell what other pages you looked at first, and perhaps identify other universities that you might be considering for your program.

Thus, we must consider the ethical obligations of those tasked with collecting and storing or managing data. What standards should they adhere to, and what should be the penalties for not doing so? What should be their guiding principles and values, and who should they regard as their ethical subject? To whom are they answerable?

The most basic condition which those entities collecting data must adhere to is the notion of **informed consent**. This idea is borrowed from the standards and protocols established within the scientific community for **Human Subjects Protocols**. These conditions are laid out in the Belmont Report, a federal document issued in 1978 by the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. This report spells out the rights of individuals in relation to biomedical and behavior research, and was updated in 2010 to include internet research. The document uses a virtue ethics approach to argue that all research should be conducted with an eye towards respect for people (including their autonomy, courtesy, respect); beneficence; and justice (United States Department of Health and Human Services, 2013; Sims, 2010). Researchers must consider the dignity and feelings of human subjects in designing an experiment. At universities, researchers normally present a petition to a **Human Subjects Review Board** in which they spell out how they will meet specific conditions. Conditions may be federally mandated, mandated on a state or local level or mandated by the university itself.

Such conditions usually include the requirement that subjects are informed about the experiment's purposes, what they can expect to encounter in the experiment (including any possible side effects), how their anonymity will be maintained when researchers report the experiment's result and how data collected will be stored, maintained or destroyed. They are also told of their rights within the experiment – such as a right to stop participating at any time. Then they must give their written consent to participate in the study. The consent notice might spell out conditions such as whether data provided by users could be sold or shared with

other corporations or websites. It might also include a statement regarding acceptable and unacceptable behaviors online and the conditions under which a user might be censured or depermitted from a site.

Human Subjects Review protocols and their internet equivalent, the consent statement, help preserve subject's rights. But several problems presently exist with consent statements: First, many are long and unwieldy and subjects may simply not read all of the dense language. They might sign their rights away without fully considering what they are agreeing to (Duvall et al., 2015).

Second, those with limited English proficiency, a low level of literacy or cognitive impairments, including the elderly, might struggle to understand user agreements. Many people frequently do not understand what they are signing (Etzioni, 2015, 1269). Finally, some issues which are addressed in consent agreements might be **novel problems** which have not been fully addressed since they have not happened. For example, in the future, we may encounter scenarios where a tech company goes bankrupt and in the process of settling their accounts, their assets might be sold off. If their major asset is data which has been collected about users, this data might be sold to a third party.

Today, some analysts feel that because of the seriousness of these problems, those who collect data often commit ethical breaches in deceiving or coercing individuals to provide data. They note that in reality, citizens don't really have the ability to 'opt out' of most consent agreements, since they may require a cell phone to do their job, for example. Culnan and Williams (2009, 681) suggest that there is a fundamental power imbalance between the citizens who furnish data and the corporations that collect it. Citizens know less about the technology, the issues and their rights than corporations might, and thus, privacy harms are likely due to this power imbalance.

And Ellerbrok (2011) describes how users might decide that a new technology is harmless or even a fun "game" due to the circumstances under which it is introduced. For example, she suggests that Facial Recognition (FR) technology actually has military applications, such as scanning a crowd in order to identify individuals who are on the United States Terror Watch List. However, because most people encounter FR when it tags their friends on Facebook, they do not associate it with military applications. Here we might call the technology's creators deceptive, since they created acceptance of the new technology by introducing it in this way without making sure that users understand all of its applications.

Box 4.5 Going deeper: what is HIPAA?

Who should have access to your medical information and under what circumstances? For health care workers and administrators, the challenge in managing health information is how to make it available quickly and efficiently to those who might need it in a disaster or emergency situation versus how to safeguard private medical information daily. Putting information into a database allows providers to quickly access information – with groups like the US military acting as leaders in the centralization and sharing of medical information, acting to make information about a soldier available wherever he is. For individuals who might be older and in poor health, it is doubly important for health care providers to be able to access their health information in the event that they cannot speak for themselves.

Today our health information is generated and stored in a variety of formats – by our own physicians or our health centers, by pharmacists and health insurance companies. Most of us appreciate the convenience of not having to be responsible for reproducing this medical information every time we need it. However, we may not be fully aware of how many people have access to our information and under what circumstances. Today, ethicists are concerned about the possibility that individuals and corporations might be able to access this information for the purposes of discriminating against us – for example, in getting insurance as a driver. In addition, Williams notes that health information may be of a

highly private or even embarrassing nature, and may include information about issues like sexual behavior or psychiatric history.

In the United States, the Health Information Privacy Act (HIPAA) mandates that patients give informed consent before their health information is shared with anyone other than themselves, including family members and in some cases, family members of minor children. HIPAA, passed in 1996, mandates that precautions be taken to mandate the confidentiality of patient data in terms of how it is collected and stored and who else may have access to it. In the final version passed in 2013, the HIPAA Omnibus Rule, stored information may also include the patients' financial information. Confidentiality may only be breached in a limited number of instances such as when a patient has a communicable disease which poses a public health risk. The legislation also provides for criminal penalties for personnel or providers who commit a HIPAA breach. Indeed, in 2010 a California nurse received jail time after she improperly accessed and shared information on celebrities' health conditions (Morris, 2013).

Breaches of patient confidentiality

Security breaches are thus particularly worrisome. Breaches fall into two types – those which are intentional, usually carried out by outside hackers aimed at getting information, and those which occur often internally because of negligence and poor skills with using databases and managing information. As Williams points out, both types of information breaches are growing in number and severity (Williams, No date). In 2013, a laptop was stolen from a physician. It contained information about approximately 57,000 patients who had been treated at Stanford University School of Medicine in Palo Alto, California. Information breaches can occur through physical theft or computer viruses. In June 2015, a large-scale attack on Anthem Healthcare led to hackers getting access to 80 million company records.

Redspin, a company that does pen testing for health care companies, reports that between 2009 and 2014, 40 million Americans suffered health information breaches.

HIPAA also mandates that patients be informed if their information will be used for research purposes. In addition, HIPAA may complicate procedures in situations where, for example, individuals are diagnosed with a genetic disease where public health practices suggest notifying other relatives who may be at risk of suffering from the same disease.

Sources

Barlow, Rick. 2015. "Horizon-Scanning Around HIPAA, HITECH." *Health Management Technology*. May 28. Available at www.healthmgttech.com/horizon-scanning-around-hipaa-hitech.php. Accessed March 12, 2017.

Morris, Kathleen. 2013. "Sing a Song of HIPPA." *Ohio Nurses Review* 88(2): 4–12.

Williams, Terri. No Date. "Ethical Challenges in the Management of Health Information." *CHron.com*. http://smalbusiness.chron.com/ethical-challenges-management-health. Accessed March 11, 2017.

However, others emphasize the fact that users also have a responsibility to inform themselves and to understand and use privacy enhancing technologies to safeguard their own data. Here, Burkert defines **privacy enhancing technologies (PETs)** as "technical and organizational concepts that aim at protecting personal identity." PETS can include technologies like encryption and encryption measures like digital signatures and pseudonyms. PETS can thus allow users to have more control over how much of their information is revealed, and in what format.

An ethical approach to data storage

What then might an ethical approach to data storage look like? Here we assume that data is ethically neutral, neither ethical nor unethical. What is ethical or unethical are the decisions which managers make in regard to that data – what to collect, how to store it and how to treat data which is stored. In this regard, Etzioni suggests that we consider three factors – the volume of information collected, the level of sensitivity of that information, and the degree of 'cybernation' which is taking place.

Here the term 'cybernation', based on a wordplay from the term hibernation, refers to the storage or stockpiling of information, to include compiling a dossier and sharing information between agencies and groups. (Etzioni, 2015, 1273) Etzioni notes that there is a difference between, for example, collecting a small volume of information about someone (such as their answers to a survey), and engaging in collection of bulk data. Here, **bulk data** is defined as "information from multiple records, whose primary relationship to each other is their shared origin from a single or multiple databases" (Information Resource of Maine, No date, no pagination). In addition, Etzioni distinguishes between the collection of **metadata** – defined as "Structured information that describes, explains, locates or otherwise makes it easier to retrieve, use or manage an information resource" (NISO, 2004, 1), and specific data related to a user, arguing that reading all of someone's e-mail correspondence, for example, is more intrusive than merely running an algorithm which looks for keywords in a large collection of data.

In addition, he suggests that collectors have a particular responsibility to safeguard sensitive information which might be of an intimate or highly intrusive nature. He states:

> Not all personal information can or should be accorded the same level of protection and that the more sensitive the information an agent seeks to collect, the more measures to protect privacy should be implemented and the higher the public interest must be before collection of the information is legitimate.
>
> (Etzioni, 2015, 1278)

In addition, those who collect data are seen as having an ethical obligation to inform citizens in situations where a privacy breach may have occurred. Here, a privacy breach is defined as "the loss of unauthorized access to, or disclosure of, personal information" (Office of the Privacy Commissioner of Canada, 2016). In the United States, this obligation is currently spelled out in state-level legislation with Congress currently debating laws to establish a national standard for data breach notification. In Europe the Directive on Privacy and Electronic Communications (E-Privacy Directive) includes a **breach notification law**.

Finally, corporations are seen as having an ethical obligation to carry out **Privacy Impact Assessments** (PIA's) prior to establishing new systems or new uses of personal information. A Privacy Impact Assessment may examine whether proposed changes in a system comply with legal requirements, as well as examining the risks associated with collecting and using personal information. It may also propose mitigation measures in situations where a breach occurs (Culnan and Williams, 2009). The E-Government Act of 2002 requires that US federal agencies carry out a Privacy Impact Assessment prior to developing public information systems.

Currently, the Council for Big Data, Ethics and Society is proposing measures to assure that subjects' data privacy is preserved. Such measures include requiring a '**data ethics plan**' in grant applications such as those administered by the United States National Science Foundation (Metcalf, 2014).

Problem four – biometrics

A final issue related to the ethics of privacy to consider is the increasing use of biometrics in online interactions. **Biometrics** is defined as "the measurement and statistical analysis of people's physical and behavioral characteristics … used for identification and access control, or for identifying individuals that are under surveillance" (Techtarget, No date, 1). As noted earlier in this chapter, biometrics can provide a way of authenticating the identities of citizens, thus providing increased security from crime, including terrorism. Biometric technologies such as requiring a fingerprint in order to operate a cell phone or other device are

effective ways of creating authentication, and assuring that unauthorized users do not access a device or impersonate the rightful user. But on the other hand, in recent years, citizens have complained that biometric technologies such as software which identifies individual's faces and then 'tags' them with their names in photos is a breach of privacy.

The first US state to enact specific legislation guaranteeing biometric privacy was Illinois. That statute, the **Illinois Biometric Information Privacy Act** explicitly forbids the collection of biometric data by means of a scan of someone's body or records without their consent. This law forbids practices like Facebook's use of facial recognition technology, based on a scan of a user's photographs, to identify their image in pictures posted to their site. (However, attempts to sue Facebook using this law have been unsuccessful as judges have concluded that since Facebook is located in California, any claims against them would need to be litigated in a California court, and not in Illinois.)

Prabakar et al. (2003) cite three ethical arguments against the use of biometric technologies. First, they argue that biometric technologies may have an unintended functional scope, revealing more information about the individual through, for example, a fingerprint scan, than he may have intended to share. (For example, they suggest that one's physical characteristics may be associated with a medical syndrome which the patient may not wish to publicize.) Next, they argue that these technologies may have an unintended application scope, in identifying people who may wish to keep their identity confidential. Finally, they argue that these technologies have the potential to provide covert recognition, and to reduce individuals' abilities to maintain anonymity in their daily lives and activities.

In their work, these analysts suggest that organizations which collect biometric data need to develop their own ethical code of conduct for professionals in this field, as well as perhaps creating an independent regulatory agency to enforce standards of behavior. They also point to provisions of the European Data Privacy Directive which establish strict protocols regarding the storage and sharing of biometric identifiers and suggest that the United States needs to develop similar national level legislation spelling out the rights of citizens in regard to use of this technology and establishing restrictions regarding how corporations and the government can collect, store, share and destroy this data.

Applying the lenses

Thus far we have looked at specific problems – such as the rights and responsibilities of both data producers and those who work with data, the ethics of using biometric data and problems related to connectivity. In our final section of this chapter, we will apply the three specific ethical lenses – Virtue Ethics, Utilitarian Ethics and Deontological Ethics – to think about the more general issues of privacy, spying and surveillance.

Virtue ethics

In 1929, United States Secretary of State Henry Stimson made the decision to close the State Department's code-breaking office, believing that the activities of spying and invading another's privacy were not in keeping with what he saw as the diplomatic mission of the State Department. Later in the aftermath of the bombing of Pearl Harbor, he was asked to explain how he had made the decision for the State Department to stop engaging in espionage activities. In response, he famously stated that "gentlemen do not read each other's mail" (Burtness and Ober, 1968, 27).

We can view this statement as a summation of the virtue ethics position on privacy. Stimson referred to breeding and character in justifying his decision to end the State Department's involvement in espionage activities, as well as to what he saw as a "gentleman's" orientation towards the rights of others, including the right to privacy. Here Stimson could be seen as supporting the virtue of **restraint** – in acknowledging that just because one has the capacity to do something, one can still decide to discipline oneself not to do it. As Steele points out in his discussion of when states should engage in restraint, Aristotle himself first asked questions

regarding the conditions under which a person should be prudent or continent, and the conditions under which one was likely to be incontinent or unrestrained. Aristotle argues that there are many situations in which one might find oneself carried forward by desire or wanting, but that restraint refers to the quality of stopping this momentum (Steele, 2014, 9). Steele notes that an individual might wish to do something due to social conditioning or peer pressure, and that restraint may thus require strength to resist these forces. Many professions include restraint as a professional ethic. As noted in the beginning of this chapter, physicians, psychologists and even priests may be in a position whereby they are provided with access to private information. However, their professional training emphasizes the fact that they are morally required to restrain themselves from either sharing or profiting from that information. Similarly, Black (1994) argues that journalists frequently engage in restraint in, for example, declining to publish the names of rape victims, even if they could profit by providing the public with this information.

Virtue ethics thus suggests that even if one has a strong desire to invade another's privacy, and even if the environment is structured in such a way that one could presumably get away with doing so, and even if one is pressured to do so, the virtuous individual (or organization or state) should choose to improve his character by engaging in restraint.

The shorthand statement "gentlemen do not read each other's mail" is also an absolute statement. It is unambiguous, and there is no room in the statement for compromise – such as allowing a limited amount of spying or invasion of privacy, or allowing it in a limited range of circumstances.

For those who came to view Stimson and his decision as responsible for the mass casualties sustained in the Japanese attack on Pearl Harbor, the virtue ethics position seemed naïve and idealistic, and not in keeping with the realities of a world which was on the brink of war. In considering their objections to Stimson's argument, we can consider why people might object to a virtue ethics argument against spying or espionage in general. First, those who disagree with Stimson point out that Stimson, in stating that "gentlemen do not read each other's mail," was not simply stating his own position, but rather was assuming that there was a norm or shared understanding amongst all who engaged in diplomacy. That is, a decision not to spy because it was not in keeping with one's character as diplomacy would only work if everyone engaged in diplomacy behaved in the same way. Otherwise, the gentleman merely stands to be taken advantage of (or exploited and defeated) by others who are less gentlemanly. Today, we might point to the actions of other nations – like North Korea or Russia – who are willing to 'read each other's mail' or engage in espionage, to make the argument that the United States could not afford to take the virtue ethics position without conceding defeat to less virtuous opponents.

Indeed, in Plato's *Republic*, Plato recounts the story of a shepherd, Gyges, who receives a ring that is able to render him invisible (and thus capable of spying). Here, Plato asks us to consider whether anyone, given such a power, would be able to restrain himself, only using the power for good. Plato suggests that inevitably, one might decide to use this power to gain an unfair advantage over one's companions. In the story, Gyges uses his power of invisibility to seduce the king's wife and to gain riches and power. Plato's story suggests that one could be a 'virtuous spy' if one were able to use these powers with right intent, but acknowledges that the temptation to use the same power for less than virtuous intents is very strong (Allen, 2008).

Similarly, Stimson's detractors suggested that he was naïve in assuming that all diplomats would have the same intent, deciding to eschew spying in order to respect other's rights. At the time that Stimson was in charge of the State Department, the United States did not have a separate Department of War, nor did it have a separate set of intelligence agencies. However, in later years, Stimson actually became the head of the United States Department of War. In this capacity, he supported the use of espionage by the military community. Thus, one might argue that Stimson's original position was naïve, since he was only able to be moral and virtuous as a diplomat because individuals in other groups – such as the military – were willing to violate their own character and principles in order to defend US national interests. It was the utilitarian ethic of others that allowed Stimson to maintain his position from virtue ethics.

Utilitarian ethics

As noted, virtue ethics focuses on character. In contrast, utilitarian ethics asks: What type of good is produced through engaging in surveillance and spying in this particular situation? Does the utility produced through engaging in privacy violations outweigh any potential harm that might come from violating someone's privacy?

Perhaps the most famous utilitarian statement on spying is the sentence uttered by the American soldier Nathan Hale, who collected intelligence about British activities during the Revolutionary War. (He was later captured and executed by the British.) Hale famously justified his espionage activities and the deception which they required by stating that "Every kind of service necessary to the public good becomes honorable by being necessary" (Quoted in Robarge, 2007, no pagination).

More recently, journalist Olga Khazan (2013) defended US and British surveillance practices, arguing that the first goal of public servants should be to advance a country's interests and keep its citizens safe. She describes how the British intelligence agency GCHQ set up fake internet cafes for delegates to the 2009 G20 meetings in London to use. The computers provided had software which logged users' keystrokes and recorded their communications. Khazan (2013) argues that a nation concerned with cyberwarfare and terrorism threats is justified in engaging in code-breaking, intercepting mail and telegraph communications. Similarly, Hladik describes the ways in which the US National Security Agency justified the surveillance practices which Snowden detailed in 2012. She notes:

> The NSA and (British) GCHQ maintain that what American and British citizens gain in security from this massive data collection outweighs what they lose in privacy, so the practice in justified.
>
> (Khazan, 2013, 3)

Hladik (2014) explains that US decision makers in particular argued that without such a massive spying program, the United States risked "going dark" or losing their ability to track the underground and covert activities of those who wished to harm America, including possible terrorists and drug cartels. Invoking John Stuart Mill, Hladik explains that US decision makers see the decision to defend America's citizens through spying as granting them happiness (or safety). The amount of happiness engendered through these actions is sufficient to outweigh the unhappiness they might encounter in having their privacy violated.

Corporations have made similar utilitarian arguments to explain why they monitor their employee's activities online. Covert (2013) suggests that such activities are a necessary evil, which allows companies to continue to operate as productive, efficient corporations, thereby enriching shareholders and continuing to provide employment for their workers.

Deontological ethics

Finally, let's consider the deontological approach. Remember, this approach includes an injunction against treating people as a means to an end. Deontologists believe that it's unethical to manipulate or deceive people in order to get access to their data, and that it would also be inappropriate to treat people merely as sources of data.

Thus, deontologists worry about issues of **gate-keeping**, where people are required to provide personal information like an e-mail address or access to their Facebook account in order to read an article or visit a website. Here users have little choice and no autonomy in deciding whether or not to provide their data. Indeed, one could argue that they are being coerced into providing this information (Alterman, 2003). Bergstrom (2015) also expresses concern about situations in which users are promised a reward in return for furnishing personal data – such as a faster download speed for an article, or additional points in an online game, for example. He asks if individuals are being manipulated or misled in some way into furnishing personal data.

Alterman (2003) argues that the collection of biometric data in particular violates deontological ethics – since it inherently treats individuals as a means to an end, rather than as an end in itself. He writes

> The use of mandatory biometric identification for people who have committed no crime, as with EURODAC, seems like a paradigmatic offense against Kantian principles, for it is a clear case of taking the person as a mere thing, using their body as a means to an end.
>
> (146)

He argues that people who object are not merely being paranoid, noting that "we do not expect that our Super Bowl ticket will make us part of a digital lineup (to capture criminals) and we might be horrified to learn that the barber sold our hair to a DNA research laboratory" (146).

Thus, in order to treat users with dignity and respect, states and corporations need to have strict procedures in regard to informed consent (Culnan and Clark; Culnan and Williams). They also need to consider questions of equity through asking: does everyone have an equal ability to refuse to provide personal information, or are those who are less literate or less wealthy at a disadvantage? Does everyone understand equally well what they are agreeing to?

However, not everyone accepts this approach. Some critics say that deontologists focus too much on individual rights while neglecting the ways in which communities often benefit through large-scale data collection. For example we can consider practices like tracking the spread of infectious disease through collecting information on internet searches for flu symptoms. Here a utilitarian would argue that preventing the deaths of vulnerable populations – like infants and the elderly – through engaging in health surveillance is a greater good than protecting the rights of individuals to be free from such surveillance.

Chapter summary

- Today, decision makers increasingly face trade-offs between an individual's right to keep his private life private and the obligations of employers and the government to keep citizens safe.
- Understandings of privacy are evolving along with new technologies which blur boundaries between public and private space and public and private life.
- It is often unclear who your data belongs to – when does it cease being yours, who has the right to collect it and what are their obligations to safeguard this data?
- Today, some analysts argue that individuals have an ethical responsibility to share their data in order to achieve large-scale social goals, like preventing a pandemic.

Discussion questions

1 Today, many cities in the United States are implementing so-called "open data programs" which allow local residents to view a city's budget and purchasing decisions. Name some privacy concerns which might arise through such an initiative and suggest how they might be resolved.

2 Many companies in the United States now offer their employees the opportunity to engage in a Wellness Program. Employees receive a financial incentive for engaging in behaviors like losing weight and exercising and data might also be shared with insurance companies. What privacy issues can be identified here and how might they be resolved?

3 Today, many younger people state that they really don't care about privacy because they have grown up sharing a great deal of personal information. Do you agree with this statement or do you think privacy is still important? Why?

4 Do you feel that individuals have the right to know personal information about their country's leaders? Should someone who wants to be president, for example, be required to provide voters access to all personal medical and financial information? Why or why not?

Recommended resources

Kendrick, Katherine. 2015. "Risky Business: Data Localization." *Forbes*. February 19. Available at http://forbes.com/sites/realspin/2015/02/19/risky-business-data-localization.htm. Accessed March 11, 2017.

Madden, Mary, and Rainie, Lee. 2015. "Americans' Attitudes About Privacy, Security and Surveillance." May 20. Philadelphia, PA: Pew Research Center. Available at www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/. Accessed March 12, 2017.

Mittelstadt, Brent, Allo, Patrick, Taddeo, Mariarosaria, Wachter, Sandra, and Floridi, Luciano. 2016. "The Ethics of Algorithms: Mapping the Debate." *Big Data & Society* 3(2): 1–16.

Nussbaum, Martha. 2001. "Is Privacy Bad for Women?" *Boston Review*. April 1. Available at http://bostonreview.net/world/martha-c-nussbaum-privacy-bad-women. Accessed December 2, 2017.

Tavani, Herbert T. 1999. "Information Privacy, Data Mining and the Internet." Ethics & Information Technology 1(2): 137–145.

Tene, Omer, and Polonetsky, Jules. 2013. "A Theory of Creepy: Technology, Privacy and Shifting Social Norms." *Yale Journal of Law & Technology* 16: 59–134.

United States Department of Homeland Security. 2012. "The Menlo Report: Ethical Principles Guiding Information and Communication Technology Research." April. Washington, DC: United States

Government Publishing Office. Available at www.caida.org/publications/papers/2012/menlo_report_actual_formatted/. Accessed April 3, 2017.

Readers are also encouraged to visit the online journal *Surveillance and Society*. Volume 10, No. 4 features a series of short articles debating the subject of online privacy. The publication is available at http://ojs.library.queensu.ca/index.php/surveillance-and-society/issue/view/Open_Dec2012. Accessed March 12, 2017.

Chapter 4 sources

Aicardi, Christine, De Savo, Lorenzo, Dove, Edward, Lucivero, Federica, Tempini, Niccolo, and Prainsack, Barbara. 2016. "Emerging Ethical Issues Regarding Digital Health Data: On the World Medical Association Draft Declaration on Ethical Considerations Regarding Health Databases and Biobanks." *Croatian Medical Journal* 57(2): 207–213.

Allen, Anita L. 2008. "The Virtuous Spy: Privacy as an Ethical Limit" *The Monist*, January 2008.

Al-Saggaf, Yeslam, and Islam, Zahidul. 2015. "Data Mining and Privacy of Social Network Sites' Users: Implications of the Data Mining Problem." *Science and Engineering Ethics* 21(4): 941–966.

Alterman, Anton. 2003. "'A Piece of Yourself': Ethical Issues in Biometric Identification." *Ethics and Information Technology* 5(3): 139–150.

Ballotpedia. No Date. "Government Transparency." Available at https://ballotpedia.org/Government_transparency. Accessed February 2, 2017.

Belloti, Victoria. 1997. "Design for Privacy in Multimedia Computing and Communications Environments." In Philip E. Agre and Marc Rotenburg, eds. *Technology and Privacy: The New Landscape*. Boston, MA: The MIT Press.

Bergstrom, Annika. 2015. "Online Privacy Concerns: A Broad Approach to Understanding the Concerns of Different Groups for Different Uses." *Computers in Human Behavior* 53: 419–426.

Black, Jay. 1994. "Privacy in America: The Frontier of Duty and Restraint." *Journal of Mass Media Ethics* 9(4): 213–234.

Bok, Sisella. 1989. *Secrets: On the Ethics of Concealment and Revelation*. New York: Vintage Books.

Boyd, Danah, and Marwick, Alicia. 2011. "Social Privacy in Networked Publics: Teens' Attitudes, Practices and Strategies." (Apophenia Blog) May 9. Available at www.zephoria.org/thoughts/archives/05/09/2011/how-teens-understand-privacy.html. Accessed February 2, 2017.

Brey, Philip. 2007. "Ethical Aspects of Information Security and Privacy." In M. Petkovic and W. Jonker, eds. *Security, Privacy, and Trust in Modern Data Management*. Heidelberg: Springer: 21–36.

Burtness, Paul, and Ober, Warren. 1968. "Secretary Stimson and the First Pearl Harbor Investigation." *Australian Journal of Politics and History* 14(1): 24–36.

Careerbuilder.com. 2014. "Number of Employees Passing on Applicants Due to Social Media Posts Continue to Rise, According to New CareerBuilder Survey." June 26. Available at www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2014&id=pr829&ed=12%2F31%2F2014. Accessed January 2, 2017.

Cavoukian, Ann, Chibba, Michelle, and Stoianov, Alex. 2012. "Advances in Biometric Encryption: Taking Privacy by Design From Academic Research to Deployment." *Review of Policy Research* 29(1): 37–61.

Chinchilla, Rigoberto. 2012. "Ethical and Social Consequences of Biometric Technologies." American Society for Engineering Education Annual Conference. Available at www.asee.org/public/conferences/8/papers/3789/view. Accessed February 2, 2017.

Colarik, Andrew, and Ball, Rhys. 2016. "Anonymous vs. ISIS: The Role of Non-State Actors in Self-Defense." *Global Security and Intelligence Studies* 2(1): 20–34.

Covert, Edwin. 2013. "The Ethics of Monitoring Your Employees." *InfoSec Island.com*. September 2. Available at www.infosecisland.com/blogview/23366-The-Ethics-of-Monitoring-Your-Employees.html. Accessed February 21, 2017.

Culnan, Mary, and Williams, Cynthia. 2009. "How Ethics Can Enhance Organizational Privacy: Lessons From the Choice Point and TJX Data Breaches." *MIS Quarterly* 33(4): 673–687.

Doyle, Charles. 2012. "'Privacy': An Overview of the Electronic Communications Privacy Act." October 9. Washington, DC: Congressional Research Service.

Duvall, Nikolina M., Copoulos, Antona, and Serin, Ralph C. 2015. "Comprehension of Online Informed Consent: Can It Be Improved?" *Ethics and Behavior* 26(3): 177–193.

Egan, Matt. 2016. "What Is the Dark Web?" *PC Advisor*, March 3. Available at www.pacadvisor.co.uk/how-to. Accessed December 2, 2016.

Ellerbrok, Ariane. 2011. "Playful Biometrics: Controversial Technology Through the Lens of Play." *The Sociological Quarterly* 52(4): 528–547.

Etzioni, Amitai. 2015. "A Cyber Age Privacy Doctrine: More Coherent, Less Subjective and Operational." *Brooklyn Law Review* 80(4): 1267–1296.

Floridi, Luciano. 2011. *The Philosophy of Information*. Oxford: Oxford University Press.

Floridi, Luciano. 2013. *The Ethics of Information*. Oxford: Oxford University Press.

Floridi, Luciano. 2015. "'Should You Have the Right to Be Forgotten on Google?' Nationally Yes, Globally No." *New Perspectives Quarterly* 32(2): 24–29.

Giang, Vivian. 2013. "Eleven Common Interview Questions That Are Actually Illegal." *Business Insider*. July 5. Available at www.businessinsider.com/11-illegal-=interview-questions-2013. Accessed March 13, 2017.

Haggard, Stephen, and Lindsay, Jon. 2015. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace." *Asia-Pacific Issues, No. 117*. Washington, DC: East-West Center. Available at https://scholarspace.manoa.hawaii.edu/bitstream/10/25/36444/1/api117.pdf. Accessed May 2, 2017.

Hirsch, Dennis. 2014. "The Glass House Effect: Big Data, the New Oil and the Power of Analogy." *Maine Law Review* 66(2): 374–389.

Hladik, Casey. 2014. "Rusbridger's 'The Snowden Leaks and the Public' and Mill's *Utilitarianism*: An Analysis of the Utilitarian Concern of 'Going Dark.'" *Stance* 7: 29–40.

Information Resource of Maine. No Date. *RE: Answers to Questions Posed by the Right to Know Advisory Committee/Bulk Records Subcommittee*. Augusta, ME: Information Resource of Maine.

ISC^2. 2016. *ISC^2 Code of Ethics*. Available at www.ISC2.org/ethics

Johnson, Deborah. 1985. *Computer Ethics*. New York: Pearson.

Kelly, John. 2015. "Domestic Terrorist Runs Gamergate Board; Hinders Free Speech and Anonymity." *Medium.com*. December 15. Available at https://medium.com/@jkellytwit/domestic-terrorist. Accessed December 3, 2016.

Kernaghan, Kenneth. 2014. "Digital Dilemmas: Values, Ethics and Information Technology." *Canadian Public Administration* 57(2): 293–317.

Khazan, Olga. 2013. "Gentlemen Reading Each Other's Mail: A Brief History of Diplomatic Spying." *The Atlantic*. June 17. Available at www.theatlantic.com/international/archive/2013/06/gentlemen-reading-each-others-mail-a-brief-history-of-diplomatic-spying/276940/. Accessed April 11, 2017.

Kligiene, Stanislava. 2012. "Digital Footprints in the Context of Professional Ethics." *Informatics in Education* 11(1): 65–79.

Kruh, Louis. 1998. "Stimson, the Black Chamber and the 'Gentlemen's Mail' Quote." *Cryptologia* 12(2): 65–89.

Li, Han, Sarathy, Rathindra, and Xu, Heng. 2009. "Understanding Situational Online Information Disclosure as a Privacy Calculus." *The Journal of Computer Information Systems* 51(1): 62–71.

MacKinnon, Katherine. 1987. *Feminism Unmodified*. Cambridge, MA: Harvard University Press.

Mansfield-Devine, Steve. 2015. "The Ashley Madison Affair." *Network Security* 9: 8–16.

Marmor, Andrei. 2015. "What Is the Right to Privacy?" *Philosophy and Public Affairs* 43(1): 3–26.

McFarland, Michael. No Date. *Ethical Implications of Data Aggregation*. Santa Clara, CA: Markkula Center for Applied Ethics.

Metcalf, Jacob. 2014. "Ethics Codes: History, Context and Challenges." *Council for Big Data, Ethics and Security*. November 9. Available at http://bdes.datasociety.net/council-output/ethics-codes-history-context-and-challenges/. Accessed January 2, 2017.

Michmerhuizen, Sue. 2007. *Confidentiality, Privilege: A Basic Value in Two Different Applications*. Washington, DC: American Bar Association Center for Professional Responsibility.

Min, Jinyoung, and Kim, Byoungsoo. 2015. "How Are People Enticed to Disclose Personal Information Despite Privacy Concerns in Social Network Sites? The Calculus Between Benefit and Cost." *Journal of the Association for Information Science and Technology* 66(4): 839–857.

Moor, James. 1997. "Towards a Theory of Privacy in the Information Age." *SIGCAS Computers and Society* 27(3): 27–32.

Moore, Adam, ed. 2013. *Information Ethics: Privacy, Property and Power*. Seattle, WA: University of Washington Press.

Moore, Adam D., and Kristene Unsworth. 2005 "Introduction to Information Ethics: Privacy, Property, and Power." In Information Ethics: Privacy, Property, and Power, Adam D. Moore, ed. University of Washington Press.

Nagel, Thomas. 1998. "Concealment and Exposure." *Philosophy and Public Affairs* 27(1): 3–30.

NISO Press. 2004. *Understanding Metadata*. Bethesda, MD: NISO Press.

Nissenbaum, Helen. 1997. "Toward an Approach to Privacy in Public: Challenges of Information Technology." *Ethics and Behavior* 7(3): 207–219.

Nissenbaum, Helen. 2005. "Where Computer Security Meets National Security." *Ethics and Information Technology* 7(2): 61–75.

Office of the Privacy Commissioner of Canada. 2016. "Privacy Breaches." November 1. Available at www.priv.gc.ca/en/privacy-topics/privacy-breaches/. Accessed January 5, 2017.

Persily, Nicholas. 2017. "Can Democracy Survive the Internet?" *Journal of Democracy* 28(2): 63–76.

Plato. 1967. *The Laws*. Cambridge, MA: LCL.

Prabakar, Sail, Pakanti, Sharanth, and Jain, Anil. 2003. "Biometric Recognition: Security and Privacy Concerns." *IEEE Security and Privacy* March/April 2003: 32–42.

Robarge, David. 2007. *Review of Fair Play: The Moral Dilemmas of Spying*. McLean, VA: Central Intelligence Agency Library Center for the Study of Intelligence. Available at www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol51no1/fair-play-the-moral-dilemmas-of-spying.html. Accessed December 2, 2016.

Rubin, Alissa J. 2017. "France Let's Workers Turn Off, Tune Out and Live Life." *New York Times*. January 2. Available at http://nytim.ms/2hM3kyZ. Accessed January 4, 2017.

Sade, Renea. 2016. "When Does a Workplace Quality as Being Hostile?" *Seattle Business Magazine*. May. Available at www.seattlebusinessmag.com/business-corner/workplace/when_does_workplace. Accessed March 2, 2017.

Sandel, Michael. 1998. *Liberalism and the Limits of Justice*. Cambridge, MA: Cambridge University Press.

Sarah, Samir. 2016. "Navigating the Digital Dilemma." *Digital Debates 2016*. October 13. Observer Research Foundation: New Delhi, India. Available at www.orfonline.org/expert-speaks/navigating-the-digital-trilemma-2/. Accessed February 5, 2016.

Saunders, William. No Date. "The Seal of the Confessional." *Catholiceducation.org*. Available at www.catholiceducation.org/en/religion-and-philosophy/catholic-faith/the-seal-of-the-confessional.html. Accessed March 13, 2017.

Sims, Jennifer. 2010. "A Brief Review of the Belmont Report." *Dimensions of Critical Care Nursing* 29(4): 173–174.

Sloan, Jeff, Cherel, Christina, and Yang, Albert. 2012. "Social Media and the Public Workplace: How Facebook and Other Social Tools Are Affecting Public Employment." League of California Cities Annual Conference. Available at www.publiclawgroup.com/wp-content/uploads/2012/12/2012-09-01-League-of-CA-CitiesSloanYang-Social-Media-and-the-Public-Workplace-FINAL.pdf. Accessed January 2, 2017.

Stanford Encyclopedia of Philosophy. 2013. "Privacy." Available at https://plato.stanford.edu/entries/privacy/. Accessed January 2, 2017.

Steele, Brent. 2014. "Of Body and Mind, of Agents and Structures: Akrasia and the Politics of Restraint." Paper presented at the 2014 ISA-West Meeting, Pasadena, CA. Available at www.academia.edu/15574573/Akrasia_and_Restraint_in_International_Relations. Accessed January 3, 2017.

Tavani, Herman. 2008. "Floridi's Ontological Theory of Information Privacy: Some Implications and Challenges." *Ethics and Information Technology* 10(2): 155–166.

Techtarget. No Date. "What Is Biometrics?" Available at http://searchsecurity.techtarget.com/definition/biometrics. Accessed May 3, 2017.

Tuffley, David, and Antonio, Amy. 2016. "Ethics in the Information Age." *Australian Quarterly* January–March: 19–24.

United States Department of Health and Human Services. 2013. "Considerations and Recommendations Concerning Internet Research and Human Subjects Research Regulations, With Revisions." Available at www.hhs.gov/ohrp/sites/default/files/ohrp/sachrp/mtgings/2013%20March%20Mtg/internet_research.pdf. Accessed January 10, 2017.

United States Department of Homeland Security. No Date. "If You See Something, Say Something." Available at www.dhs.gov/see-something-say-something. Accessed December 2, 2016.

Van den Hoven, N.J. 1997. "Privacy and the Varieties of Moral Wrong-Doing in an Information Age." *SIGCAS Computers and Society* 27(3): 29–37.

Van den Hoven, Jeroen. 2008. "Information Technology, Privacy, and the Protection of Personal Data." In: Jeroen van den Hoven and John Weckert, eds. *Information Technology and Moral Philosophy*. New York: Cambridge University Press.

Warren, S.D. and Brandeis, L.D. 1890. "The Right to Privacy." *Harvard Law Review* 4(15): 1–19. Available at http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Accessed February 2, 2017.

Wilkins, Lee, and Christians, Clifford. 2008. *Handbook of Mass Media Ethics*. New York: Routledge.

Workplacefairness.org. 2014. "Social Networking and Computer Privacy." Available at www.workplacefairness.org/social-network-computer-privacy-workplace. Accessed March 13, 2017.

5 The problem of surveillance

Learning objectives

At the end of this chapters, students will be able to:

1. Define different types of surveillance (covert, asymmetrical, differential)
2. Describe laws which affect surveillance practices
3. Articulate a Virtue Ethics, Consequentialist/Utilitarian and Deontological argument in favor of and against surveillance
4. Describe the trade-offs between privacy, surveillance and security
5. Compare and contrast ethical and unethical surveillance practices
6. Describe what is meant by differential surveillance and identity three ethical issues associated with differential surveillance

As we consider the ethical problem of surveillance in this chapter, we can consider five real-life situations involving the use of surveillance by a government, corporation or individual:

- In 2016, the online retailer Amazon received a legal request for access to all of the data collected by the Amazon Echo in-home device belonging to James Andrew Bates of Bentonville, Arkansas. Bates is accused of having murdered Victor Collins in Bates' home in November 2015, and prosecutors believed that the Amazon Echo might have recorded the altercation which led to the murder, storing the data on the device as well as on Amazon's servers. At this time, judges have not ruled whether data collected in this manner is admissible in court as evidence, and whether Amazon can be compelled to furnish this data (Morris, 2016; Swearingen, 2016).
- In the fall of 2016, US intelligence agencies expressed concerns regarding foreign interference in the US presidential election process. They noted that in the summer of 2016, Russian intelligence agents had perhaps compromised the integrity of the US election process through hacking into voter databases in Illinois and Arizona, as well as making public the contents of e-mails sent by presidential candidate Hillary Clinton and members of the Democratic National Committee (Fritcke, 2016).
- In the United States, many employees who work off-site may have their activities monitored by their employers through GPS tracking in a company vehicle or company-

provided phone. Employees are often monitored not only during working hours, but every time they drive the vehicle or use the phone. Recently, reporter Kaveh Waddell (2017, 1) asked readers to consider the following: "Someone's tracking your phone or has placed a GPS device on your car. They know if you're at home, or a pregnancy clinic, or church, or a gay bar." Currently there is no federal level legislation regarding the rights of employees, and decisions as to what constitutes a violation are often made on a case by case or state by state basis.

- In recent years, the Dutch government has encouraged citizens to engage in what it terms '**participatory surveillance**.' Citizens who find themselves in an emergency situation – such as a natural disaster or terrorist event – are encouraged to use their phones to record videos of the scene, in order to aid law enforcement later in finding the perpetrators. The Dutch government defines participatory surveillance as a logical part of what it terms responsible citizenship (Timan and Albrechtslund, 2015).
- In 2015, a British company developed software (known as Fin Fisher) which could be used to monitor and search internet communications. It sold the software to many government clients, intending that it be used as a weapon in the fight against terrorism. However, it was later revealed that clients like the governments of Belarus and North Korea had purchased the software, not for the purposes of carrying out counterterrorism measures to protect their own citizens, but rather as a way of monitoring the communications of their own citizens to make sure that they were not engaged in dissident or anti-state activities (Wagner and Bronowicka, 2015).

What do these stories show? First, they illustrate that surveillance actually encompasses several different types of activities carried out by a variety of actors – including corporations, nation-states and nonstate actors, as well as private citizens. Surveillance activities may be illegal, legal or in some cases may fall into a grey area where they are poorly regulated and understood. In the United States, legal scholars often use the term '**surveillance**' to refer only to the *unauthorized* collection of personal or professional information, as well as associated activities such as the unauthorized publication or sharing of that information. As we saw in Chapter 4, individuals and groups in the United States are frequently asked to, and agree to provide data to other individuals, groups and the government for a variety of reasons. Individuals may consent to a licensing agreement when they upgrade the software on their phone, or they may agree to participate in a clinical trial of a new medication. Individuals who agree to furnish their personal information to others to see, use and share do so according to a process of informed consent, in which they are informed of their rights to share or not share information, the ways in which their information will be used and their right to change their mind later about the information that they have shared.

Surveillance, however, is often taken to mean the collection of information in the absence of informed consent. Under US law, an entity (such as the government or a corporation) is said to be engaged in electronic surveillance if they are acquiring wire or radio communications – through the use of an electronic, mechanical or other surveillance device. The entity must be

collecting information which was sent by or received by an American who is in the United States – when the individual could have a reasonable expectation of privacy, and where one would normally require a warrant in order to collect this information for law enforcement purposes. It is also considered electronic surveillance if an entity installs a device on your computer or other device in order to collect information – in a circumstance where you could expect to have privacy or where a warrant would be required to collect this information for law enforcement purposes (Chapter 50 of US Criminal Code, Section 1801). US law explains the circumstances under which it is illegal to engage in electronic surveillance and the conditions under which it is legal (such as when one is suspected of plotting to harm the United States, and the proper authorities have given the entity permission to collect this information). This definition assumes that the individual or group which is the subject of surveillance is unaware of the fact that they are being surveilled and that they have not been informed or warned in any way. They have thus not consented to the surveillance.

Wurster distinguishes between **detection from a distance** and **obtrusive detection**. Detection from a distance might include a drone collecting information from the sky, use of a spy satellite or the use of closed circuit television systems (CCTV), which record information and may also engage in specified activities – such as identifying license plate numbers. If we think back to the example of the employee whose employer is using a GPS to track their activities, this is an example of detection from a distance – since the employee is unaware that he's being tracked. In contrast, obtrusive detection may include using a scanner (such as at the airport), biometrics or access control cards. Here the individual knows that his information is being collected and he consents to surveillance.

Next, these stories show that the people and groups being watched might not yet have committed a crime or experienced a negative outcome. Instead, surveillance activities may include using analytics to *preemptively* detect patterns of inquiry or activity which could lead to future harm. Then, an agency can take steps to preempt that negative outcome. Here, **analytics** is defined as "the use of information technology to harness statistics, algorithms and other tools of mathematics to improve decision-making" (Schwartz, 2). We can see how healthcare personnel use analytics in conducting health surveillance. By monitoring disease patterns, public health officials can act preemptively – such as beginning a vaccination campaign – to prevent an epidemic. Today, physicians may conduct health surveillance by having school nurses monitor and report the body mass index (BMI) of elementary school children, in order to identify children at risk of developing obesity and take steps to prevent this outcome (Longjohn et al., 2009).

Third, these stories show that not all surveillance is equally intrusive. They show that one can conduct ethical surveillance – through setting limits on the type of information collected, establishing norms for the storage and sharing of this information, and establishing rules for respecting the rights of those who are the subject of surveillance.

Fourth, these stories show that those who engage in surveillance may have a wide variety of motives for doing so – some of which might be ethically justified, while others cannot. For example, public health officials are protecting citizens' health and security; therefore,

monitoring – even in situations where it might be regarded as intrusive by the subjects – is necessary to provide health security to society as a whole. Similarly, computer scientists use algorithms to monitor employee behavior within an organization in order to predict who is likely to be an **insider threat**. Here, certain types of activities suggest that someone might be a malicious insider – such as patterns where they are accessing data that they have no job-related need for, erasing logs of their attempts to access information, or their use of programs to map internal networks or identify weaknesses in a system (Azaria et al., 2007). In other instances, such as the use of Fin Fisher software by an authoritarian government to identify those opposed to the government, surveillance cannot be justified, as it represents a human rights violation. As Figure 5.1 illustrates, surveillance encompasses a variety of activities carried out for a variety of reasons.

Finally, these stories raise questions regarding the responsibilities of those who produce, provide and use surveillance technologies. To what degree should they be held ethically responsible if others misuse the technologies they have created? In the wake of the 2013 Edward Snowden revelations, analysts asked whether internet sites like Google and Facebook knew that US government agencies were carrying out surveillance of individuals who visited those sites. And in recent years, two nations – Australia and the Netherlands – have objected to the ways in which the US government used information collected through an intelligence sharing agreement. In both cases, the host country's government agency granted the US government the right to collect information (including phone and internet communications) for purposes of combatting global terrorism. However, the US military used information collected in both instances to acquire targeting coordinates to carry out drone strikes.

Actor	*Motive for Surveillance*	*Activity*
Public Health Officials	Provide health and security to society as a whole	Monitoring individual and group health of populations
Citizens	Provide law enforcement with clues and information	Engage in social media surveillance after a significant event
Government	Identify those engaged in anti-government activity	Use software to scan citizens' e-mails and social media posts
Government	Preempt and prevent terrorism against citizens	Use analytics to scan electronic communications
Government	Engage in psychological warfare; Undermine confidence in an adversary's electoral system	Monitor communications of election candidates and their advisors
Corporations	Assure that employees are being productive and using company resources wisely	Monitor activities of employees using GPS technology and electronic surveillance
Government or Corporation	Identify employees most likely to pose an 'insider threat'	Use analytics to identify employees who are disgruntled or actively violating company information access policies

Figure 5.1 Motives for engaging in surveillance

Box 5.1 Going deeper: who is Edward Snowden?

In December 2012, American citizen Edward Snowden made news headlines when he released a large number of classified government documents to the journalist Glenn Greenwald, who worked for the British newspaper, *The Guardian*. Snowden, who is facing charges in the United States for violating the Espionage Act, is estimated to have released between 50,000 and 200,000 US documents, as well as large number of Australian and British documents. Snowden received access to these documents while working as a Central Intelligence Agency contractor, and the documents are predominantly from the US National Security Agency (NSA).

Prior to Snowden's release of documents, American citizens and the international community were unaware of the amount of surveillance which the NSA was engaged in, both in the United States and abroad. Citizens were also unaware of the amount of information which the NSA was collecting and saving. As a result of the Snowden revelations, the US Congress held hearings on the question of surveillance and many citizens have become more conscious of the ways in which their privacy may be at risk.

Snowden has been called both a traitor and a hero. He currently resides in Russia where he was granted political asylum, and is only 33 years old. He has been the recipient of numerous prizes in the areas of human rights and freedom of the press and has been nominated for the Nobel Peace Prize. Some see him as a whistleblower – calling attention to corrupt and dangerous practices at his place of work. However, others believe that he has endangered US national security by calling attention not just to US intelligence collection practices, but also to procedures and methodologies used by these agencies. In doing so, he has arguably made it harder for the United States to defend itself against terrorists, since they quickly abandoned certain practices once these details became known.

Others have questioned security procedures at the intelligence agencies themselves. Snowden was largely self-taught as a computer programmer, did not have a high school diploma and was given unprecedented access to US government computers as he worked on a data migration project. Ironically, Snowden achieved Certified Ethical Hacker qualifications, and may have used these skills in his later unauthorized and illegal exploits.

The US Legal Dictionary (No date) defines **complicity** as "a situation where someone is legally accountable or liable for a criminal offense based upon the behavior of another." Some have suggested that Google and Microsoft were complicit in depriving citizens of their privacy, while Australian and Dutch citizens accused their governments of complicity in carrying out drone strikes – even though all they did was provide information gathered through surveillance. Most ethicists today recognize levels of complicity – depending on how much information the 'helper' had about the activities which the perpetrator was likely to engage in, whether or not there is a power differential between the helper and the perpetrator and what the helper's intent was.

So why did Google cooperate with the US National Security Agency in furnishing information about citizens' Google searches? Were they compelled, did they cooperate freely and were they aware of how the information might be used? The situation which Google faced in 2013 was not unique. Rather, individuals in other professions have already debated what to do in situations where one's work is used in unexpected or unanticipated ways by others. Consider, for example, a biologist who develops a drug or vaccine which he hopes will help mankind. However, the knowledge which he created about a pathogen is later used by another researcher not to make a vaccine, but rather to create a harmful biological weapon.

The term '**dual-use technology**' refers to technologies which have both civilian commercial and military uses. In recent years, the term has been expanded to refer not only to physical items such as biological and chemical materials but also to information, including code. In international law, the **Wassenaar Arrangement** regulates the export of dual use technologies, while in the United States, **export control regimes** put into place by the US Department of Commerce require companies wishing to export dual-use technologies to apply for an export license. Recently, regulators attempted to extend the Wassenaar Arrangement to cover the export of computer code but the effort was unsuccessful.

Surveillance in history

Although the examples which began our discussion are all from the 21st century, surveillance is hardly a new idea. Indeed, as Stoddert points out, most major religions have a concept of a God who watches over his people. Such a God is omniscient, or all-knowing, as well as omnipotent, or all powerful. Stoddert argues that historically, people have been comforted by this notion, counting on their God to provide them with security, as well as justice – believing that their God sees who is behaving unethically and perhaps even intervenes to punish the unjust and reward the just. Thus, we have always had an idea of benevolent surveillance, rather than regarding surveillance as inherently 'creepy.'

In addition, we can trace the field of public health back to the Middle Ages. Throughout the late 1400s into the 1700s, communities collected information or intelligence on the spread of plague in order to prepare and hopefully save their villages from destruction. Officials were appointed to put into place procedures like quarantine zones based on the observation of patterns of disease movement or health surveillance. The goal here was to stop the spread of disease through establishing procedures for monitoring its transmission and lethality.

Finally, we can point to the experiments by Jeremy Bentham, a British social reformer. In the late 1780s, Bentham developed a plan for a prison which he referred to as the 'panopticon'. As McMullan describes the arrangement:

> The basic setup of Bentham's panopticon is this: there is a central tower surrounded by cells. In the central tower is the watchman. In the cells are prisoners… . The tower shines bright light so that the watchman is able to see everyone in the cells. The people in the

> cells, however, aren't able to see the watchman, and therefore have to assume that they are always under observation.
>
> (McMullan, 2015, no pagination)

Here we should remember that Bentham was one of the first utilitarian philosophers. He supported this form of surveillance because it was as an extremely efficient use of resources. One watchman could watch a larger population and again could preempt problems before they occurred, thus conserving resources. Surveillance allowed for the reduction of risk and uncertainty and thus reduced the likelihood of loss or damage. In addition, Bentham argued that, not knowing whether or not they were under surveillance at any given time, the prisoners would begin to self-police their own behavior, thinking twice before engaging in forbidden activities, since they never knew if they were being watched. Self-policing would allow for the expenditure of fewer resources to watch the prisoners.

The legal climate

We can formulate arguments both in favor of and against surveillance. Some of the strongest arguments against surveillance come from the American and international legal communities, which have suggested that surveillance is often illegal and unconstitutional.

Here we should note that government surveillance of citizens – and legal opposition to this surveillance – did not begin with 9/11. The NSA began reading international corporate communications sent by telegram after World War Two, and both the Central Intelligence Agency and the NSA engaged in opening and reading the mail of individuals and groups during this time frame. And as America learned during the McCarthy hearings, US intelligence had also surveilled US citizens (including celebrities) whom it suspected of being Communist agents throughout the 1950s (Donahue, 2012).

In 1975, the US Congress conducted the Church Committee Hearings, looking into what they saw as overreach by the US intelligence community – in the aftermath of the Watergate scandal. (The Watergate scandal concerned activities by the Republican National Committee, which was interested in re-electing Richard Nixon, through collecting information on his opponents by means of illegal wire-tapping of their election headquarters' phones.) The mandate of the intelligence community was to engage in the monitoring of foreign threats – but the Church Committee found that the intelligence community had exceeded its bounds, also monitoring the communications of Americans within the United States, and that it had not been sufficiently attentive to the Constitution and the system of checks and balances described in the Constitution.

These hearings led to the passage of the **Foreign Intelligence Surveillance Act of 1978**. This act spelled out the specific circumstances under which the US government could monitor communications, both of US citizens and of people residing within the United States. It placed the intelligence community's activities under both legislative and judicial oversight. In cases

where an American citizen's communications would be collected, those collecting the information were required to get a warrant issued by a court authorizing the surveillance.

The Foreign Intelligence Surveillance Act was updated and amended several times as technologies and threats facing the United States changed. Beginning in 2007, in response to increasing al Qaeda threats, an amendment known as the **Protect America Act** was added. This amendment allowed the US government to engage in increased surveillance of US persons outside of the United States under certain circumstances. The Amendment established the understanding that a citizen abroad might not have the same expectation of privacy as a citizen has in the US (Bazan, 2008, 10).

Today, legal analysts are attempting to resolve questions of **jurisdiction**, or whose laws should apply, in a globalized world where data storage and access patterns may not always neatly align with geographical boundaries. As Cordero (2015) has pointed out, some nations have very strict laws regarding the situations in which an ISP must be required to provide data to local or national authorities, some have lax laws and some have none at all. She argues that while some people find US laws problematic, the bigger problem is that nations which have no legal framework governing surveillance may still be engaged in surveillance, creating a situation where the citizen has few rights to object or even to know that surveillance is taking place.

Legal analysts also worry about a situation where a French citizen might perform a search using Google which seems suspicious to American authorities. Some analysts would say that the data here is French since the searcher was a French person performing a search on her home computer located in France. However, others might say that the data is American, since it is being housed on a Google server in the United States. The question is thus whose laws would apply. Is the French citizen protected from having to share her data with the NSA, for example, under French law – or does American law supersede French law if the data is American?

Within international law, countries sign **Mutual Legal Assistance Treaties (MLAT)** which allow them to ask each other for assistance in carrying out criminal prosecutions. In the cyber arena, this means that countries can use MLAT's to ask other countries to share data. However, this is a lengthy, bureaucratic process. The United States has argued that in prosecuting cases like terrorism, it takes too long for the other country to get a warrant and carry out the necessary steps in order to provide the data. Thus, in April 2014, a New York district court ruled that Microsoft was obligated to turn over data – even though it was stored in Ireland – because Microsoft was an American corporation, incorporated in the United States under US laws. However, in other Supreme Court cases, the ruling has been that the United States does not have the right to seize property located outside of the United States.

In November 2015, Microsoft unveiled a new plan. Under this plan, foreign users can store their data at a center located in Germany, operated by a German provider. This is referred to as **data localization**. The German provider is referred to as a **data trustee**. This entity then decides who may access the data and under what circumstances, under local laws. As Basu argues, "For this trustee model to work, the country in which the data is being hosted must

have a robust data protection framework within its domestic law" (Basu, 2015, 1). While this solution seems to provide increased privacy rights to users, opponents claim it destroys the flexibility of the internet, where data can and should be duplicated around the world for backup and efficient access. People are afraid that localization will lead to balkanization, or the creation of separate national internets with different rules governing them, and a slowing of the efficiency in which data currently zooms around the world.

Currently, legal analysts disagree about whether different countries should have different standards and laws regarding how much encryption to allow, how much surveillance to allow, and how a nation's government can behave in an extraordinary situation (i.e. whether a national government should be allowed to intervene to shut down the internet if it perceives some form of threat – like terrorism or outside manipulation of an event like a national election). As noted in Chapter 4, different societies may have different understandings of what constitutes an invasion of privacy or improper use of surveillance, with different standards prevailing in different nations and regions. What one nation regards as a reasonable set of precautions in order to preserve citizen rights may seem unduly restrictive to another nation's government, based on national understandings and the kind of threat that they are facing (Saran, 2016a). And as Saran points out, more secure communications are more expensive communications. In mandating the use of only the most current and best technology for securing communications by citizens, he argues that those in the developing world may be left behind or closed out of the communications revolution.

Saran (2016b) thus suggests that rather than focusing on privacy or surveillance, providers should focus on what he terms **data integrity** – ensuring the integrity of citizen data from government intrusion, bad actors including nonstate actors, criminal exploitation and commercial exploitation.

Box 5.2 Going deeper: what was WikiLeaks?

WikiLeaks is an online "media organization" founded in 2006 by Julian Assange, an Australian citizen. The organization first gained international attention in 2010 when it served as the hosting site for the cache of approximately 250,000 US diplomatic cables said to have been illegally provided by US military analyst Bradley Manning. Manning is also believed to have provided an additional 500,000 documents, including classified materials related to US activities in Afghanistan and Iraq.

According to Assange, WikiLeaks serves as a repository for whistleblowers – aimed at maintaining freedom of the press and ensuring that governments will always operate in a transparent fashion, sharing information with citizens rather than acting without their knowledge. WikiLeaks maintains a secure drop box where individuals can upload information which is untraceable.

Over the years, WikiLeaks has hosted material about a great many issues – from the Trans Pacific Pipeline, to the detention of prisoners at the US military facility in

Guantanamo Bay, Cuba. WikiLeaks is regarded as both transnational – hosting material from many nations – and nonpartisan. It has released information which is damaging to individuals and groups from all sides of the political spectrum. It again achieved media attention in fall 2016, during the US election cycle, when it published a series of e-mails from Democratic presidential candidate Hillary Clinton, as well as from members of the Democratic National Committee.

Legal status

While Assange sees his mission as ethical, many national governments regard his activities as both unethical and unlawful. After the initial release of diplomatic cables in 2010, the US government announced plans to prosecute Assange under the 1917 Espionage Act. They argued that the release of these diplomatic cables was harmful to US national security and that WikiLeaks had willfully disclosed information that they knew would endanger US national security interests and US citizens (Bellinger, 2010). In the United States, violators of the Espionage Act could face the death penalty (BBC, 2015).

Assange is also wanted on criminal charges in Sweden, his former home – as it is alleged that he committed both rape and sexual assault there.

Assange currently resides in the Ecuadorian Embassy in London, where he has been granted asylum on human rights grounds, since he claims that he could be sentenced to death if he were extradited to the United States.

The server which hosts WikiLeaks has been moved several times to different nations, as many nations have engaged in judicial proceedings regarding the legality of WikiLeaks and the legality of hosting WikiLeaks. WikiLeaks has also been the target of cyberattacks during its history, including DDos attacks.

Status of WikiLeaks as a journalistic source

WikiLeaks has also been the target of criticism for its decision not to curate content or edit it in any way. At one point, WikiLeaks included documents which had people's social security numbers in them. For this reason, there is also a controversy about the fact that legitimate broadcast networks have used content from WikiLeaks. Critics have asked whether this is responsible journalism by these organizations, and whether WikiLeaks should actually be classified as a media source – since it has a political agenda and does not strive to be neutral (even if that agenda is merely to create greater transparency). It also does not abide by many journalistic ethics and norms, such as protecting sources.

The organization is run largely by volunteers and financed by donations.

How WikiLeaks protects itself and its information

Because Assange is concerned that at some point he might be extradited to face prosecution in either the United States or Sweden, he has adopted a system of 'insurance' that is aimed at preempting any attempts to shut down WikiLeaks. From time to time, WikiLeaks sends out files of particularly damaging information to torrent sites. The information is encrypted and those that hold it can't read it – though they can use a hash number to check that the information they have has not been corrupted or tampered with in some way. However, should something happen to Assange, there are plans to automatically send out a key (via a Deadman's switch) which would make the information readable, so that WikiLeaks' supporters could share the information (Swearingen, 2016).

Sources

BBC News. 2015. "Q and A: Julian Assange and the Law." March 13. Available at www.bbc.com/news/world-europe-19426382. Accessed March 1, 2017.

Bellinger, John. 2010. "The Legal Case Against WikiLeaks." *Council on Foreign Relations*. December 13. Available at www.cfr.org/media-and-foreign-policy/legal-case-against-wikileaks/p23618. Accessed March 12, 2017.

Swearingen, Jake. 2016. "Something Weird (or Weirder Than Normal) Is Happening at WikiLeaks." *New York Magazine*. November 16. Available at http://nymag.com/selectall/2016/11/wikileak-hashes-dont-match-so-whats-going-on.html. Accessed March 3, 2017.

Zittrain, Jonathan, and Sauter, Molly. 2010. "Everything You Need to Know About WikiLeaks." *Technology Review*. December 9. Available at www.tedchnologyreview.com/s/42/everything-you-need-to. Accessed January 20, 2017.

Ethical critiques of surveillance

In addition to legal critiques and challenges in the area of surveillance, we can identify ethical critiques. As Buff (2013), has argued, data itself is neutral. However, the use of data is not ethically neutral. Managers and technicians who work in the field of surveillance make and carry out ethical decisions regarding what data to collect, store, distribute and use. They may do so based on a strong ethical code which emphasizes respect for the targets of surveillance, but there also exists the potential for abuse by those who engage in surveillance or watching.

The most common ethical criticisms of surveillance focus on the ways in which it establishes **power asymmetries** between the watcher and the watched; the ability of surveillance regimes to create an atmosphere of suspicion and mistrust in which people may either have their rights to freedom of speech and assembly curtailed, and actively engage in measures in which they curtail their own rights to these goods; and the fact that surveillance is often applied differentially, with those who are most disenfranchised in society often becoming the subject of greater surveillance. As Michael and Michael write:

> The incongruity behind traditional surveillance technologies is that, generally, individuals of power and influence are not subjected to the extreme and exaggerated types of surveillance techniques designed and planned for everyone else.
>
> (15)

As the example of Bentham's panopticon showed, surveillance technologies automatically set up a power asymmetry in which the watchers have a great deal of power and the watched have very little. In such a situation, the watcher could easily abuse his power. Indeed, watching often conveys a sense of ownership over the subject and the subject's body. An abusive husband might hire a detective to watch his wife; pregnant women may find that strangers pay attention to whether they are smoking or drinking alcohol; celebrities may find that the general population pays attention to whether they are pregnant or merely getting fat. In countries with strict population policies, government agents have historically watched women to be sure that they were not planning to abort a pregnancy (in Romania) or to have a second child (in China).

Box 5.3 Application: what is cyberstalking?

A recent study suggests that as many as one in ten individuals in Great Britain have been victims of cyberstalking. Women are twice as likely to be cyberstalked (Horsman and Conniss, 2015). But what is cyberstalking, why does it occur and what is being done to stop it?

The US Department of Justice defines **stalking** as "a course of conduct directed at a specific person that involves repeated visual or physical proximity, non-consensual communication, or verbal or implied threats or a combination thereof that would cause a reasonable person to fear" (Tjaden and Thoennes, 1998). Merritt (2015) defines **cyberstalking** as "the use of technology, particularly the internet, to harass someone." She notes that "communication characteristics include false accusations, monitoring, threats, and identity theft and data destruction of manipulation. Cyberstalking also includes exploitation of minors, be it sexual or otherwise."

For Merritt, the chief characteristic of cyberstalking is that it is unwanted. The person who is being monitored does not want to be the subject of this surveillance and has likely asked the watcher to stop. In addition, the relationship is asymmetric. It is not one of mutual surveillance but is rather imposed by one party upon another. It also has a repeated character, and is not benevolent surveillance aimed at keeping the person safe, but rather is likely malevolent, aimed at injuring the surveilled individual emotionally or psychologically as well as perhaps physically.

Cyberstalking involves acts intended to "kill, injure, harass or cause substantial emotional distress to another, using any interactive computer" (United States Department of Justice. United States Criminal Code 18, section 2261A "The Federal Interstate Stalking Punishment and Prevention Act," as quoted in Shimizu, 2013, 126.

Cyberharassment refers to "repeated threatening or harassing e-mail messages, instant messages, blog entries or websites dedicated solely to tormenting an individual" (Cox, 2014, 277).

Most criminologists do not see any of these crimes as new types of criminal behavior; instead, they emphasize that traditional crimes like stalking and harassment have become easier with the advent of technology. Today, a stalker may use GPS technology to track his victim or conduct a search on a site like Spokeo in order to get more information about his victim, such as her home address. They also note that it has become harder for the police to catch harassers since these criminals can now use online services to send spoof or anonymized SMS messages, as well as using services like Tor to cover their tracks (Horsman and Conniss, 2015).

Currently, cyberstalking is prohibited by both US federal and state laws. Specific legislation has been written to address the crime of cyberstalking, and existing legislation regarding telephone harassment and traditional stalking has also been extended to cover cyberstalking as well. US lawmakers are also considering legislation which would outlaw the practice of sending spoofed messages through websites designed for this purpose.

Sources

Cox, Cassie. 2014. "Protecting Victims of Cyberstalking, Cyberharassment and Online Impersonation Through Prosecutions and Effective Laws." *Jurimetric: The Journal of Law, Science and Technology* 54(30): 277–302.

Horsman, Graeme, and Conniss, Lynne. 2015. "An Investigation Into Anonymous and Spoof SMS Resources Used for the Purposes of Cyberstalking." *Digital Investigation: The International Journal of Digital Forensics & Incident Response* 13: 80–93.

Merritt, Marian. 2013. "Straight Talk About Cyberstalking." *Norton.com*. July 1. Available at http://us.norton.com/cyberstalking/article. Accessed March 12, 2017.

"Straight Talk About Cyberstalking." Available at http://us.norton.com/cyberstalking/article. Accessed July 1, 2013.

Shimizu, Aily. 2013. "Domestic Violence in the Digital Age: Towards the Creation of a Comprehensive Cyberstalking Statute." *Berkeley Journal of Law, Gender and Justice* 28(1). Available at http://scholarship.law.berkeley.edu/bglj/vol28/iss1/4. Accessed March 12, 2017.

Tjaden, Patricia and Thoennes, Nancy. 1998. "Stalking in America: Findings From the National Violence Against Women Survey." *National Institute of Justice 2.* Available at www.ncjrs.gov/pdffiles/169592.pdf Quoted in Shimizu, 2013, 117.

United States Department of Justice. United States Criminal Code 18, section 2261A "The Federal Interstate Stalking Punishment and Prevention Act." Quoted in Shimizu, 2013, 126.

While there are laws governing surveillance, there is no mechanism that assures that the watchers behave ethically 100 percent of the time and do not misuse this power, nor any requirement that the watchers treat those they watch with respect and empathy. Thus, critics often ask "Who watches the watchers?" (Schneier, 2006).

At the same time, analysts worry that surveillance technologies will automatically lead to an expansion of state power. In his work, Mark Neocleos (2003, 13) quotes the American reformer Ben Franklin, who famously stated that "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." Individuals who support a limited role for government in society therefore may be more suspicious of the benefits of surveillance and more attuned to its risks.

Here, Michael and Michael (2011) argue that surveillance often reduces questions to stark black and white terms. They argue that often leaders are neither 100 percent honest and scrupulous, nor 100 percent dishonest and unscrupulous. Thus, they worry about a situation where any evidence of wrongdoing might be used to eliminate someone from consideration for a position of leadership. They write "Had the private lives of colossal and 'untouchable' figures such as John F. Kennedy and Martin Luther King been subjected to never-ended surveillance, how might that not only have affected the biography of these two men, but changed the course of history itself?" (13). Still others have noted that oftentimes, when a social norm is changing, some types of 'grey area' behaviors might be tolerated in the margins, before a consensus develops that such behavior is acceptable, and it is then allowed to become mainstream. For example, one can argue that in the period before homosexuality was decriminalized in the United States, there was a period where it was tolerated at the margins, if not publicized. These analysts worry that in an area where every activity and every decision is a matter of public record, it might be harder for norms related to tolerance of activities like inter-racial or same-sex marriage to become established and changed, since individuals who might pioneer a norm would instead likely be arrested.

In considering power asymmetries, we can also consider the question of equity and the ways in which those who have better access to information could manipulate that situation to their advantage. Perlforth (2014) describes a situation which occurred on Wall Street when a group of former Morgan Stanley employees worked together to engage in unauthorized surveillance of company files. They used their access to gain insider information about a number of companies, which they then used to commit securities fraud. In her analysis, Scheppele argues that though the employees did not actually steal from their former employer, they committed an ethics breach through violating the principle of fairness. She argues "the hack was against the company but the crime was actually against other investors" who did not have access to the same information in making their own investment decisions (Scheppele, 1993, 125). Koene et al. also raise equity concerns, noting that:

> We can foresee a situation where employers can simply use profiles to predict who would be the best employee and no longer feel compelled to publicize job openings, give individuals the opportunity to apply for jobs or allow people to interview for jobs.
>
> (Koene et al., 2015, 170)

Surveillance vs. "spying": the problem of transparency

In thinking about surveillance, it is also important to consider the value of **transparency**. The principle of transparency as understood in a democratic society means that citizens have a right to know what their government is doing – the activities it is engaged in, and the money that it spends. Transparency is seen as a key element in providing **accountability**, or of making governments (and corporations) accountable to people – their constituents or their clients. Transparency is thus seen as a very powerful way of combatting corruption or secrecy within government. Turilli and Floridi (2009, 107) describe information transparency as "enabling" other values including accountability, safety, welfare and informed consent. Companies need to disclose problems with their products in order to keep their users safe, and governments need to disclose information about their activities because they are accountable to citizens. They argue that governments do not have a right to keep secrets from citizens – except in dire situations such as a wartime situation where it might be dangerous to share information too widely. Furthermore, governments should act with the consent of the people, and people cannot consent – or object – to something (like surveillance) when they are unaware that it is taking place.

The ethical value which Edward Snowden was defending then in objecting to surveillance was transparency. In speaking to the British media in 2013 about the National Security Agency's surveillance program, he expressed concern that the government was undertaking surveillance of citizens without their awareness or their consent. Furthermore, he expressed concern that the government was not disclosing information to citizens about these activities because they were aware that such actions were illegal and unconstitutional.

Today, similar ethical concerns have been raised regarding the use of big data analytics. Turilli and Floridi (2009) describe the obligation of a company to inform users of a software package, for example, of what information about them and their use might be compiled as a result of their using the product, as well as the circumstances under which this information might be disclosed or shared and to whom.

Suspicion and distrust

Other analysts ask what it does to people's sense of identity when they know that they are being watched, and even begin to alter their behavior in response to this knowledge (Vaz and Bruno, 2003). Individuals who know that they are the subject of surveillance can be said to have less freedom than others in society. They may also begin to think differently about themselves, no longer engaging in processes of self-expression and self-discovery, but rather

being careful of how they and their behaviors are perceived – since their own government may regard them not as innocent but rather as potentially disloyal. In a surveillance society, people may feel that they have a responsibility to monitor their own behavior to avoid becoming a subject of suspicion.

The American Library Association has, for this reason, spoken out against unwarranted government surveillance, arguing that patrons should have the right to search for information without worrying about whether their searches will arouse suspicion. The American Library Association Code of Ethics (2008) states that "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted."

Differential surveillance

Critics also suggest that not everyone in society is equally likely to be the subject of surveillance. In the United States, many African-American citizens refer to a phenomenon known as 'driving while black,' pointing out that an African-American driver is stopped more often by the police, even when he has not broken any traffic rules. He is simply watched more closely because of his minority status in society. Those who receive government assistance sometimes note that when they shop at a grocery store, other customers may examine the contents of their shopping carts, wanting to make sure that tax dollars are not being wasted on frivolous food purchases.

Here, analysts argue that while surveillance claims to produce a collective good (such as security), not everyone actually pays the same for this collective good. For example, the Japanese-Americans who were interned during World War Two paid more than other Americans did to preserve security. They were defined as potentially disloyal Americans, they sustained economic losses and lost employment opportunities, as well as being separated from friends and family (Gillion, 2011). Further, one may argue that there is a mismatch between the individuals who probably should be most closely watched and those who in fact are. Those who have strong reasons to evade surveillance (such as those engaging in terrorist or criminal activities) may also have resources which will enable them to do so (such as access to anonymous browsing software). Conversely, those who have the fewest means to evade surveillance may become the target of increasing surveillance.

Use of resources: is surveillance wasteful?

Finally, today some critics are beginning to question the amounts of money, manpower and resources which the United States in particular devotes to engaging in surveillance. They wonder if given the relative infrequency of terrorist events, such resources couldn't be better spent on other activities of American civic life. In addition, one might ask whether a company should devote so many resources to identifying disgruntled company insiders, and whether those resources might be better spent actually learning what employees want and need, implementing programs that might keep them from becoming disgruntled.

Box 5.4 Critical issues: what is Bitcoin?

Bitcoin is a fundamentally new type of currency which presents some fundamentally new problems. In 2013, Nobel prize-winning economist Paul Krugman called Bitcoin "evil." But what does he mean by this and is it an accurate characterization? As we think about the government's ability to monitor individual and corporate activities online, it is helpful to understand what a cryptocurrency is, and why it matters when it comes to surveillance.

Currency is a medium of exchange which enables us to buy, sell, invest and trade with our neighbors. Dollars or another currency substitute for the goods themselves, enabling us to carry out complex financial transactions without actually exchanging physical objects. With traditional currencies, money is issued by a government-owned mint which is the subject of **national fiscal or monetary policy**. Policymakers regulate the market through establishing economic conditions – such as setting interest rates and deciding how much currency can be in circulation. These conditions then affect the currency's **exchange rate** (how much a particular currency is traded for relative to other currencies on the world market) and the currency's purchasing power. Banks serve as intermediaries – storing, clearing and helping to transfer currency from place to place. It is the actions of governments and banks which allow individuals and corporations to make both long-term and short-term investments both domestically and internationally, since everyone involved in the system trusts or relies on the government and banks to keep these values relatively stable.

In contrast, Bitcoin is not issued by a central bank or a government but is rather a type of **peer to peer lending medium**. Individuals allow their computer systems to serve as 'banks' and the currency does not have a fixed rate determined by a government or a central bank. A mathematical algorithm sets the currency's price, shifting the exchange rate depending on how many are purchased and in circulation. Exchanges are recorded in a **block chain** which serves as a public ledger of all transactions. This ledger is transferred with the currency every time it moves within the system.

Ethical issues presented by Bitcoin

There are two major issues which we can identify with Bitcoin:

First, **bitcoin transactions are not monitored or regulated by any government**. Traditionally, when people engage in international financial transactions like lending or donating money or exporting products or services, they have been subject to many government regulations. These transactions are regulated by export regimes, tax regulations and duties and tariffs. Regulations ensure that exports and imports meet safety standards

> and that the rights of all parties are respected. Financial transactions which seem suspicious are reported to national counterterrorism agencies.

In contrast, groups can use Bitcoin to carry out transactions without national or international government regulations. Bitcoin is referred to as a **cryptocoin or cryptocurrency** (Surowicki, 2011) since this is the equivalent of carrying out encrypted transactions. Many analysts suggest that Bitcoins are used predominantly for illicit or illegal purposes – including tax evasion, money laundering and drug trafficking or terrorist financing (Georgetown University, 2015; Baker, 1985; Stross, 2013). A Pentagon report notes that "The introduction of virtual currency will likely shape threat finance by increasing the opaqueness, transactional velocity and overall efficiencies of terrorist attacks" (Fung, 2014). Bitcoins might be used to violate export regimes, to evade taxation or to trade in shoddy or substandard goods. Chevinsky worries that consumers may lose out if government is unable to intervene to ensure that products meet standards of consumer safety.

The second ethical issue is equity. Surowicki argues that unregulated currency is more likely to be used for speculation than genuine trade. He worries that individuals will hoard the currency and argues that Bitcoin doesn't act like a regular currency which is a medium of exchange among a community. Stross worries that cryptocurrencies will compete with legitimate currencies, ultimately winning. He argues that if Bitcoins become the norm, this will affect the ability of governments to carry out legitimate financial transactions such as distributing pensions.

Should Bitcoin be outlawed?

Enthusiasm for Bitcoin varies worldwide. Chinese investors are keen on Bitcoin due to concerns about the volatility of their own currency on the world market. However, Russian legislators are considering legislation which would impose fines for engaging in unregulated financial transactions and using unofficial currency (US Government Printing Office, 2013). Economist Lawrence Kotlikoff has proposed limiting the purposes for which "neobanks" could be established, making some purposes legal while others are not (Hayat, 2017).

However, other analysts see an upside to Bitcoin. Angel and McCabe (2015) argue that Bitcoin is merely a tool or technology, and that in and of itself, it is neither evil nor good. He compares it to the painkiller OxyContin which can provide pain relief for ill people but is also subject to abuse by others. He notes that Bitcoin can help consumers to more cheaply send money abroad to relatives through remittances, and can save them from having to pay high fees to credit card companies. Bitcoins could also be used to pay people who were too poor or marginalized to have bank accounts.

More recently, analysts have begun to suggest that Bitcoin's reliance on block chain technology means that the increased use of cryptocurrencies could actually increase

financial transparency within the financial system. Digital forensics may allow using block chains to trace financial transactions and to look for patterns. For this reason, in the United States, many states are considering new legislation which would make it possible to subpoena block chains for use as evidence in law enforcement proceedings.

Sources

Baker, Ashley Nicole. 2016. "If You Build the Blockchain, Regulators Will Come." *Freedomworks.org*. July 12. Available at www.freedomworks.org/content/if-you-build-blockchain-regulators-will-come. Accessed March 2, 2017.

Chevinsky, Jennifer. 2013. "Doctor, a Bitcoin for Your Two-Cents?" *Bioethics.net*. May 23. Available at www.bioethics.net/2013/05/doctor-a-bitcoin-for-your-two-cents/. Accessed March 12, 2017.

Fung, Brian. 2014. "The Military Thinks Bitcoin Could Pose a Threat to National Security." *Washington Post*. May 6. Available at www.washingtonpost.com/news/the-switch/wp/2014/05/06/the-military-thinks-bitcoin-could-pose-a-threat-to-national-security/?utm_term=.2d8ff1d77770. Accessed March 12, 2017.

Georgetown University School of Business. 2015. "The Ethics of Bitcoin." January 30, 2015. Available at http://msb.georgetown.edu/newsroom/news/ethics-bitcoin. Accessed March 1, 2017.

Hayat, Usman. 2017. "Limited-Purpose Banking: Can It Fix the Financial System?" *Enterprising Investor*. July 12. Available at https://blogs.cfainstitute.org/investor/2011/07/12/limited-purpose-banking-can-it-fix-the-financial-system/. Accessed March 12, 2017.

Stross, Charlie. 2013. "Why I Want Bitcoin to Die in a Fire." *Charlie's Diary*. December 18. Available at www.antipope.org/charlie/blog-static/2013/12/why-i-want-bitcoin-to-die-in-a.html. Accessed March 1, 2017.

Surowicki, James. 2011. "Cryptocurrency." *MIT Technology Review*. August 23. Available at www.technologyreview.com/s/425142/cryptocurrency/. Accessed March 12, 2017.

United States Government Printing Office. 2013. "Beyond Silk Road: Potential Risks, Threats and Promises of Virtual Currency." Hearing Before the Committee on Homeland Security and Governmental Affairs, United States Senate. November 13, 2013. Available at www.gpo.gov/fdsys/pkg/CHRG-113shrg86636/pdf/CHRG-113shrg86636.pdf. Accessed March 1, 2017.

Do we have a right not to be surveilled?

In the aftermath of the Snowden revelations, several governmental bodies in the United States, in Europe and internationally spoke out against the phenomenon of unauthorized mass surveillance. In December 2013, the United Nations General Assembly suggested that the ability of governments to carry out large-scale surveillance could have an impact on human rights. The US Privacy and Civil Liberties Oversight Board described NSA surveillance as a violation of the Electronic Communications Privacy Act, and possibly of the First and Fourth Amendments. The European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee) cautioned that even in a situation where the monitoring seemed justified – such as in a fight against terrorism – there was no justification for "untargeted, secret and sometimes even illegal mass surveillance programmes" (2014, 16–17).

An Amnesty International report, entitled "Two Years after Snowden," (2015, 8) also noted that 71 percent of respondents to a fifteen-nation poll about surveillance were strongly opposed to government's spying on their citizens. Here, they note that citizens may differ in the degree to which they oppose surveillance, reflecting different national norms, nonetheless, no country voiced overwhelming support for such practices.

In 2016, the European Community adopted the **European Data Privacy Directive**, which will become a regulation or law in 2018. This regulation states that European citizens do have a right to data privacy, and that their data can only be collected under specific conditions, and for a legitimate purpose (i.e. city planning vs. prurient curiosity). The directive spells out the specific ways in which EU businesses and government entities must protect and store user data, and the conditions under which it can be shared (Hawthorne, 2015). The directive includes very specific conditions for the transfer of EU citizens' personal data outside the European Union, such as to the United States (European Commission, 2016). In situations where citizens feel that their data privacy has been breached, they may claim financial compensation. They can also demand that their data be erased.

Encryption as a response to surveillance

One way in which users have responded to the threat of unauthorized surveillance (by one's own government or by malicious actors) is through the development of strong encryption technologies.

Encryption is defined as "the process of using an algorithm to transform information to make it unreadable for unauthorized users" (Techopedia, No date, no pagination). Encryption is a technology, and it is neutral. It is not necessarily unethical; indeed, we can make many strong arguments for and against the use of encryption technologies. Some analysts compare it to using an envelope in exchanging written communications. Using an envelope is not unethical, though one could certainly enclose illegal *or* unethical content within an envelope.

On the positive side, encryption creates a more secure system which allows for the building of trust and cooperation between users. Our personal information – like a credit card number – is encrypted when it travels over the internet as we conduct activities like online shopping. Encryption assures that only authorized users who have a key are able to access the data and read it. Thus, encryption preserves people's privacy and provides confidentiality. Encryption also provides **authentication**. Through the use of keys, everyone engaged in a transaction is assured that the people with whom they are interacting are who they say they are. Encryption also provides **nonrepudiation**, by providing proof of which party sent a message and who received it. It also contains time-date stamping, thus providing proof of when the message was created, sent and received (Roberts, No date).

While encryption protects lawful users' information, it can also be used by unlawful users. **Ransomware** crimes are crimes in which individuals are contacted and told that they have downloaded a piece of malware which will encrypt all of their data unless they pay a fee to the

'kidnapper.' who then provides the key to decrypt the data. If victims do not pay by a certain date, their data can be destroyed. To date, many types of entities – including hospitals – have been the victims of ransomware, with innocent medical patients the victims if their data is lost. Encryption technologies may also be used by groups like terrorists, in order to pass secure communications within a network without observation or monitoring by law enforcement.

Roberts notes that encryption is legal when it is used within US borders. However, encryption technologies can also be regarded as munitions or weapons, and are thus subject to export controls (No date).

Roberts writes:

> Government security specialists fear that the widespread use of encryption could protect information involving criminal activities such as terrorism or drug trafficking. The government thus restricts the export of all sophisticated cryptography in the interests of national security.
>
> (No date, http://cs.stanford.edu/people/eroberts/courses/cs181/projects/public-key-encryption/ee.html)

Roberts also notes: "Industry also has a vested interest in limiting encryption. Companies fear that disgruntled employees could encrypt corporate databases and throw away the key or hold them hostage" (Roberts, No date).

In the United States and internationally, norms of encryption are still evolving and nations have adopted vastly differently policies regarding what level of encryption is regarded as legal. In 2016, Great Britain passed the **Investigatory Powers Bill**. This legislation grants authority to the government for bulk collection, lawful hacking and allows the government to order the removal of electronic protection (encryption) applied by an operator to any communications or data. The legislation was seen as creating the authority for the government to require a '**back door**' which would allow them to bypass any encryption. And in the aftermath of the 2016 terror attacks in France, the government declared a state of emergency, simultaneously passing legislation which would fine technology companies that refused to decrypt message for law enforcement. However, within the European Union, both The Netherlands and Germany strongly support strong encryption and grant only limited powers to the government to force decryption. In December 2015, China passed an anti-terrorism law which requires telecommunications companies and internet service providers to provide technical interfaces, decryption and other services to state security. In India, the government has attempted to pass laws banning certain forms of end-to-end encryption, including the WhatsApp application, often used for communications by both legitimate and illegitimate actors (Digital Frontiers, 2016). However, these proposed laws were withdrawn from consideration in 2015 due to the actions of Indian civil rights groups.

Despite limited support for back doors and government control over encryption in many nations, in 2016 the United Nations High Commissioner for Human Rights stated that encryption and anonymity help to enable human freedom of expression and opinion and the

right to privacy. Thus, the United Nations has indicated that they strongly support the widespread availability of encryption technologies to citizens (US House of Representatives, Homeland Security Committee Staff Majority Report, 2016).

Box 5.5 Critical issues: the ethics of cyberliability insurance

What's wrong with insuring yourself or your business against losses that might arise from a data breach, hack attack or the actions of a disgruntled employee? People and organizations have been able to buy **cyberliability insurance cover** (CLIC) since 2006.

Today, law firms, hospitals and financial investment firms are all responsible for millions of pieces of client data and businesses depend on their ability to keep this information safe and confidential (Zureich and Graebe, 2015). Currently 46 of 50 American states have **mandatory data breach notification laws** which require firms to let clients know if their data has been compromised, thus opening up the possibility of lawsuits or legal damages if this occurs. Protecting client data is both a financial imperative and also an ethical responsibility for individuals in many professions, including the law and medical professions. A lawyer who fails to protect a client's data could be disbarred or lose his license to practice law (Zureich and Graebe, 2015). CLIC thus provides protection for individuals and corporations who might be sued by clients for activities which put their data at risk. CLIC can also help corporations fund the costs of other penalties which a firm might encounter as a result of a data breach – such as the costs of notifying clients or replacing software and infrastructure which has been damaged (NASW Assurance Services, 2014).

What does insurance do?

An insurance contract is essentially an agreement between a policy holder, the corporation and other policy holders to share in the risks associated with a particular activity. Everyone pays into a common account and an individual who suffers an incident can collect some of the proceeds from that pool. If we consider the example of individuals purchasing insurance against flood damage to their homes, we can see that not everyone experiences the same level of risk (some individuals may live higher above sea level or farther away from waterways). Thus, individuals are grouped into pools and they pay different prices for the insurance depending on the likelihood that they might someday experience an incident and collect from the pool. Most policy holders will never collect from a policy since they will not suffer an incident. However, in the event that they do, they would receive proceeds collected not only from themselves but from all others in

their risk pool. In the case of cyberliability insurance, policies are written to ensure a corporation against a data breach, as well as to ensure specific individuals in the event that their actions are seen to have caused a data breach.

The problem of moral hazard

The most common ethical critique against insurance relates to the idea of moral hazard. **Moral hazard** is a short-hand term for the phenomenon in which people who are insured behave differently than those who are not. They see themselves as able to take on greater levels of risk since the weight of these risks will never fall merely on them but rather on the entire pool of users. In this way, they feel free to engage in riskier behaviors since they will not bear the full consequences of their individual decisions. They have less incentive to behave with restraint.

Many analysts blame the 2008 Financial Meltdown in the United States on moral hazard. They note that many banks made subprime home loans to individuals without fully investigating whether these individuals were a good credit risk and whether they would be able to pay back the loans. Because the banks knew that the US government would bail them out if the loans became worthless, they took on more risk than they might otherwise have done (Mintz, 2010; Claasen, 2015).

Cyberliability and moral hazard

Thus, one danger that might arise from cyberliability insurance is the possibility that corporations might become sloppy about ensuring that their data is protected, since they would be less likely to bear the full costs of any possible data breach. One way for insurance companies to protect against moral hazard is to draft very specific guidelines regarding the types of incidents and damages covered by this insurance. For example, a policy might stipulate that damages would not be paid if the damages were caused by the actions of a disgruntled employee. This stipulation would decrease a corporation's incentives to pay less attention to vetting their employees as a result of purchasing liability insurance. A policy might also stipulate that corporations need to implement specific protocols for encrypting data as a requirement for obtaining the insurance.

Here a utilitarian might argue that even with the possibility of moral hazard arising, cyberliability insurance serves a greater good – since without it, many smaller firms might be unable to practice since they would not be able to survive if they were to experience a data breach or cyberattack and they had to bear all the costs of that attack themselves. Thus, cyberliability insurance helps to assure a free market through making it possible for all sorts of businesses – both larger and small – to function in today's markets which depend heavily upon the cyber arena.

Sources

Claasen, Rutger. 2015. "Financial Crisis and the Ethics of Moral Hazard." *Social Theory and Practice* 41(3): 527–551.

Mintz, Steven. 2010. "Moral Hazard and Ethical Relativism." *Ethicssage.com*. October 3. Available at www.ethicssage.com/2010/10/moral-hazard-and-ethical-relativism. Accessed February 1, 2017.

NASW Assurance Services. 2014. "What Is Cyber Liability?" June. Available at www.naswassurance.org/malpractice/malpractice-tips/cyber-liability. Accessed September 12, 2016.

Sembhi, Sarb. 2013. "An Introduction to Cyber Liability Insurance Cover." *Computerweekly.com*. July. Available at www.computerweekly.com/news/22402703/An-introduction. Accessed January 15, 2017.

Zureich, Dan, and Graebe, William. 2015. "Cybersecurity: The Continuing Evolution of Insurance and Ethics." *Defense Counsel Journal*. April. Available at www.questia.com/library/journal/1G1-413336360/cybersecurity-the-continuing-evolution-of-insurance. Accessed October 2, 2016.

Establishing conditions for ethical surveillance

As we have seen thus far in the chapter, one can make ethical arguments both for and against the technologies of surveillance. In the remainder of this chapter, we will consider the virtue ethics, utilitarian and deontological arguments for and against surveillance. We will also lay out the difference between 'good' and 'bad' surveillance, and the conditions under which surveillance might be considered ethical.

The deontological lens

As noted in Chapter 2, the deontological approach to ethics rests on the assumption that it is inappropriate to treat individuals merely as a means to an end, rather than as an end in themselves. In this approach, the highest value should be on maintaining the dignity and happiness of individuals.

In considering the ethics of surveillance, then, a deontologist would ask: How might a computer user feel if he or she found out that their data was being collected and analyzed? How likely is it that doing so would cause the user to feel harm or embarrassment?

In this approach, any long-term payoff that might come from examining a user's data without their knowledge or consent would be irrelevant – if it was felt that the users were somehow harmed or made to feel uncomfortable through the use of surveillance. In her work, Landau (2016) describes an experiment which researchers carried out in relation to earlier diagnoses of pancreatic cancer. She writes:

> Medical and computer science researchers discovered they could anticipate queries concerning diagnosis of pancreatic cancer based on earlier Bing search queries… . Pancreatic cancer is very hard to treat because it presents late – so this work is intriguing. Could you advise that people go to the doctor based on their queries? Could this lead to earlier diagnosis? Early treatment?

(2016, no pagination)

She concludes that although some lives might be saved as a result of the creation of analytics which linked people's symptom queries to specific diseases, the research was nonetheless unethical. She argues that the targets of the research would likely feel that their privacy had been invaded if they became aware that their private medical searches were being tracked and analyzed. She notes that in this situation no one had volunteered for the study, nor were they informed that it was being conducted.

Schwartz argues that even in a situation where a company might legally carry out a specific action, such as collecting and analyzing data, ethically it might still be suspect. He writes that "a company should use analytics through accountable processes. Accountability begins with an acknowledgement that analytics can have a negative as well as a beneficial impact on individuals" (2010, 3). He describes patterns in which a company engages in surveillance without a citizen's authorization or consent as a violation of trust, and warns that ultimately such violations can destroy the relationship between an individual and the entity engaged in surveillance – whether it is a company or the government. Schwartz argues that corporations who wish to engage ethically with consumers need to ask a series of questions, including: what information is my company collecting, about who and for what purposes? They also need to ask: with whom is it shared and what might be the potential ramifications of the collection of this data on users of my system? What might be the potential ramifications if this data is leaked or shared?

In considering who is most often affected by surveillance, we can also reference the work of John Rawls, introduced in Chapter 2. Rawls suggested that in making an ethical decision, the decider should don the 'veil of ignorance' such that he did not know which participant in the scenario he might ultimately be. Then, he should make the decision in the way that the least powerful participants would not be disadvantaged by the decision, and that if there were any gains from the decision, these gains should favor the least powerful member. In applying Rawls' theory of justice to the question of surveillance, we would identify with the individual who was most marginalized in society and thus perhaps most likely to be the subject of surveillance. How might I think about the utility and need for surveillance if I were an Arab-American, a Japanese-American whose ancestors had been interned or an African-American man or woman who was already the subject of differential surveillance? What limits might I want to see on the government's ability to carry out surveillance and what conditions might I place on that surveillance?

Utilitarian ethics

As noted in Chapter 2, utilitarian ethical frameworks offer the greatest flexibility in the sense that the right thing to do might vary according to the environment or circumstances. That is, utilitarian ethics allows for the possibility of situational ethics – or the idea that a choice that would seem ethically wrong in one situation might not be so in another.

The most common justification given by the US government for its increasing surveillance practices is that ever since 9/11 the United States has found itself in a highly unusual situation. Since the United States currently has many enemies which wish to harm the country and its citizens, the argument goes, we should thus consider the sorts of ethics which would be appropriate during wartime. According to this argument, during peacetime, for example, the role of government might be 'reined in,' but during a time of grave danger to America's citizens, people might be more willing to give their government more powers to watch its citizens and their activities. Here, analysts point to the US Patriot Act, a piece of legislation which was passed in the immediate aftermath of 9/11, and which ceded extraordinary power to the US government.

One can also consider who surveillance targets. Here a utilitarian would argue that while in general citizens should have the right to be free from surveillance, individuals who are suspicious or who pose a danger to national security should necessarily have their rights curtailed.

In the aftermath of the 2013 Snowden revelations, Britain's former GCHQ chief, David Omand, published an op-ed in the British newspaper *The Guardian* (Omand, 2013) in which he made an argument that a government could ethically carry out covert surveillance of citizens provided certain conditions were met. (**Covert** here refers to secret surveillance both in the sense that the subject may not know that he is being surveilled and in the sense that the conduct of this surveillance may not be a matter of public record within the government itself.) In the op-ed, Omand (2013) made two types of ethical arguments. First, he made an argument from duty, stating that the intelligence community was carrying out its duties, which included the imperative that they take measures to keep citizens safe. He then went on to defend the actions of corporations like Google and Facebook that allowed the NSA access to customer communications – again making an argument from duty. He notes that they were merely complying with US law and should not be faulted for doing so.

In addition to making an argument for duty, Orman (2013) also advanced a consequentialist argument, noting that "most reasonable people would welcome the security that such intelligence can bring to our nations." In this argument, then, the risk and the costs of failure – to provide security to one's country and citizens – are so great that the 'cost' of depriving citizens of their rights is offset by the greater cost of failing to provide security.

However, not all ethicists agree with the utilitarian support of a pro-surveillance position. In a recent – and controversial – article in *Philosophy Now*, Emrys Westacott presents a thought experiment involving the use of surveillance technologies. She asks:

> Imagine that right after briefing Adam about which fruit was allowed and which was forbidden, God had installed a closed-circuit television camera in the Garden of Eden, trained on the tree of knowledge… . The serpent sidles up to Eve and urges her to try the forbidden fruit. Eve reaches her hand out. But at the last second, she notices the CCTV and thinks better of it. Result: no sin, no fall, no expulsion from Paradise.
>
> (2017, 1)

If we accept the conditions that God exists and that s/he is all-powerful, then certainly God could have done just that. However, Westacott argues that God wanted people to make their own right choices for their own right reasons, and not because they were being compelled to do so by a power differential. He wanted their choices to be voluntary and to be driven by the right motive.

She thus asks if people who are the subjects of ubiquitous surveillance are being deprived of the opportunity to build moral character, or to develop their own moral reasoning. She writes "increased surveillance may carry certain utilitarian benefits, but the price we pay is a diminution of our moral character. Yes, we do the wrong thing less often … but it also stunts our growth as moral individuals" (2017, 9).

Journalist David Brooks (2010) also makes a utilitarian argument against what he describes as "the culture of exposure." He describes how politicians are nearly always in the public eye, yet argues that the media – until recently – accepted the virtue of restraint, exercising judgment in deciding what to report. He writes, "The exposure ethos, with its relentless emphasis on destroying privacy and exposing impurities, has chased good people from public life, undermined public faith in institutions and elevated the trivial over the unimportant" (no pagination).

Finally, Michael and Michael (2011) argue that there are many costs associated with surveillance which utilitarian philosophers may have failed to consider. They argue that it is not inconceivable that someone might commit suicide as the result of being publicly humiliated through the publication of personally compromising information. They note that a completely transparent society characterized by total surveillance could thus have psychological consequences, citing "increased cases of mental illness – new forms of obsessive compulsive disorder and paranoia; a rise in related suicides; decreased levels of trust and the impossibility of a fresh start" (2011, 14).

Finally, we can use utilitarian thinking to consider the costs of surveillance, as well as the opportunity costs to society. What is the likelihood that some individuals will choose not to visit the United States, to invest in the United States or to work in the United States due to the presence of ubiquitous or differential surveillance? And in establishing ubiquitous surveillance, what opportunity costs would a nation sustain? What other services might a nation have to forgo in order to pay the bill for establishing an expensive system of surveillance? Does it make economic sense to engage in anticipatory surveillance in order to preempt an expensive terrorist attack, or should those resources be deployed elsewhere?

Virtue ethics

Much of the virtue ethics position on surveillance was presented in Chapter 4, when we examined US Secretary of State Henry Stimson's statement that "gentlemen do not read each other's mail." Here, Stimson argued for the virtue of restraint, a virtue which appears in Aristotle's own writing. A virtue ethics position might thus identify certain types of surveillance activities as inappropriate – not because of the harm to the victims that they might

generate – but because the conduct of such activities would not be in keeping with the character of a virtuous 'spy.' For example, the American Civil Liberties Union (No date) has described the ways in which individuals in authority have misused surveillance technologies – describing law enforcement officers who have used surveillance videos to stalk women, threaten and harass ex-spouses and blackmail individuals photographed patronizing gay bars. All of these represent the use of surveillance for wrong motives.

We can identify elements of the virtue ethics position in the Association of Computing Machinery's (ACM) own Code of Ethics, in particular in section 1.7, which reads "respect the privacy of others." Recently, Regalado (2013) has advanced the argument that ACM members who worked for the National Security Agency in 2013 were thus in violation of the ACM ethical code since they did not, in fact, engage in restraint in respecting individual privacy. Others disagreed with him, making a utilitarian argument. In response to Regalado, Eugene Spafford, an ACM official and a professor at Purdue University, argued (much as Stimson's critics did in the original scenario) that a greater good may be served if surveillance leads to information which prevents a terrorist outbreak (Regalado 2013).

What does ethical surveillance look like?

In an article written in 2013, David Omand, the former head of Britain's Signals Intelligence Organization, the GCHQ, proposed six principles that can be used to determine the ethicality of communications intercepts. These principles are loosely based on Just War ethical principles, as we will see in Chapter 7.

In his article, he proposes that:

- There must be a sustainable or genuine cause for which communications intercepts are necessary. That is, it is unethical for an agency (or an individual) to merely engage in a 'fishing expedition' where they poke around in communications in hopes of finding something illegal to prosecute.
- There must be a motive for conducting surveillance, and those seeking permission to engage in surveillance should be forthright and honest in declaring what that purpose is. (That is, they shouldn't lie about their motives or their aims.)
- The surveillance methods should be proportionate or limited. Omand argues that those conducting surveillance need to be aware of possible harms and determine that the possible benefits outweigh the harm. If at all possible, they should exercise restraint in deciding who to surveille and under what conditions.

Here Omand (2013) is utilizing a deontological lens in explicating the doctrine of minimum trespass or minimum force. This idea is borrowed from military ethics. Minimum trespass means that in carrying out an activity, the party should strive to do minimum damage against national and individual human rights. In other words, he should respect the dignity of the individual. Those who collect intelligence write that the collectors should be minimally intrusive and minimally invasive (Jones, 2009, 37). In his writing, military ethicist Pfaff (2009)

also distinguishes between soldiers, who are legitimate military targets since they have entered into a conflict freely and are aware of the dangers they are subjecting themselves to, and civilians, who are not. In writing about surveillance, he argues that an individual who is suspected of plotting harm could be a legitimate target of surveillance, but not his family members or others. He notes that "exploiting them may be the most expedient way to get information but it is not the most moral because none of these groups have knowingly and intentionally entered the 'game' in the way the other groups have" (83).

In addition, Omand (2013) notes that:

- There should be **rightful authority** – meaning that there should be documentation of surveillance patterns, with the clear establishment of accountability and a chain of command.

    This is the reason why ethicists have raised objections to new forms of **automated surveillance** – because of a lack of rightful authority. The blog *Arstechnica* describes a technology which the United States National Security Agency has used since 2010 known as Turbine. Turbine is used to hack millions of accounts a day. It automatically installs malware onto internet-connected devices, after targeting individual accounts. Using a program called Turmoil, it looks for cookies from many different services – like Google, Yahoo, Twitter, etc., as well as some Russian cookies from servers like Yandex. Once the 'implants' are installed onto a user's system, the NSA and Britain's GCHQ are able to extract data, monitor communications and even attack networks (Gallagher, 2014). The program thus creates an ethical distance between any potential harm created (such as an invasion of privacy) and the legally accountable organization (the National Security Agency). In this scenario, one might argue that Turbine was responsible for the invasion of privacy, and since Turbine is not human, it cannot be held morally accountable for the damage which it has created.

    In a similar example, Fogg (2003) describes a situation where a food service company installs a technology to check whether employees wash their hands prior to returning to work. He argues that an ethical system would notice a breach and prompt the employee to go back and wash his hands, while an unethical system would automatically notify the employer, resulting in the employee's termination. In the first scenario, the employee knows he is being monitored and he "buys in," cooperating with the software. In the second scenario, the employee may not even know why he was terminated, and is unable to place blame on the surveillance system for having harmed him by costing him his job (Fogg, 2003, 233).

- There should be a reasonable prospect of success expected when making a decision to conduct surveillance.

- Finally, Omand notes that the collection of secret intelligence should be a **last resort** when other methods of extracting information, such as diplomacy, have failed.

Omand's six points thus include virtue ethics arguments (including the notion of integrity); duty arguments (including the establishment of rightful authority); and consequentialist arguments (such as proportionality and reasonable prospect of success).

Good versus bad surveillance

So how might a computer programmer, asked to engage in surveillance activities, think about his actions? We will conclude this chapter by comparing and contrasting ethical and unethical surveillance. As we have seen in this chapter, good surveillance is benevolent. That is, the intent of surveillance matters. It is also controlled and regulated. In surveilling regular citizens – and not those accused of crimes – people should be made aware that they are being surveilled. (This is why citizens in Britain, for example, see so many signs on their streets and on their public transport informing them that they are under surveillance.) In some instances, good surveillance might give people the option of opting out of surveillance. And finally, good surveillance is not differentiated but is equal opportunity.

	Ethical Surveillance	*Unethical Surveillance*
Awareness	Citizens are aware they are being surveilled	Citizens are unaware of surveillance
Intent	Intent is to provide safety	Intent is to harm user or collect information aimed at harming user
Differentiated	All are equally subject to surveillance	Surveillance may be differentiated by race, gender, religion, etc.
Symmetrical/ Asymmetrical Relationship	Relationship may be one of equality	'Watcher' has power over watched (i.e. domestic abuse, stalking)
Opt Out Provision	In some instances, individuals may opt out of surveillance	No one may opt out of surveillance

Figure 5.2 Ethical and unethical surveillance

In contrast, unethical surveillance might be carried out for bad intentions, and it might be perceived by those who are surveilled as intrusive, humiliating or threatening. It is often asymmetric, with someone in a greater position of power watching someone with less power to object. Unethical surveillance often does not warn people, even private citizens, that they are under surveillance. It may not provide the ability to opt out of surveillance and it is often differentiated, by social class, gender or race.

Chapter summary

- The 'right to surveillance' belongs to corporations, agencies and states while the right to privacy belongs to individuals.
- **Differential surveillance** refers to practices in which certain groups – including the poor, ethnic and racial minorities and the disenfranchised – are more likely to have their behavior monitored and their rights curtailed.
- **Ubiquitous computing** means that today more people are watched in more places at more times and more data is stored and shared. Critics suggest that the 'death of privacy' is therefore inevitable and that surveillance and privacy are incompatible.
- People in different cultures may hold different views about acceptable levels of surveillance and privacy. As a result, nations may have different laws regarding surveillance and citizen rights.
- Today globalized patterns of data storage complicate surveillance activities since it is not always clear whose jurisdiction prevails when national laws differ regarding surveillance.

Discussion questions

1 You are asked to write a program which would engage in keystroke monitoring of your organization's new employees during a six-month probationary period of employment.

Do you feel that this is an ethical use of surveillance? What are some ethical concerns that you might have related to this policy?

3 Your supervisor asks you to implement measures to monitor the website usage and keystrokes of all employees who are not citizens of the country where you are located. These measures will be implemented without the employee's knowledge. Is this order either unlawful or unethical? How might you respond to an employer who asks you to engage in these activities?

4 Your company believes that it may be the subject of an insider threat. Your company's CEO issues a memo asking all employees to turn in their personal cell phones to company security officers along with the passwords they use on all social media sites. Do you comply with this order? Do you regard this order as either unlawful or unethical?

5 You are offered a job in a nation which has a very weak record of upholding civil rights, including the right to privacy. You are concerned that you may be asked to help design and service technologies which might be used against the nation's citizens, including members of vulnerable religious and ethnic groups. How might you use the concepts covered in this chapter to think through your decision whether or not to take the job?

Recommended resources

Materials available at the website of the Electronic Frontier Foundation (https://www.eff.org/)

Center for Democracy and Technology. November 2013. Analysis of surveillance laws in 13 countries.

CRS Report for Congress; The Foreign Intelligence Surveillance Act: a brief overview of selected issues. Elizabeth Bazan. Congressional Research Service)

Vodafone, June 2014, law enforcement transparency report: includes a legal annex analyzing the laws requiring ISPs to cooperate with law enforcement in 29 different countries

Chapter 5 sources

American Civil Liberties Union. No Date. "What's Wrong With Public Video Surveillance." Available at www.aclu.org/oither/whats-public-video-surveillance. Accessed January 24, 2017.

American Library Association. 2008. "Code of Ethics" Available at: http://www.ala.org/tools/ethics.

Amnesty International. 2015. "Two Years After Snowden: Protecting Human Rights in an Age of Mass Surveillance." Available at www.amnestyusa.org/research/reports/two-years-after-snowden-protecting-human-rights-in-an-age-of-mass-surveillance. Accessed April 12, 2017.

Angel, James, and McCabe, Douglas. 2015. "The Ethics of Payments: Paper, Plastic, or Bitcoin?" *Journal of Business Ethics*, 132(3): 603–611. Available at: "http://econpapers.repec.org/article/kapjbuset/"

Azaria, Amos, Richardson, Ariella, Kraus, Sari, and Subramanian, V.S. 2007. "Behavioral Analysis of Insider Threat: Survey and Bootstrapped Prediction in Imbalanced Data." *Journal of Latex Class Files* 6(1): 135–155.

Basu, Arandajit. 2015. "Why Microsoft's 'Data Trustee' Model Is a Potential Game-Changer in the Privacy War." *The Wire*. November 17. Available at https://thewire.in/15735/why-microsofts-data-trustee-model-is-a-potential-game-changer-in-the-privacy-war/. Accessed April 12, 2017.

Bazan, Elizabeth. 2008. *The Foreign Intelligence Surveillance Act: A Brief Overview of Selected Issues*. Washington, DC: Congressional Research Service.

Brooks, David. 2010. "The Culture of Exposure." *The New York Times*. June 24. Available at www.nytimes.com/2010/06/25/opinion/25brooks.html. Accessed April 12, 2017.

Buff, Anne. 2013. "Data's Ethical Landmines." *Information Management*. September 30. Available at www.information-management.com. Accessed April 12, 2017.

Cordero, Carrie. 2015. "Expanding on the International vs. US Surveillance Law Comparisons." *Lawfare Blog*. February 24. Available at www.lawfareblog.com/expanding-international-vs-us-surveillance-law-comparisons. Accessed April 12, 2017.

Donahue, Kathleen G. 2012. "Access Denied: Anticommunism and the Public's Right To Know" (pp. 21-50) In: Kathleen G. Donahue, ed. *Liberty and Justice for All?: Rethinking Politics in Cold War America*. Amherst, MA: University of Massachusetts Press.

European Commission. 2016. "Protection of Personal Data." November 24. Available at http://ec.europa.eu/justice/data-oprotection/. Accessed January 23, 2017.

European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE Committee). 2014 "Draft Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs" August 1. Available at: http://www.europarl.europa.eu/cmsdata/59881/att_20140306ATT80626-3142669982679416130.pdf

Fogg, BJ. 2003. *Persuasive Technology: Using Computers to Change What We Think and Do*. Boston, MA: Morgan Kaufman Publishers.

Fritcke, Emily. 2016. "Hacking Democracy." *Pacific Standard*, October 5. Available at https://psmag.com/hacking-democracy-38d7b2350416#.p0q5h0ydx. Accessed April 12, 2017.

Gallagher, Sean. 2014. "NSA's Automated Hacking Engine Offers Hands-free Pwning of the World." *Ars Technica*. March 12. Available at http://arstechnica.com/information-technology/2014/03/nsa-automated. Accessed January 8, 2017.

Gillion, J. 2011. *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy*. Chicago: The University of Chicago Press.

Hawthorne, Nigel. 2015. "Ten Things You Need to Know About the New EU Data Protection Regulation." *Computerworld UK*. May 6. Available at www.computerworlduk.com/security/10-things-you-need-know. Accessed January 23, 2017.

Jones, R.V. 2009. "Intelligence Ethics." In Jan Goldman, ed. *The Ethics of Spying*. Lanham, MD: Scarecrow Press: 18–38.

Koene, Ansgar, Perez, Elvira, Carter, Christopher, Statche, Ramona, Adolphs, Svenja, O'Malley, Claire, Rodden, Tom, and McAuley, Derek. 2015. "Privacy Concerns Arising From Internet Service Personalization Filters." *SIGCAS Computers and Society* 45(3): 168–171.

Landau, Susan. 2016. "Is It Legal? Is It Right? The Can and Should of Use." *IEEE Security and Privacy*. September/October. Available at http://ieeexplore.ieee.org/document/7676177/. Accessed April 12, 2017.

Longjohn, Matt, Sheon, Amy, Card-Higginson, Paul, Nader, Philip, and Mason, Maryann. 2009. "Learning From State Surveillance of Childhood Obesity." *Health Affairs* 29(3): 3463–3472.

McMullan, Thomas. 2015. "What Does the Panopticon Mean in the Age of Digital Surveillance?" *The Guardian*. July 23. Available at www.theguardian.com/technology/2015/jul/23/panopticon-digital. Accessed April 12, 2017.

Merritt, Marian. 2015. "Straight Talk About Cyberstalking." *Norton Symantec*. Available at http://us.norton.com/cyberstalking/article. Accessed April 12, 2017.

Michael, M.G. and Michael, Katina. 2011. "The Fallout from Emerging Technologies: Surveillance, Social Networks and Suicide." *IEEE Technology and Society Magazine* 30(3): 13–19. Available at http://ro.uow.edu.au/cgi/viewcontent.cgi?article=9868&context=infopapers

Morris, Ian. 2016. "Amazon Echo Now an Expert Murder Witness?" *Forbes*. December 28. Available at www.forbes.com/sites/ianmorris/2016/12/28/amazon-echo-now-an-expert-murder-witness/#26942381dab9

Neocleos, Mark. 2003. *Administering Civil Society: Towards a Theory of State Power*. London: Macmillan.

No Author. 2016. "In Focus – #encryption Norms." *Digital Frontiers*. December 13. Observer Research Foundation. Available at www.orfonline.org/expert-speaks/in-focus-encryption-norms/. Accessed April 12, 2017.

Omand, David. 2013. "NSA Leaks: How to Make Surveillance Both Ethical and Effective." *The Guardian*. June 11. Available at: https://www.theguardian.com/commentisfree/2013/jun/11/make-surveillance-ethical-and-effective

Perlforth, Nicole. 2014. "Hackers Using Lingo of Wall St. Breach Health Care Companies' Email." *New York Times*. December 1. Available at www.nytimes.com/2014/12/02/technology/hackers-target-biotech-companies.html?_r=0. Accessed April 12, 2017.

Pfaff, Tony. 2009. "Bungee Jumping Off the Moral High Ground: Ethics of Espionage in the Modern Age." In Jan Goldman, ed. *Ethics of Spying: A Reader for the Intelligence Professional*. Lanham, MD: Scarecrow Press: 66–104.

Regalado, Antonio. 2013. "Cryptographers Have an Ethics Problem. Mathematicians and Computer Scientists are Involved in Enabling Wide Intrusions on Individual Privacy." *MIT Technology Review*. September 13. Available at www.technologyreview.com/s/519281/cryptographers-have-an-ethics-problem/. Accessed April 12, 2017.

Roberts, Eric. No Date. "Encryption" Available at: http://cs.stanford.edu/people/eroberts/courses/cs181/projects/public-key-encryption/ee.html.

Saran, Samir. 2016a. "Cyber (in)security in India." *Lawfare*. February 16. Available at www.lawfareblog.com/cyber-insecurity. Accessed April 13, 2017.

Saran, Samir. 2016b. "Navigating the Digital Trilemma." *Digital Debates*. October 13. Observer Research Foundation. Available at www.orfonline.org/expert-speaks/navigating-the-digital-trilemma-2/. Accessed April 13, 2017.

Scheppele, Kim Lane. 1993. "It's Just Not Right: The Ethics of Insider Trading." *Law and Contemporary Problems* 56(3): 123–174.

Schneier, Scott. 2006. "Who Watches the Watchers?" *Schneier on Security blog*. January 16. Available at www.schneier.com/blog/archives/2006/01/who_watches_the_watchers. Accessed December 2, 2016.

Schwartz, Paul M. 2010 "Data Protection Law and the Ethical Use of Analytics." *The Centre for Information Policy Leadership*. Available at https://iapp.org/media/pdf/knowledge_center/Ethical_Underpinnings_of_Analytics.pdf. Accessed January 1, 2016.

Stoddart, Eric. 2011. *Theological Perspectives on a Surveillance Society*. New York: Routledge.

Swearingen, Jake. 2016. "Can an Amazon Echo Testify Against You?" *New York Magazine*. December 20. Available at http://nymag.com/selectall/2016/12/can-an-amazon-echo-testify-against-you.htm. Accessed January 15, 2017.

Techopedia. No Date. "What Does Encryption Mean?" Available at www.techopedia.com/definition/5507/encryption. Accessed May 1, 2017.

Timan, Tjerk, and Albrechtslund, Anders. 2015. "Surveillance, Self and Smartphones: Tracking Practices in the Nightlife." *Science and Engineering Ethics*.

Turilli, Matteo, and Floridi, Luciano. 2009. "The Ethics of Information Transparency." *Ethics of Information Technology* 11(2): 105–112.

US House of Representatives, Homeland Security Committee Staff Majority Report. 2016. "Going Dark, Going Forward: A Primer on the Encryption Debate" June 2016. Available at: https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf.

US Legal Dictionary. No Date. "Complicity" (definition). Available online at: https://definitions.uslegal.com/c/complicity/.

Vaz, Paolo, and Bruno, Fernanda. 2003. "Types of Self-Surveillance: From Abnormality to Individuals 'at Risk.'" *Surveillance and Society* 1(3): 272–291.

Waddell, Kaveh. 2017. "Why Bosses Can Track Their Employees 24/7." *The Atlantic*. January 6. Available at www.theatlantic.com/technology/archive/2017/01/employer-gps. Accessed January 10, 2017.

Wagner, Ben, and Bronowicka, Joanna. 2015. "Between International Relations and Arms Controls: Understanding Export Controls for Surveillance Technology." *Przeglad Politologiczny*. Available at https://cihr.eu/wp-content/uploads/2015/11/Between-International-Relations-and-Arms-Controls_pp-2015-3-153-article_14.pdf. Accessed May 10, 2017.

Westacott, Emrys. 2017. "Does Surveillance Make Us Morally Better?" *Philosophy Now* 79: 6–9. Available at https://philosophynow.org/issues/79/Does_Surveillance_Make_Us_Morally_Better. Accessed January 24, 2017.

6 The problem of piracy

Learning objectives

At the end of this chapter, students will be able to:

- Describe traditional ethical arguments in favor of the right to own physical property
- Identify at least three objections to the application of Locke's Theory of Property Rights to the notion of intellectual property and three arguments in favor of doing so
- Define key terms in the discussion of intellectual property (IP) issues – including fair use, economic right, moral right, piracy and intellectual property
- Apply the virtue ethics, utilitarian and deontological lens to thinking through the ethical issues of intellectual property
- Analyze the issue of establishing norms to protect intellectual property, identifying sources of support for these norms, as well as problems which make achieving consensus difficult

As we consider the ethical problems of piracy or theft of intellectual property, we can consider five real-life situations involving theft of intellectual property:

- In 2014, several pharmaceutical and medical device companies – including Medtronic, St. Jude and Boston Scientific – were the subject of hacker infiltration. Investigators believe that the hackers were attempting to steal proprietary information related to medical devices so that the technology could be replicated in China (Lindsay, 2014).
- In January 2016, the international College Board testing organization cancelled the administration of the Scholastic Aptitude Test (an exam used for

college entrance in the United States) in five nations – China, Macau, Spain, Bahrain and Kazakhstan – amidst allegations that some students had seen the test questions prior to the administration of the examination (Schultz, 2016).

- In 2014, a number of US citizens and foreign nations, most in their early twenties, were prosecuted by the US Department of Justice after they hacked into and stole simulation software used by the US Army to train Apache helicopter pilots. The perpetrators carried out their actions both within the US and abroad (No Author, "Hackers Charged in Software Theft from US Army," 2014, 1).
- In 2010, three Chinese citizens were the subject of legal action by Gucci America due to their online activities. The group had been selling high quality imitation products which consumers abroad had purchased, believing they were genuine Gucci products (Volodzko, 2015).
- In 2015, four American men pled guilty to stealing more than 100 million dollars' worth of intellectual property. Over a two-year period, they hacked into the networks of Microsoft, Epic Games, Zombie Studios and the Valve Corporation. They stole software, trade secrets and prereleased copies of games which they then sold for a profit (Walker, 2015).

What do these cases have in common? As these examples show, the term piracy covers a wide variety of different types of activities. These activities vary in severity, in the intent of the perpetrator and in the harms which they create. Some readers might question whether all actions constitute theft or criminal activity. These examples illustrate the grey areas created by rapidly developing technologies and less rapidly developing legal regimes both in the United States and abroad. They also show the lack of consensus regarding the norms and ethics governing piracy.

And again, in this chapter the uniqueness debate rears its head. In considering the theft of intellectual property in cyberspace, observers don't all agree that intellectual property (IP) theft in cyberspace is the same as stealing a physical object. In what ways does the unique environment of the internet facilitate theft of intellectual property and perhaps even invite it? And should we use the same or different criteria for thinking about the ethics of IP theft than we do in thinking about theft of physical property?

In this chapter, we ask several questions: What are rights of creators to 'own' the products they produce online or in the real world? How should cyberspace be governed to allow for the idea of private ownership and should it be set up in this

way? And how should individuals consider their own actions in cyberspace – regarding whether and under what conditions they respect the right to private property?

We begin by defining key terms. We then dive into ethics of ownership, and the key differences between cyberspace and real space. We then consider legal and ethical understandings relevant to understanding this problem. We conclude by applying our three models – virtue ethics, utilitarianism and deontological ethics – to thinking about IP issues in cyberspace.

What is intellectual property?

We begin by considering the broader notion of intellectual property. What does it mean to own an idea? Although this sounds like a very modern notion, we can trace the idea of intellectual property back to 500 BC, when chefs in the Greek colony of Sybaris were given a monopoly over their ability to produce a particular culinary dish. Intellectual property is also recognized in British law, going back to the **Statute of Monopolies**, passed in 1624 and the **Statute of Anne**, passed in 1710. The Statute of Monopolies still provides the basis for the American and British systems of patent. Nasheri defines a **patent** as "an exclusive right granted for an invention (a product or process that provides a new way of doing something or offers a new technical solution to a problem)." A patent lasts for a specific time period, is for a specific geographic area (such as the United States) and requires that the inventor publicly disclose his process or product specifications through filing a patent (2005, 5).

The Statute of Anne established the notion of copyright for literary works. **Copyright** is granted for artistic products and can be given to the creator and can also be passed on to his or her heirs. Copyright protects artistic works – like novels, plays, photographs, music, etc. – while industrial property laws and regimes protect inventions and industrial designs through the use of patents and trademarks (Nasheri, 2005).

In considering patents and copyrights, we see how technological developments made these ideas necessary. With the invention of the printing press, individuals were able to make multiple copies of a document and it became necessary to establish the conditions under which a document could be reproduced and shared. Today, with the growth of the internet, it is easier than ever to download and

upload files and images, and new legal developments are establishing new understandings of what it means to own ideas.

Anglo-American intellectual property arguments rest on utilitarian theory: United States president Thomas Jefferson – himself an inventor and the creator of both the swivel chair and the pedometer – argued that the inventor didn't have a 'natural right' to control his output and its use but that it was a reward granted to him so that society as a whole could progress. In utilitarian theory, society maximizes utility by giving rights to authors as an incentive towards progress (Moore and Unsworth, 2005).

As Varelius states, "**intellectual property rights** protect the financial interests and reputation of creators of intellectual objects – objects like inventions, melodies, concepts, methods and (expressions of) ideas" (2014, 299). She notes that the claim that one can "own" an idea rests on the legal idea of ownership of physical objects. Full ownership of material objects is seen to include a right to use them, transfer them and to destroy them and modify them. The owner can also decide who to share them with or refrain from sharing them with. Varelius distinguishes between **moral rights** and **economic rights**. An economic right is the right to be financially compensated if someone else uses your intellectual property. This is the basis **for licensing agreements** where, for example, someone who wanted to make and sell a t-shirt or a mug with a cartoon character on it would have to pay a fee to the person who originally drew the image. In addition, the agreement would specify the conditions under which the image could be used and the ways in which it could and could not be modified. Nasheri defines a **trademark** as: "a distinctive name, logo or sign identifying the source of goods or sources; counterfeiting includes actions to sell a product under a false trademark" (2005, 5).

A **moral right** is the right to be recognized as the creator of the idea or concept (in other words, not to have your work plagiarized) and the right to control how the object is modified – so that one's reputation is not sullied. (For example, the creator of a cartoon image might object to someone making and selling a pornographic or nude version of that image.)

Within the United States, specific legal doctrines uphold intellectual property rights claims. **Fair Use laws** specify the amount of a work which can be quoted in a book or document or the percent of an object (like a song) which can be borrowed without payment of a licensing fee. Copyright and patent procedures allow an artist or creator to claim ownership of a cultural product or idea, and copyrighted and patented objects cannot be used without payment of a licensing fee.

However, despite the fact that legislation exists within the United States and international agreements like the World Intellectual Property Organization Broadcasting Treaty have been agreed upon, there is still debate about both the legal and ethical/moral aspects of intellectual property rights. There is no clear consensus among nations regarding the ethics and laws which should govern this area of internet production. Instead, one can identify good and compelling ethical and moral arguments from all perspectives (utilitarian, virtue ethics and deontological) both for and against upholding legal restrictions like copyright.

What is piracy?

The term **piracy** refers to practices by which individuals upload or download, share, transmit or distribute audio or visual information files which are copyrighted. Piracy refers to transmittal of digital information. Individuals engage in piracy whether they are uploading or downloading information to unauthorized web sites, using a program to share these materials from one person to another, or making an audio file from a video which might be online. The **piracy rate** is defined as "the number of pirated software units divided by the total number of units put into use" or the percentage of software acquired illegally. Every nation is estimated to have at least a 20 percent piracy rate, with two nations having a piracy rate of 90 percent (Akman and Mishra, 2009).

In the United States, the costs of piracy are estimated at 12.5 billion dollars per year. The Motion Picture Association puts its economic losses at 3 billion dollars per year, noting that piracy means the loss of over 70,000 jobs in the recording industry. States and localities also incur losses, since those purchasing bootlegged copies of videos or music do not pay sales tax which goes back into the community (Moustis and Root, 2016). The Business Software Alliance notes that almost 20 percent of US business software is unlicensed, leading to a monetary loss of 10 billion dollars per year. This organization notes that "when you purchase software, you do not become owners of the copyright." They argue that a user purchases rights to use a copy of software but not to distribute it without authorization. The BSA does not distinguish between large scale redistribution and sharing copies with friends. Both are regarded as unlawful or unethical (BSA.org, No date).

While content producers agree on the definition of what constitutes unauthorized use of their products – or piracy – not everyone agrees regarding the definition of piracy. The only international definition is included in **United Nations Agreement**

on Trade-Related Aspects of Intellectual Property Rights (the so-called **TRIPS Agreement)**. The agreement notes that:

> Pirated copyright goods shall mean any goods which are copies made without consent of the right holder or person duly authorized by the right holder in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country of importation.
>
> (art 51, n 14, from UNESCO.org)

Thus, it is clear that piracy is regarded as criminal activity which violates specific copyright laws, both in the country of origin and internationally. But what specifically makes copyright piracy unethical?

The ethics of property ownership

In the West, our thinking about what it means to own something, and what gives someone an ethical claim to ownership derives from the thinking of John Locke, an English political philosopher from the 17th century. However, as Tavani (2005) notes, analysts today disagree about whether Locke's thinking is still relevant in a world of intangible cyber assets. When Locke (1632–1704) was writing his theory of property, he was concerned with the dispersion of **tangible assets** (things that can be felt, seen and touched). He asked: What are the conditions under which someone can claim to own something? And how do we distinguish between those things that are owned in common and those things that someone might have a right to own? Finally, he asked whether there were any limits to ownership. In other words, could someone rightfully (legally and ethically) make a claim to own all of something, if doing so meant that others might be deprived of the ability to own that thing?

In his *Second Treatise*, Locke argues that you earn the right of ownership through taking an object (like farmland) and "mixing (your) labor with it." That is, land might be held in common by a village, but the farmer who farms the land can claim to own the land as well as the vegetables which he grows on it. Here, Locke argues that because we own our bodies – and have the right to do so – if we mix our bodily labor with that object, then we can also claim ownership of that object (Himma, 2013).

However, as Tavani (2005) points out, Locke didn't believe that this claim to ownership was unlimited. He clearly stated that you couldn't take all of something (like fruit picked from a fruit tree) if you didn't intend to use it, but instead were going to waste it. He cautioned against hoarding something up, which he viewed as unethical. He also cautioned against taking all of something, believing you should leave "enough and as good" for others.

Applying property ethics to cyberspace

While many scholars begin with Locke in discussing intellectual property, others argue that intellectual property is so different from tangible assets that the argument doesn't fit. Here they identify two problems: Some scholars ask if using one's mind to write code or invent an app is really the same as "mixing one's labor" with something physical. Tavani asks whether having an idea come to you while sitting on the beach is really the same as toiling in a field all day. He describes this as the problem of "the indeterminacy of labor" (2005, 89). Next, some scholars object to the fact that there is no actual tangible "thing" that a creator or inventor mixes his labor with. For example, in composing a symphony, what exactly is it that the creator is using as the raw materials? Hardy et al. (2013 describe the differences between tangible and nontangible objects and how these affect people's perceptions of ownership and property. They describe the relationship between physical property and physical boundaries, noting that you steal something when you remove it from someone else's store or home, but that there is no similar "signal" in cyberspace to connote that you are stealing something. They also note that when a physical object is taken there is less of it for everyone else, whereas in cyberspace, a text, a snippet of code or a graphic object is not actually taken but cloned. The "thief" is merely making a copy of something, but is not actually removing it from its original location so that no one else can use it there.

Box 6.1 Applications: the ethics of BitTorrent

BitTorrent is a technology developed in 2005 which allows for peer to peer sharing of material. Individuals download the BitTorrent program onto their computers and then send out a message requesting a certain file (such as an

audio file or movie). The software queries other BitTorrent users and when it finds a computer that has the material, it begins downloading. An exchange is set up in which both parties can take files from each other's computers (How BitTorrent works). In a regular download, material is sent to a server from which the client downloads a file. But in a P2P relationship, each party acts as their own server and connects directly to the other computer (Pace, No date).

BitTorrent represents an unusual ethical situation. Throughout this text, we have contended that a technology does not on its own have an ideology or ethics – but that something is ethical or unethical depending on how it is used. Presumably BitTorrent could be used either for good or evil. But Brad Buckles, Vice President for anti-piracy at the Record Industry Association (RIAA), states that BitTorrent currently enables 75 percent of all piracy of recorded material. Thus, one could argue that BitTorrent's purpose is overwhelmingly bad. Indeed, if BitTorrent were eventually used to share files which provided the specifications for goods to be manufactured on 3D printers, then people could even begin manufacturing on their own, bypassing corporation's altogether (Bowie, 2013).

RIAA has appealed to BitTorrent to exercise good corporate citizenship in sharing information with law enforcement regarding who has accessed the site (Mullin, 2015). In other communications, the RIAA describes all P2P technologies as associated with piracy, and warns visitors to its site that utilizing these services to access unlicensed material carries criminal penalties (RIAA).

But Matt Mason, Chief Content Officer at BitTorrent, argues that sharing happens "outside the system" (Mullin, 2015). He does not accept the premise that BitTorrent is guilty of committing piracy, or even, indeed, of enabling piracy, and he does not accept the RIAA's contention that BitTorrent has a social obligation to help prevent the misuse of its site and the conduct of piracy.

Attempting to police use of BitTorrent

In the US, the Comcast cable company has been accused of taking steps to disrupt peer-to-peer file sharing. The Electronic Frontier Foundation has accused Comcast of interfering electronically with user's BitTorrent and Gnutella sessions. The US Federal Communications Commission (FCC)

weighed in in 2008, stating that Comcast could only take measures to disrupt these services if its attempts to carry out these measures were transparent. In addition, the fact that certain types of online activities are being treated differently and interfered with has been described as a violation of net neutrality protocols. Some individuals and groups have filed class action suits against Comcast (Paul, 2008).

In addition, the law firm Steele Hansmeier, which protects intellectual property rights, has attempted to use laws which would forbid mass file-sharing and allow the prosecution of large numbers of intellectual property pirates at a time. Although peer-to-peer network sharing only links two users together – with each user's computer serving as its own network – the law firm tried to make the case that everyone who visited the same website to, for example, download an illegal movie, could be considered to be engaged in 'mass file sharing' and thus it would be permissible to prosecute 180 people at the same time. However, this lawsuit was not successful (Anderson, 2011).

Applying the frameworks

A utilitarian might decide that the costs of using BitTorrent are not worth it. Pace argues that using BitTorrent is dangerous since it relies on a trust between clients in P2P that is probably not warranted. He cautions that the other computer could easily load malware onto your server.

A Rawlsian would ask if using P2P technology was just and equitable. Here ethicists at Theconversation.com argue that those who download files illegally are committing a type of 'free riding,' since they are allowing legal users of the media to subsidize their illegal use. The artists cannot continue to make new work unless they are subsidized, and it is only the legal purchasers who provide that subsidy.

Finally, a virtue ethicist might zero in on the virtue of respect, noting that respecting copyright is the best way to respect an artist and his work (*theconversation.com*, 2015).

Ethical arguments in favor of BitTorrent

But one can also make an ethical argument in favor of file-sharing. Bowie describes P2P sharing as a type of "friendship," noting that friends share things.

He also makes a Robin Hood argument in arguing that corporate interests punish the poor, while BitTorrent serves as a Robin Hood, robbing from the rich to give to the poor. He describes his view as one based on higher moral reasoning, in which he is opposing laws which he views as inequitable and unjust. He notes that "if sharing were utilized instead of criminalized, it would have transformative results on society, especially low-income societies that have difficulty accessing higher education and cultural media."

Ethicists at "the conversation" believe that both laws and norms can change and evolve over time, often as a result of people becoming more enlightened, educated and open-minded. For example, they argue, "Same-sex relationships, divorce and many other practices that are now widely regarded as morally acceptable were once outlawed and criminally sanctioned" (*theconversation.com*, 2015). They also do not argue that individuals who download an illegal product may have the opportunity to sample some merchandise that they may then go on to purchase. In this way, illegal use builds demand for legal products and benefits producers. Finally, a blogger at the "using bit torrent" blog on Wordpress points out that there are actually uses of BitTorrent which are legal. They include the downloading of materials which have an expired copyright or which are in the public domain, the downloading of material which has a Creative Commons license and the downloading of material which is not copyrighted – which might include home movies, private photographs and so forth.

Sources

Anderson, Nate. 2011. 'BitTorrent Users Don't 'act in concert', So Judge Slashes Mass P2P Case." *Arstecdhnica.com*. August 29. Available at http://arstechnica.com/tech-policy/2011/08/bittorrent-users-dont-act-in. Accessed March 1, 2017.

Bowie, Nile. 2013. "BitTorrent Ethics: Punishing Piracy or Criminalizing Sharing?" *RT.com* October 19. Available at www.rt.com/op-edge/torrent-piracy-sharing-law-440. Accessed March 13, 2017.

How Stuff Works. "How BitTorrent Works." Available at *computer.howstuffworks.com/bittorrent.htm*. Accessed March 11, 2017.

Mullin, Joe. 2015. "RIAA Says BitTorrent Software Accounts for Seventy-Five Percent of Piracy, Demands Action." Available at https://arstechnica.com/tech-policy/2015/08/riaa-says-bittorrent-software-accounts-for-75-of-piracy-demands-action/. Accessed August 1, 2017.

No Author. 2010. "Legal Uses of Bit Torrent." June 9. Available at https://usingbittorrent.wordpress.com/. Accessed March 2, 2017.

Pace University. No Date. "Copyright, Peer to Peer (P2P) and Illegal File Sharing." Available at www.pace.edu/its/it-security/copyright-peer-to-peer-and-illegal-file-sharing. *Accessed* January 12, 2017.

Paul, Ryan. 2008. "FCC to Investigate Comcast BitTorrent Blocking." January 9. Available at https://arstechnica.com/tech-policy/2008/01/fcc-to-investigate-comcast-bittorrent-blocking/. Accessed February 15, 2017.

Riaa.com . "Resources and Learning." Available at www.riaa.com/resources/learning/about-piracy/. Accessed January 6, 2017.

Theconversation.com . 2015. "Is Downloading Really Stealing? The Ethics of Digital Piracy." *The Conversation*. April 13. Available at http://theconversation.com/is-downloading-really-stealing-the-ethics-of-digital-piracy-39930. Accessed March 2, 2017.

Others, however, find Locke useful for analyzing IP theft, since it considers problems like scarcity and hoarding. These scholars suggest that regulations like copyright restrictions and paywalls in particular are the intangible equivalent of hoarding – since they can serve to close people out of particular areas of the internet. Here, they describe the internet as an '**information commons**', which is the intangible equivalent of a patch of shared farmland which abuts a village. Just as one man's decision to take all the farmland might leave others worse off and perhaps even kill them through starvation, these scholars argue that a firm's decision to wall off large parts of the internet through charging access fees could potentially harm others, leaving them out of the information revolution and obstructing their abilities to engage in commerce or learning. (For example, if we conceive of the internet as a conduit for information which would make us all better and more informed citizens, then a system where all of the top newspapers charged a high access fee, might mean that in reality the only free news available was of poor quality, and citizens were not able to effectively inform themselves using online resources.) In its most extreme formulation, the 'information commons' argument suggests that any attempt to regulate copyright and protect intellectual property on the internet is unethical (Himma, 2011). Here Himma also takes issue with the notion of 'scarcity' in cyberspace, wondering if a scarcity of access to information is really the same as the scarcity of access to food (2011, 221).

Here, Tavani suggests that we apply Locke to cyberspace through asking two questions:

> Does a particular law or policy diminish the information commons by unfairly fencing off intellectual objects? And are ordinary individuals made worse off as a result of that law or policy when they can no longer access information that had previously been available to them?
>
> (2005, 92)

Some analysts suggest that we all have an ethical responsibility to preserve the information commons through sharing objects and not recognizing copyright. In recent years, we have seen this stance reflected by a movement in the medical community which seeks to make medical information accessible to everyone who wants to read it, rather than allowing it to be placed beyond paywalls where only those with access to subscriptions to medical journals or a medical library can read it (Maisel, No date). Here, activists have suggested that since people pay taxes which are used in part to fund medical research through groups like the National Institutes of Health, then all people should have a right to read any research that might result from these grants. In the most well-known case, libertarian computer activist **Aaron Swartz**, bulk downloaded the archives of the JSTOR scholarly database using a guest account on the Massachusetts Institute of Technology's computer network. Swartz, a co-founder of the online discussion board Reddit, was threatened with prosecution for his 2010 actions. He has been described as a 'martyr' of the open access movement, as he committed suicide in January 2013 at the age of 26. JSTOR eventually made 4.5 million articles from its archives available for free to the public. Subsequently, many institutions – like the National Institutes of Health, the Massachusetts Institute of Technology and Harvard University – have implemented Open Access mandates – requiring research the institution helps fund to be made openly available through open access journals or in an institutional repository (Hockenberry, 2013, 7). Swartz's actions in fighting for open access have been described as a form of civil disobedience. In his **Guerilla**, **Open Access Manifesto**, he referenced the fact that people have a moral obligation to oppose unjust laws. He saw the **Stop Online Piracy Act (SOPA)** as an unjust law.

However, others argue that the information commons/physical commons analogy is not really apt. Himma notes that while the farmland available to a village is preexisting (provided by the universe or a god), the resources which we find on the

internet are created by content providers. The news is available because someone wrote it and gathered it, and that person needs to be compensated for the products of his or her labor (2013, 7).

As we see here, moral philosophy arguments about the information commons have also become entwined with policy stances derived from philosophy of technology, as we described in Chapter 1. Many of those who argue that the information commons must be preserved base their arguments not on Locke, but on stances regarding the nature of cyberspace/the internet or the nature of information itself. Here they reference not Locke, but Paul Barlow, an early internet pioneer who spoke of the internet as an unregulated space which should not be ruled by laws (Himma, 2011). They may also reference the nature of information itself in arguing, for example, that 'information wants to be free, not regulated.' Both of these stances reference the character of the internet or the character of information, rather than referencing the ideas about justice and equity, fairness and compensation, which Locke used in building his property argument.

Box 6.2 Critical issues: do you own your genetic data?

How do ethicists approach a situation where there are two competing sets of values and two competing solutions? This is the situation that ethicists, lawyers and policy analysts have found themselves in when they begin to confront the issue of 'genetic information.'

The issue is this: Each of us has a unique set of DNA and a unique set of genetic information. Yet many research projects attempt to make scientific and medical progress through aggregating the data they collect about a large set of individuals. In Iceland, researchers in the deCODE Genetics project have been able to isolate particular segments of people's genetic code and then compare these segments to other people whom they are related to. Then, if they know an individual and a family's medical history, they can begin to make connections between shared patterns which individuals have and particular diseases and attributes which the family may share.

Thus, this genetic information belongs to you, but arguably, should also belong to the medical and scientific community. Is it selfish to refuse to share

your genetic information and to hoard it to yourself based on the claim that you 'own' it, if doing so keeps others from receiving needed medical diagnoses and treatments? But some individuals fear being exploited by, for example, a pharmaceutical company which might profit from developing a drug or therapy derived from their genetic material. Shouldn't they have a right to share in these profits too? Both arguments sound plausible, so how do ethicists decide which one is right?

Some ethicists believe you can own your genetic material. Some even support **genetic exceptionalism**, arguing that genetic material is even more entitled to protection in the form of property rights and privacy rights. In Iceland, the Association of Icelanders for Ethics and Science, and the Icelandic Medical Association are concerned that deCODE has used individuals' genetic material without their full knowledge and consent. They support better methods of informed consent and better legal mechanisms for regulating these activities. In the United States, many states have passed laws declaring that individuals do indeed own their genetic information and that they have a right to privacy in that regard.

Others argue that the researcher's greatest ethical duty is to individuals who might benefit from a therapy. They argue that it's inefficient for a company to have to contact – and compensate – everyone whose genetic material might have been used in a research effort. Such rigorous rules will ultimately slow down progress, they claim.

Still others argue that it is researcher's labors which create a new product, noting that you can patent a gene. They feel that ownership should belong to the creator, not the person who contributed to it in some way.

In his work, Spinello advances a deontological argument. He writes:

> An impartial observer, behind the Rawlsian veil of ignorance would not want to risk the loss of control over his or her genetic information. That person would not want such information to be made available to others without permissions … she would want to be able to restrict access and determine how that information is utilized by third parties.
>
> (2004, 38)

Which of these arguments best describes your own position on this issue?

Source

Spinello, Richard. 2004. "Property Rights in Genetic Information." *Ethics and Information Technology* 6: 29–42.

Applying the lenses

What do the three ethical lenses introduced in Chapter 2 – virtue ethics, utilitarian ethics and deontological ethics – have to say about intellectual property?

Virtue ethics

As we saw in Chapter 2, virtue ethics prioritizes developing moral or ethical character, and suggests that the most ethical decision is in line with the decider's values, allowing them to develop these values. In considering intellectual property, we might reference the value of 'care for others' and argue that intellectual property violations are unethical because they expose others to risk. For example, former US Deputy Undersecretary of Commerce for Intellectual Property Stephen Pinkos has stated that currently 10 percent of all medicine sold worldwide is counterfeit. He argues that states and individuals thus have a duty to oppose counterfeiters since their actions can endanger others (United States Patent and Trade Office).

Another virtue we might consider is integrity – or the idea that your actions and values should be consistent across environments. It would thus require treating all acts of IP theft as equally wrong – not distinguishing between 'borrowing' a photo and installing bootleg software on all of one's office computers. In addition, virtue ethics forces us to consider the related ethical issue of **complicity**, or "aiding and abetting" in the commission of wrongdoing. Urbas argues that in order for an event like pirating software from a legitimate vendor to occur, multiple individuals and groups must cooperate. He suggests that everyone who cooperates – through making a website available as a space for illegal transactions, passing along information, or purchasing a good which they suspect is stolen – is both legally and morally involved and therefore responsible for the consequences which ensue, regardless of their small or large part in it.

Box 6.3 Critical issues: bulletproof hosting

What is bulletproof hosting? **Bulletproof hosting** (sometimes known as bulk-friendly **hosting**) is a service provided by some domain **hosting** or web **hosting** firms that allows customers considerable leniency in the kinds of material they may upload and distribute.

Such facilities are often hosted in nations where the legal conditions regarding internet activities are murky and law enforcement ability is weak. In many instances, individuals or groups who wish to engage in an activity which is illegal in their own country (such as sharing child pornography, carrying out internet fraud scams or trading in malware) will contract to have their activities hosted in another country. In such a situation, it may be difficult to establish jurisdiction and prosecute those responsible, particularly if the United States does not have an extradition agreement with the host nation. Countries which are in chaos and turmoil are often particular candidates for locating a bulletproof hosting services. Currently, many are located in Panama, Lebanon, Ukraine, Russia and Iran. In addition, criminals may move their operations frequently from one nation to another and one server to another.

Trend Micro, a company which researches cyber security, notes that a bulletproof host server can be rented for about 70 dollars a month. Clients can also rent malware, and even have access to a helpdesk at the server that they can call if they have problems.

Why is bulletproof hosting unethical?

Bulletproof hosting is not in itself unethical. Indeed, some analysts argue that some needs for a BPH are legitimate. For example, current Russian law makes it difficult to send out legitimate bulk e-mails which consumers may actually want; therefore, business people may turn to a BPH.

However, bulletproof hosting raises the issue of complicity, since it may provide a venue for other types of criminal and unethical activity. Goncharov (2015) suggests that it would be similar to renting out your house to be used by a criminal network. Palmer (2016) writes that "Bulletproof hosting … enables cybercrime. It is the technological equivalent of a physical hideout. Just as a gang needs a place to cache weapons and stolen goods, cyber

criminals need internet-connected servers on which they can keep the malicious software they use for attacks, fake internet sites used for scams and the data they have stolen."

Goncharov also acknowledges levels of complicity, depending on how involved the provider is in supporting the activities. The hosting server's personnel may also be guilty of deception if they are helping to conceal the existence of the operation by, for example, compromising a dedicated legitimate server by renting parts of it out to malicious parties (Goncharov, 2015).

Sources

Krebs, Brian. 2016. "Body Armor for Bad Web Sites." *Krebs on Security*. November 10. Available at http://krebsonsecurity.com/tag/bulletproof-hosting. Accessed March 3, 2017.

Goncharov, Max. 2015. "Criminal Hideouts for Lease: Bulletproof Hosting." *Trend Micro*. July 15. Available at www.trendmicro.fr/media/wp/wp-criminal-hideouts-for-lease-en.pdf. Accessed March 2, 2017.

Palmer, Maija. 2016. "Rogue States Play Host to Outlaw Servers." *Financial Times*. March 14. Available at www.ft.com/content/c926b4ec-da25-11e5-98fd-06d75973fe09. Accessed March 1, 2017.

However, one can also make a virtue ethics argument in favor of violating intellectual property – if one adopts a non-Western mindset. Chien describes an Asian mindset in which objects might belong to a family or a community rather than individual; where one might copy a sage or scholar as a sign of respect, not wanting to risk making a mistake by paraphrasing his thoughts; and where an author might be viewed as having a responsibility to share his knowledge with society without requiring citation or acknowledgement (2014, 124). At the same time, Gatig and Russell (2015) note that "in traditionally oral Arab culture, the information comes from wisdom, poetry, songs and folk stores, not books. In this respect, information is essentially in the public domain" (812). Their studies show that many Turkish students, for example, are unaware of the Western notion of plagiarism.

Thus, in cultures unfamiliar with Western notions of intellectual property, it may be difficult to establish a consensus about the ethics of such an action. Indeed, Ocho argues that within the Chinese context, one could frame a virtue ethics argument in

favor of 'sharing' information. He notes that in a culture which valued collaboration, what we view as an intellectual property violation might actually be seen as an admirable gesture, rather than something to be eschewed. In addition, we can identify divides along economic lines as well as along cultural lines. In developing countries, the 'borrowing' of unlicensed software or the downloading of content like journal articles or video entertainment may be more tolerated, since individuals and corporations often cannot afford to pay the fees associated with acquiring these goods legally. Here, they may argue that it is a matter of justice and equity. It is not fair that a scientist should miss out on reading about the latest biology or chemistry advances just because his university is poor, and thus he will perhaps ask a colleague in a wealthier university to share a copy of an article with him. The wealthier colleague, in turn, may view his act as one of benevolence and sharing, rather than a copyright violation.

Mancic (2010) makes a similar argument, asking us to consider the case of the virtuous or altruistic pirate. He argues that often "cyberpirates do much better to the world than copyright or patent holders," arguing that if anyone is immoral, it's the people who refuse to share lifesaving information. The author, a Serbian citizen, writes that many people today are unable to buy a book they need for improving their surgery skills, or purchase some software which might help a company improve its business and employ more people. This is the place where certain people, called "pirates" step in. In his work, he distinguishes between three kinds of pirates: those whose motives are purely to make a profit through selling counterfeit goods or information; those who want to disrupt the system for political or criminal ends, such as terrorism; and those who 'pirate' out of compassion, such as wanting to make medical information or proprietary information used to manufacture lifesaving devices available to all who need this information or device. Here, he describes their activity as a form of altruism since they are simply wishing to help the less fortunate. His argument thus forces us to consider the matter of intent.

The utilitarian perspective

Clearly, the easiest ethical argument to formulate in relation to intellectual property violations is that of utilitarian consequentialism. Here one simply needs to argue that any gains which the individual accrues through piracy are outweighed by the damage to the collective which ensues. As Akman and Mishra (2009) write, piracy results in economic losses to the producers of cultural and business products, like software.

In addition, crimes like intellectual property theft and plagiarism of one's ideas disincentivize employees and corporations whose job it may be to make new discoveries and knowledge. Czarnitzki et al. (2015) describe how often many firms will need to cooperate to bring a new product to market. However, they argue, if you cannot trust that your partners will play fairly and that your rights will be protected, you face a higher degree of risk; that is, there is less guarantee that you will receive the payoff you are expecting, including the profits from research and development. They note that in nations which do not have a strong tradition of upholding intellectual property rights, firms worry about whether they will get a patent recognizing their right to own a particular idea; the scope of the patent they may receive; how long the patent might be good for, and how much the new knowledge is worth and how it might potentially be used (Czarnitzki et al., 2015, 185). Czarnitzki et al. argue that stable intellectual property regimes help all players to create and enjoy trust with one another, better enabling them to cooperate and share information.

Nasheri argues on behalf of copyright, noting that "industrial property rights make it possible for the creators of innovations (goods, processes, apparatus, etc.) to establish themselves more readily, to penetrate new markets with a minimum of risk and to amortize the investments made in the research that led to innovations in the first place" (2005, 12).

Here the good to be secured is free trade and the capitalist model of profitability. Intellectual property restriction is seen as a necessary cost in order to realize these goals – including the patriotic goals of the United States, related to national security.

Furthermore, a consequentialist argument would note that intellectual property theft ends up costing those consumers who purchase the product more money, since prices may be raised to cover losses. More specifically, we can think of those who profit from a good without paying for it as 'free riders.' In viewing a movie without helping to fund its production through purchasing a ticket, or using software without helping to fund research and development through purchase or subscription, nonpaying users harm not only the producers of the good, but also those other individuals or groups who paid for the good. Theft raises the price of a good for legitimate users, and also may hamper research and development efforts leading to a better product in the future.

In addition, Schakelford (2016) points out that cyberattacks aimed at securing accessing to intellectual property – including economic information and trade secrets – can be part of a larger strategy of acts short of warfare carried out by an

adversary – either a nonstate actor or a nation-state. He argues that intellectual property violations need to be taken seriously since it is not always obvious whether they are separate acts or part of such a larger strategy. In this case, the utilitarian argument is that 'an ounce of prevention is worth a pound of cure.' In other words, it is better for nations to act preemptively to combat intellectual privacy violations before they become more dangerous and harder to combat in the future.

However, one can also make a utilitarian argument against copyright protection. In this view, if we view creativity as a deterministic process, in which new ideas are constantly created and old ones are constantly modified – in order to produce the most social goods for everyone in society – then notions like copyright and fair use may be seen as an unfair barrier or impediment to this process. They keep new content from being created which is of benefit to all in society. Any damages to the ownership and reputation of the original creator are therefore seen as a cost which is worth absorbing.

Indeed, many practitioners today are highly supportive of practices in which **open source code** is shared among programmers without charge or even a need to seek permission. Even the US government has frequently utilized open source code in configuring websites and programs used by the federal government. Here, federal government procurement officials note that it is unreasonably expensive and wasteful to create new snippets of code from scratch (to "reinvent the wheel") when existing programs already solve technological problems, including those faced by the federal government. They note as well that the government acquisition process for hiring contractors and writing new programs can be bureaucratic, slow and unwieldy. In addition, ideally all federal government agencies and programs would be interoperable, able to run together and communicate. This is more likely to happen with open source code than it is from practices where all agencies write their own code. Thus, many analysts see the practice of utilizing open source code as efficient and logical. Under the Obama Administration, the Second Open Government National Action Plan sought to establish a norm that whenever possible, government agencies should '**default to open source**' (Bohannon, 2016). Today, government agencies are encouraged to practice technology neutrality, meaning that the government should analyze several alternatives when solving a problem, including the use of proprietary, open source and mixed source technologies (Bohannon, 2011).

Box 6.4 Application: the ethics of spam

Spam is defined as e-mails (and increasingly texts) which are unsolicited by the user, and which typically advertise a product or service. They are messages which are sent in bulk, not to a specific user but to a batch of users who may number in the thousands or even the millions.

Spam is annoying for sure, but is it unethical? Spinello (1999) suggests that sending spam e-mails is unethical for several reasons. While technically spam is a form of free speech – which is a right protected by the US Constitution – spam is not economically free. Instead, a situation exists where a spammer can send as many bulk or junk e-mails as he or she wishes without paying any costs while the recipient of the e-mail is charged. In this way, it's like sending a package "postage due" where the receiver pays the postage costs.

Spinello notes that the recipient pays several costs. If he is in a nation where he must pay for connection time to the internet by number of e-mails received, or number of minutes connected, then he is being asked to pay for something that he didn't request and doesn't want. If the e-mails are copied onto his home computer, then his disc space is being wasted. Lots of spam e-mails can also slow down one's computer connection, creating costs for other users whose own downloads will be slower. Spam e-mail also creates costs for internet service providers. Their systems are slowed down, and they may have to pay for additional storage or maintenance to cope with large amounts of spam. These costs are again passed on to the consumer. Economists refer to these costs which are borne by others as externalities. Other anti-spam activists have described spam as similar to pollution, arguing that it amounts to putting large amounts of garbage in someone else's space and as a result, robbing every one of their ability to enjoy the space.

Increasingly, spamming is being used as a delivery vehicle for other types of dangerous cyberweapons. A spam attack may involve utilizing junk e-mails as a way of delivering malware, spyware, viruses and Trojans. Spam and junk e-mail may also be used as part of a phishing scheme.

The 2003 **United States Can-Spam Act** made the sending of spam illegal, allowing a fine of up to 11,000 dollars per e-mail sent to be levied. It also required that spammers provide a physical postal address to recipients so that they could contact the sender. However, despite this legislation, spam is still a

persistent problem on the internet. We may think of the case of spam as another area where there is not a clear or acceptable norm against spamming.

Nonetheless, many professional organizations concerned with computer ethics have inserted language into their codes of ethics and codes of conduct addressing this problem. The SEO Toolset Code of Ethics and the SCRUM Code of Ethics include an explicit prohibition against the use of spamming tactics.

Source

Spinello, Richard. 1999. "Ethical Reflections on the Problem of Spam." *Ethics and Information Technology* 1: 185–191.

The deontological lens

As noted in Chapter 2, deontologists search for a categorical imperative, or a rule which could be applied in all situations. In his work, Spinello (2003, 17–19) argues that you could show that cyberpirates are immoral if their mottos cannot pass test of categorical imperative. He states that the categorical imperative would be: it is allowed for any of us to copy and distribute information belonging to someone else, without the author's permission.

Deontological ethics also asks us to adopt the principle of reciprocity, in asking whether I myself would accept the action being suggested if I were not the actor but the person acted upon in the scenario. A deontological argument in favor of intellectual property laws would focus on those who would be harmed if everyone felt free to engage in intellectual property theft. Here one can build on the Hegelian argument that personal or private property is a means of personal freedom and self-expression (Himma, 2011). Hegel felt that people should have a right to own things since this allowed them to experience meaningful lives. Private property was thus a way to experience human flourishing. Thus, one can argue, individuals whose work is taken from them and used or misused by others will have been robbed of something valuable which decreases their quality of life and Tavani (2005) says because I would feel bad if my information was 'stolen', I should not be in favor of stealing anyone else's. In his work, Dames (2009) quotes Vice President Joe Biden's address to the Motion Picture Association of America in 2009. In this address, he

stated that piracy is "pure theft, stolen from the artists and quite frankly from the American people as consequence of loss of jobs and as a consequence of loss of income." And the Business Software Alliance describes it as a theft, not of an object, but as stealing from original creators who lose the ability to be fairly compensated for their work (Business Software Alliance, No date).

But like utilitarian and virtue ethics lenses, the deontological lens can also be used in two ways – both to condemn and defend piracy. In Chapter 2, we also considered the thought of John Rawls, who argued in favor of justice and equity. Rawls stated that the most moral solution to a problem was one which levied the least penalties on the most disenfranchised group. He recommended making decisions through the veil of ignorance, in which one did not know what one's role or position in a given scenario was. If we adopt the veil of ignorance, then we might view ourselves not as the software developer but as the poverty stricken individual in the developing world who might never be able to 'legally' afford a subscription to an online medical journal or access to a library database, but who nonetheless would profit greatly from being granted such access. In this situation, one might argue that the most just or equitable action would be to look the other way if one suspected that unauthorized access was taking place, rather than seeking to rigorously root out and punish all cases of unauthorized access or use (Himma, 2011).

In order to create an equitable and just internet, then, these analysts argue that everyone should be able to access the same information online without worrying about paywalls or fees, since it makes little sense to talk about a right to information in cyberspace if many users cannot afford to access that information. Here one can argue that everyone has the right to inform themselves from credible sources, particularly in a democratic society, and that those who seek to regulate cyberspace should focus on making sure that everyone has access to more information rather than less.

To bolster this point, we might consider the example of the Socially Awkward Penguin meme. As Dewey (2015) notes, the image of the Socially Awkward Penguin was originally from a photo taken by a National Geographic photographer. The image is owned by the National Geographic Society and is for sale, via a licensing agreement with Getty Images. Since the advent of the popular meme, Getty Images has contacted many bloggers and small media outlines demanding payment for their use of the image. Dewey (2015) describes the issue as one of equity or justice, noting that small bloggers who cannot afford a 900-dollar licensing

fee are thus able to exercise their own creativity or contribute as equal partners to the creative process taking place in social media. She asks:

> Is it silly? Yes. It's a talking penguin. But it's also the cornerstone of a thriving mashup culture, one that transforms even the staidest nature photography into commentaries on politics, technology and modern life (Dewey, 2015).

Adam Moore also calls our attention to inequities – in this case, the privilege which larger actors like states and corporations have in cyberspace, compared to individual users and small groups. He argues that states and corporations therefore use copyright and intellectual property laws in order to control who can access and consume information through erecting paywalls and firewalls. For this reason, Libertarians (those who believe that government and regulation should play only a limited role in public life) often refute conventional notions of intellectual ownership – seeing these claims as a threat to individual liberty and rights (Varelius, 2014, 300).

Today, much online piracy takes place through the use of peer-to-peer networks, in which users are able to exchange files directly with one another, through directly accessing each other's hard drives, sometimes mediated through a server which may be located in a country with weak copyright restrictions. Some well-known **peer-to-peer networks** which have existed include Napster, Gnutella and Pirate Bay (Mittal, 2004). While corporations argue that such technologies allow for the large-scale theft of intellectual property including music and movies, some activists claim that they provide an important service through allowing people to subvert government and corporate authority by connecting them directly to each other. They thus frame their activities as rooted in civil disobedience, in which activists organize to oppose laws which they view as unjust and inequitable.

In his work, Mancic (2010) offers a more nuanced argument. He says you cannot categorically say that piracy is always wrong, or always admirable. Instead, he argues for case-specific ethics – arguing that sharing information about how to make a bomb would be wrong, but that sharing information which heart surgeons in developing countries can use to save lives is not. That is, he argues, the violation depends not on the action but on the nature of the content being pirated.

Arguments against intellectual property protection

Despite the compelling arguments made here – in regard to the rights of authors, producers and other consumers – today there is not a strong international normative and ethical commitment to the preservation of individual intellectual property rights. But why has it been so difficult to establish an international consensus in regard to the matter of intellectual property?

There are actually several arguments which those who oppose copyright protections have made – in addition to the ones explored here using the three lenses. Many of these arguments cross disciplines, borrowing not only from moral philosophy but also from literary theory and political theory. They point to arguments made by theorists who borrow from literary theory and the work of Francois Foucault in particular. In the 1970's, Foucault and others made a splash in literary criticism circles by suggesting that a piece of literature may have no exact, foundational meaning. The story might not be 'about' only one thing, they argued, but rather would be interpreted differently in different cultures, in different languages, and in different eras. As a result, Foucault argued that one could not rightly speak of only one 'author' of a particular work, since the act of reading involved labor both on the part of the writer and the reader, and that finished product, the making of meaning, was actually a collaborative effort by both participants (Himma, 2011).

This argument, the **authorship argument**, is used today by many of those who defend people's rights to re-use and recycle content which they find on the internet, modifying it to make memes and mash-ups. Chabonpin calls our attention to hip hop as a unique cultural artifact which draws upon a tradition of improvisation. He argues that this music style in particular is not well suited to be judged by dominant Western intellectual tradition and understandings of property (2012, 620). Thus, these analysts come down on the 'unique' side of the uniqueness debate, arguing that a new environment (the internet) has created new art forms (like memes and mash-ups) which cannot be treated either ethically or legally in the same way which traditional forms of property and property ownership have been treated.

Two particular cultural products which help to illustrate this point are the meme and the mash-up. The term **meme** was first used by Richard Dawkins in 1976 in his book *The Selfish Gene*. The meme is a unit of cultural material that spreads virally, passed from person to person via electronic means. It includes phrases, audio and video files, photos and images (Whatis.com). As it spreads, it may be modified or changed. For example, one can find pictures online of former President George Bush falling off a Segway riding vehicle in 2003. The image was passed around the

internet, with later users adding additional photos of individuals riding the vehicle including a chimpanzee and Barbara Bush (whatis.com).

The term **mash-up** is more commonly applied to audio productions, where, for example, a rap artist might 'sample' a track, using snippets and pieces of recognizable older songs as a background or rhythmic accompaniment to a rap. These snippets might be altered from the original by altering tempo, key signature or instrumentation. As Rosen writing on the *Yale Law and Technology blog*, explains:

> Mashup artists can provide critical commentary on those works, expressing their own perspectives on the songs being utilized. As a result, mash-up can yield the sort of first amendment expressions that the fair use doctrine was meant to protect.
>
> (2010, no pagination)

The terms remix and sampling may also be applied to this type of 'borrowing' (Chabonpin, 2012). Here, Lankshear and Knobel (2007) note that writing satires and reintroducing old themes and content in new and clever ways is not, however, actually a new practice. Indeed, they point to the English playwright William Shakespeare (1564–1616) as a master of this type of craft.

As these examples show, producers and users (or re-users) may disagree about what content can be owned legally, what content can be shared, as well as the point at which a drawing or tune can be said to belong to the public. As noted earlier in this chapter, a copyright is often awarded for a finite period of time, and it may also expire when the original work's author dies. In this instance, the work then reverts to the **public domain**, where the term public domain refers to "non-copyrighted intellectual property (such as computer software, designs, literature, lyrics, music) that can be copied and freely distributed (but not sold) by anyone without payment or permission" (businessdictionary.com, No date). Items which reside in the public domain may be freely used, borrowed and modified.

Today, this matter of borrowing and re-using is even more complicated since the internet is often described and perceived as a sharing culture. Programmers may produce and use **open-source code**, which may be written collaboratively by multiple producers, and which is produced without a copyright, so that others may utilize, share and improve the code. Similarly, artists may produce visual content

under a **Creative Commons license**, making it clear that their work is available for borrowing, changing or reusing.

Indeed, earlier in this text we referenced Koller on 'conventional morality'. He argued that laws often align with what people think of as wrong or immoral behavior, but that laws may be difficult to enforce when they do not align with people's norms and ideas. And it appears that not everyone feels that borrowing or sampling content is inherently ethically wrong, nor that it should be unlawful. This helps to explain why it has been so difficult to enforce copyright laws both domestically and internationally. Noted legal scholar Lawrence Lessig has weighed in on the uniqueness debate, in arguing that technological changes have necessitated new thinking about what it means to own a piece of intellectual property. He argues that we are creating new forms of writing and literacy that may include the ability to use and manipulate various types of files – audio, video – and to put them together in new ways. He calls our attention to practices like writing fanfiction in which an author might conceive of new adventures and new types of adventures for characters who have already appeared in published literature written by another author (including retellings of stories related to *Breaking Dawn, Harry Potter*, or *Fifty Shades of Grey*) and Photo-shopping images and posting them.

Lessig describes the old model as one in which culture is "read only," while new culture is one in which readers can speak back and alter texts – so that it is read/write (refers to settings on old floppy discs where one could format them so that they could only be written to, versus where they could be altered). Lessig argued that traditional copyright laws choked and blocked these types of creative processes since its default is 'all rights reserved.' He argues today for the establishment of a creative commons in which materials are freely available for borrowing and re-use and where the default is that you can use something, rather than that you cannot (Beckedahl and Weitzmann, 2012).

Building an international norm against piracy

As the arguments above show, there is not always a consensus regarding the legality or ethics of intellectual property theft in cyberspace. For this reason, some analysts are pessimistic about the possibility of establishing any sort of binding international legislation which would create a uniform acceptance of the norm that intellectual property law still holds in cyberspace. In explaining why that is difficult, analysts argue that not all cultures share the same understandings of property, since

these understandings come from a Western legal and ethical tradition. Others argue that young people in particular may not share outdated or antiquated notions of ownership, having been raised with the sharing culture of the internet. Others point out that psychologically, people may simply not think the same way about 'stealing' a computer file or image as they do about 'stealing' a physical object from a friend's home. We will consider each of these arguments in detail.

In recent years, several analysts have argued that the norms and ethics governing intellectual property are not actually international. Rather, they say, these ethics are based on understandings which evolved in Western democratic societies over hundreds of years, including the notion of individual political rights, including property rights (Ocko, 2013). Therefore, imposing these laws on non-Western (and nondemocratic) societies through international agreements may not succeed because the underlying values and ethics behind these laws may be meaningless to these people in other societies.

In addition, some nations simply do not have a long history of respecting intellectual property, and may not have the same reverence or respect for intellectual (or personal) property in their more collectivist culture. Here, Akman and Mishra (2009) argue that people's ethical decision making is a function of their knowledge of ethics, and exposure to ethical principles, including those of their profession; the norms of their workplace and the expectations of their workplace and their own personal code. They argue that often an employee may be pressured by his own organization to look the other way in regard to ethical violations of intellectual property – such as being asked to install unlicensed software on his computer. A company may have made a decision to cut costs by disregarding intellectual property regimes and the employee may be pressured to comply. In their study of IP issues in Turkey, they found evidence of IP violations in both government and corporate organizations. The question thus remains as to whether and how successful an anti-piracy norm might be given these cultural differences.

The International Center for Information Ethics, headquartered in Switzerland, describes three different orientations towards information production: First, they describe a European approach which stresses the notion of authorship of a cultural product in which the author has a right to say how his or her information will be shared or used – and reused (for example, whether or not a piece of classical music should be used to accompany a commercial for fast food). Here, the primary concern is preserving the integrity of the author's artistic vision. Next, they identify an Anglo-American approach which focuses less on artistic integrity and more on

the economic rights for the person whose 'property' the creation is. Finally, they point to an Asian tradition which may view copying as a sign of respect for a master (International Center for Information Ethics, 2017).

It is widely known that electronic piracy is a global problem, particularly among young people. Up to 47 percent of Americans admit to having engaged in piracy at one time, and of US college students who admit to engaging in the activity routinely, most have an average of up to 800 illegally downloaded songs (Moustis and Root, 2016). Some analysts suggest that young people in particular simply do not subscribe to outdated notions of privacy and private property, including the private ownership of ideas. Unfortunately, studies of young people in particular indicate that they often do not regard IP theft as an ethical issue (Hu et al., 2012, 127). Hu et al. indicate that people didn't believe that downloading music illegally, for example, meant that you weren't a good person. They saw the issue as unrelated to questions about their moral character. And Panas and Ninni (2011, 485) suggest that students do not engage in long, protracted moral searching before engaging in piracy. Instead, their research shows that people tend to put their knowledge about piracy into practice almost immediately after learning the techniques, with over 50 percent doing so less than a week after they acquired the know-how.

Hardy et al. (2013, 1) suggest that a major factor influencing students' decisions to download music may be the fact that they perceive a great distance between themselves and their victims. Stealing from an anonymous corporation which might then pass the costs on to a recording artist can feel very different from stealing a physical object from a storeowner whom you might see or have a relationship with. In addition, they suggest that students don't perceive their behavior as risky since they think that the likelihood of being caught is quite low. In their research, they have also discovered that students who download music often go on to help others to do so by sharing their knowledge and expertise. They found that 80 percent of students downloading music received help from a friend or classmate to do so, while the remaining students looked up the techniques online (Panas and Ninni, 2011, 845). In addition, Hardy et al. (2013) suggest that those who engage in large-scale piracy may be psychologically different from other consumers. They describe how some individuals derive a sense of psychological excitement from participating in risky behaviors (the so-called "shoplifter's high"). Such individuals frequently display less fear of getting caught and less respect for the rules.

And while advertising campaigns against piracy make the case that this activity is illegally and also morally wrong, not everyone agrees. Indeed, some individuals and

groups claim that piracy is an acceptable moral or ethical choice. Individuals making this claim may refer to piracy as a victimless crime or they may argue that stealing from a corporation is different from stealing from an individual since 'it's only a corporation'. In a blog post called "Why I Love Shoplifting from Big Corporations," Anonymous makes a Marxist argument, stating that he does not agree with an economic system which permits individuals or corporate entities to own goods which others may have need of. He feels that it is fundamentally unjust for a large corporation to make millions of dollars while there are others who are poor in that same country. He thus views his decision to enter a store and take products there as a way of voicing his objection to what he sees as an immoral economic decision (Anonymous, No date, 1). Babin and Griffin (1995) note that older Americans may also make ethical arguments in, for example, objecting to a company which they perceive as setting its prices too high and making goods unaffordable for older Americans.

Gatig and Russell (2015) however dispute the finding that millennials and digital natives think differently about copyright and intellectual property due to exposure to digital remixing and similar practices. They also dispute the finding that other cultures may have a significantly different view of copyright and intellectual property.

Companies that have been victimized by electronic piracy – including the Recording Industry Association of America, often mount large-scale advertising campaigns aimed at changing the behaviors and thought patterns of would-be pirates. Here, they aim at changing the narrative or the story that people tell themselves and others about piracy – that it is a harmless activity. Instead, they aim to establish a norm that recognizes it as an unethical and criminal activity. These campaigns often have a simple message, that piracy is a form of theft and that it is not actually a victimless crime. Indeed, some estimates are that a recording artist or studio could lose up to 20 percent of their projected profit on a project as a result of online piracy (Panas and Ninni, 2011, 836).

Commercials and educational materials aim at teaching the public about the legal penalties associated with online piracy, which can include fines and even imprisonment. Would-be pirates are encouraged to think about both the risks and the consequences of their actions. However, despite the budget for advertising of this type, the scope of the crime is actually growing. It appears that there is not a strong or well-established **norm** against engaging in piracy, either in the US or elsewhere in the world.

Legal measures against piracy

Furthermore, some scholars (Hardy et al., 2013) wonder if education campaigns are really effective. They suggest that measures like increased monitoring and penalties are likely to be far more effective in preventing piracy than are measures aimed at appealing to citizens regarding the morality of their activity. This is because while individuals may have strong individual ideals, they are often influenced by their environments. In the case of piracy, individuals may think that the activity is wrong but they may still be influenced by their peers who engage in the activity, as well as their beliefs that the activity is so widespread and common that there is little to be gained by opposing it (Hardy et al., 2013, 3). Furthermore if, as argued above, ideas like the Western intellectual tradition of private property have emerged over hundreds of years, then some doubt whether a similar understanding can be replicated in other cultures merely through education, particularly in the space of a few years.

Nonetheless, many nations do have strong laws prohibiting the theft of intellectual property in cyberspace. Currently US laws are some of strongest in world. They include the **Copyright Act of 1976**, the **Communications Act of 1984**, and **the Piracy Deterrence and Education Act of 2003**. In addition, the FBI has run sophisticated sting operations aimed at combatting and shutting down piracy (Nasheri, 2005).

International efforts have also been mounted, mainly through the **World Intellectual Property Organization (WIPO) of the United Nations**. The World Intellectual Property Organization Copyright Treaty and WIPO Performances and Phonograms Treaties are aimed at combatting piracy internationally as well as encouraging nations to enforce copyright rules within their own nations (Nasheri, 2005). WIPO also works to harmonize national intellectual property laws, as does the European Union Patent Office (Franklin, 2013).

In addition, the **International Federal of the Phonographic Industry (IFPI)** and the **International Anti-Counterfeiting Coalition (IACC)** work to represent the interests of companies concerned with intellectual property enforcement. The IACC puts out a list of nations which have been warned that they are not displaying a serious enough commitment to combatting piracy. Nations on this list include Canada, India, Malaysia, Mexico, Philippines, Poland, Russia, Japan, Panama, Romania and Turkey (Nasheri, 2005, 30). The IACC issues a list of Priority Foreign

countries – including Ukraine, China, and Paraguay – which are judged as having allowed particularly egregious copyright violations.

Legislation	*Date*	*Provisions*
World Intellectual Property Organization (WIPO) Broadcasting Treaty	**2004**	Afford broadcasters economic rights, akin to copyright protection, in their broadcasts for up to 50 years. Allows broadcasters to claim rights to their signals, as well as content like webcasts, produced by other individuals, in their signals as well as rights to the creative content produced by other individuals.
Anti-Counterfeiting Trade Agreement (ACTA)	**November 2010**	Designed to combat the production and distribution of counterfeited goods and the infringement of copyrighted works.
PRO-IP Act (Amendment to the U.S. Copyright Act)	**2008**	Strengthens protection for rights holders and increases penalties for counterfeiting and infringement of intellectual property rights. Allows President to appoint an Intellectual Property Enforcement Coordinator ("IPEC") to develop a Joint Strategic Plan to help combat infringement and counterfeiting of intellectual property in the United States and in foreign countries.
Stop Online Piracy Act (SOPA)	**2012**	Aimed at reaching foreign websites dedicated to providing illegal content. The various bills defined different techniques for blocking 'blacklisted' sites. Each would interfere with the internet's domain name system. SOPA would also allow rights holders to force payment processors to cut off payments and advertising networks to cut ties with a site simply by sending a notice. Defeated by domestic US lobbying efforts in 2012.

Figure 6.1 Select US and international legislative initiatives to combat piracy

Practitioners who work in cybersecurity are thus advised to pay close attention to the laws governing intellectual property, and to make sure that they are observing these laws in situations where they may borrow code, content or images. They should not assume that all content can be borrowed and need to pay attention to the type of license which is associated with particular content – which will specify whether and under what conditions content may be borrowed, modified and shared.

Chapter summary

- The right to claim ownership of an idea is not new. However, new technological developments which make the reproduction of information (in written, auditory and visual forms) easier have created new issues in IP.
- It has been difficult to establish a consensus regarding IP norms because of the architecture of the internet itself, a traditional 'pro sharing' attitude on the part of many internet users, and the fact that many different cultures with different traditions use the internet.
- Utilitarian arguments focus on the economic and intellectual costs of IP theft – arguing that it makes it harder to make progress in science if inventors can't count on being compensated for their advances.
- Virtue ethics arguments recommend that users cultivate the virtues of restraint and respect for others, even in situations where it seems easy to engage in IP Theft.
- Deontological arguments ask would-be IP thieves to consider the perspective of the creators of new technologies.

Discussion questions

1 Do you feel that existing institutions should adapt to take into account large numbers of non-Western programmers and the fact that they might have different ways of "doing" IP? Are you optimistic about the creation of a universal norm against IP theft in the future? Why or why not?

2 Do you feel that software should be "classified" if it is used in government agencies?

Should programmers working for the government be prohibited from using open source code? Why or why not? What are some arguments for and against?

3 What, if anything, can be done to make individuals more aware of the moral and ethical consequences of piracy?

4 Compare and contrast physical and intellectual property. Are the arguments about ownership, theft and sharing the same or different? Do you regard

intellectual property as the same as stealing a physical object? Why or why not?

Recommended resources

GNU.org . No Date. "What Is Free Software?" Available at gnu.org/philosophy/free-sw.html

Hyde, Lewis. 2005. *Frames From the Framers: How America's Revolutionaries Imagined Intellectual Property*. Cambridge, MA: Berkman Klein Center for Internet and Society. Available at https://cyber.harvard.edu/publications/2006/Frames_from_the_Framers.html

Scherer, Dana A. 2016. "Money for Something: Music Licensing in the Twenty-First Century." January 29. Washington, DC: Congressional Research Service.

Schwartz, Aaron. 2008. "Guerilla Open Access Manifesto." Available at https://archive.org/stream/GuerillaOpenAccessManifesto/Goamjuly2008_djvu.txt. Accessed November 2, 2016.

United States Office of Management and Budget. 2016. "Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software." August 8. Available at www.actiac.org/federal-source-code-policy-achieving-efficiency-transparency-and-innovation-through-reusable-and. Accessed February 2, 2017.

Students may also wish to visit the website for the Recording Industry Association of America (RIAA.org) to read their materials about infringement, licensing and piracy.

Chapter 6 sources

Akman, Ibrahim, and Mishra, Alok. 2009. "Ethical Behavior Issues in Software Use: An Analysis of Public and Private Sectors." *Computers in Human Behavior* 25(6): 1251–1257.

Anonymous. No Date. "Why I Love Shoplifting From Major Corporations." *Looking Glass News*. Available at www.lookingglassnews.org. Accessed April 28, 2016.

Babin, Barry, and Griffin, Mitch. 1995. "A Closer Look at the Influence of Age on Consumer Ethics." *Advances in Consumer Research* 22: 668–673.

Beckedahl, Markus, and Weitzmann, John. 2012. "Ten Years of Creative Commons: An Interview With Co-founder Lawrence Lessig." *Governance Across Borders*. December 18. Available at https://governancexborders.com/2012/12/18/10-years-of-creative-commons-an-interview-with-co-founder-lawrence-lessig/. Accessed March 1, 2017.

Bohannon, Mark. 2011. "US Administration's 'Technology Neutrality' Announcement Welcome News." *Opensource.com*. January 10. Available at https://opensource.com/government/11/1/us-administrations-technology-neutrality-announcement-welcome-news. Accessed February 1, 2017.

Bohannon, Mark. 2016. "A Fresh Look at the US Draft Policy on Federal Sourcing." April 28. Available at https://opensource.com/government/16/4/draft-policy-federal-sourcing. Accessed February 15, 2017.

Business Dictionary.com. No Date. "What Is Public Domain?" Available at www.businessdictionary.com/definition/public-domain.html. Accessed May 2, 2017.

Business Software Alliance. No Date. "Software Piracy and the Law." Available at www.bsa.org/anti-piracy/tools-page/software-piracy-and-the-law/?sc_lang=en_US. Accessed February 1, 2017.

Chabonpin, Kim D. 2012. "Legal Writing, the Remix: Plagiarism and Hip Hop Ethics." *Mercer Law Review* 63: 597–638.

Chien, Shish-Chien. 2014. "Cultural Constructions of Plagiarism in Student Writing: Teachers' Perceptions and Responses." *Research in the Teaching of English* 49(2): 120.

Czarnitzki, Dirk, Hussinger, Katrin, and Schneider, Cedric. 2015. "R&D Collaboration With Uncertain Intellectual Property Rights." *Review of Industrial Organization* 46(2): 183–204.

Dames, K. Matthew. 2009. "Why the Frame of Piracy Matters." *Information Today, Inc.* June. Available at www.infotoday.com. Accessed January 1, 2016.

Dewey, Caitlin. 2015. "How Copyright Is Killing Your Favorite Memes." *Washington Post.* September 8. Available at https://www.washingtonpost.com/news/the-intersect/wp/2015/09/08/how-copyright-is-killing-your-favorite-memes/?utm_term=.60f6e4182496. Accessed November 12, 2016.

Franklin, Jonathan. 2013. *International Intellectual Property Law.* February 8. Washington, DC: American Society of International Law. Available at www.asil.org/sites/default/files/ERG_IP.pdf. Accessed December 10, 2016.

Hardy, Wojciech, Krawczyk, Michael, and Tyrowicz, Joanna. 2013. "Why Is Online Piracy Ethically Different From Theft? A Vignette Experiment." *Working Papers No. 24.* Warsaw, Poland: University of Warsaw Faculty of Economic Sciences.

Himma, Kenneth. 2011. "Richard Spinello and Maria Bottis: Understanding the Debate on the Legal Protection of Moral Intellectual Property Interests: Review Essay of *A Defense of Intellectual Property Rights*." *Ethics of Information Technology* 13: 283–288.

Himma, Kenneth. 2013. "The Legitimacy of Protecting Intellectual Property Rights." *Journal of Information, Communication and Ethics in Society* 11(4): 210–232.

Hockenberry, Benjamin. 2013. *The Guerilla Open Access Manifesto: Aaron Swartz, Open Access and the Sharing Imperative.* November 21. Rochester, NY: St. John Fisher College Fisher Digital Publications. Available at http://fisherpub.sjfc.edu/library-Pub. Accessed December 2, 2016.

Hu, Qing, Zhang, Chenghong, and Xu, Zhengchaun. 2012. "Moral Beliefs, Self-Control and Sports: Effective Antidotes to the Youth Computer Hacking Epidemic." 45th Hawaii International Conference on System Sciences. Available at http://ieeexplore.ieee.org/document/6149196/. Accessed April 11, 2017.

International Center for Information Ethics. 2017. "The Field." *International Review of Information Ethics.* Available at http://icie.zkm.de/research. Accessed February 1, 2017.

Lankshear, Colin, and Knobel, Michele. 2007. "Digital Remix: The Art and Craft of Endless Hybridization." Keynote presented to the International Reading Association Pre-Conference Institute "Using Technology to Develop and Extend the Boundaries of Literacy", Toronto. May 13.

Lindsay, Joel. 2014. "Hacked: Medtronic, Boston Scientific, St. Jude Networks Suffer Cybersecurity Breaches." *Med Device Online*, February 11. Available at

www.meddeviceonline.com/doc/hacked-medtronic-boston-scientific-st-jude-networks-suffer-cybersecurity-breaches-0001. Accessed May 2, 2017.

Maisel, Yoni. No Date. "A Call for Open Access to Medical Journals for Rare Disease 'Detective' Patients and Advocates." *Global Genes.org*. Available at https://globalgenes.org/raredaily/a-call-for-. Accessed December 4, 2016.

Mancic, Zeljko. 2010. "Cyberpiracy and Morality: Some Utilitarian and Deontological Challenges." *Filozofija I Drustvo* 3: 103–117.

Mittal, Raman. 2004. "P2P Networks: Online Piracy of Music, Films and Computer Software." *Journal of Intellectual Property Rights* 9(5): 440–461.

Moore, Adam, and Unsworth, Kristene. 2005. "Information Ethics: An Introduction." In Adam Moore, ed. *Information Ethics: Privacy, Property and Power*. Seattle, WA: University of Washington Press.

Moustis, John Jr. and Root, Austin. 2016. "Curing Americans Kleptomania: An Empirical Study on the Effects of Music Streaming Services on Piracy in Undergraduate Students." *Timelytech.com*. Available at http://illinoisjltp.com/timelytech/curing-americans-kleptomania-an-empirical-study-on-the-effects-of-music-streaming-services-on-piracy-in-undergraduate-students-2/. Accessed January 2, 2017.

Nasheri, Hedi. 2005. Addressing Global Scope of Intellectual Property Law (final report). NIJ, The International Center, (US Department of Justice). Available at: https://www.ncjrs.gov/pdffiles1/nij/grants/208384.pdf

No Author. 2014. "Hackers Charged in Software Theft From US Army, Others." *Phys Org*, September 30. Available at https://phys.org/news/2014-09/hackers-software-theft-army.html. Accessed May 10, 2017.

Ocko, Jonathan. 2013. "Copying Culture and Control: Chinese Intellectual Property Law in Historic Context." *Yale Journal of Law and Humanities* 8(2). Available at http://digitalcommons.law.yale.edu/yjlh/vol8/iss2/10. Accessed December 11, 2016.

Panas, Epaminondas and Ninni, Vassilia. 2011. "Ethical Decision-Making in Electronic Piracy: An Explanatory Model Based on the Diffusion of Innovation Theory and Theory of Planned Behavior." *International Journal of Cyber Criminology* 5(2): 836–859.

Rosen, Brad Evan. 2010. "Mashup: A Fair Use Defense – by 'Ryan B'." *Yale Law Tech blog*. February 4. Available at https://yalelawtech.org/2010/02/04/mashup-a-fair-use-defense/. Accessed May 2, 2017.

Schakelford, Scott. 2016. "Protecting Intellectual Property and Privacy in the Digital Age: The Use of National Cybersecurity Strategies to Mitigate Cyber Risk." *Chapman Law Review*. Available at www.chapmanlawreview.com/wp-content/uploads/2016/09/19-2_Shackelford.pdf. Accessed March 12, 2017.

Schultz, Abby. 2016. "SAT Integrity Falls Victim to China Cheating Scandal." *Barron's*. January 25. Available at www.barrons.com/articles/sat-integrity-falls-victim-to-china-cheating-scandal-1453713163. Accessed October 3, 2016.

Spinello, Richard A. 2003. *CyberEthics: Morality and Law in Cyberspace, 2nd Edition*. London: Jones and Bartlett Publishers International.

Spinello, Richard A., and Herman T. Tavani. 2005. "Intellectual Property Rights: From Theory to Practical Implementation" In Richard A. Spinello and Herman T. Tavani, eds. *Intellectual Property Rights in a Networked World: Theory & Practice*. New York: IGI Global: 1–6.

Tavani, Herman. 2005. "Locke, Intellectual Property Rights and the Information Commons." *Ethics and Information Technology* 7(2): 87–97.

United Nations Educational, Scientific and Cultural Organization. No Date. "What Is Piracy?" Available at http://portal.unesco.org/culture/en/ev.php-URL_ID=39397&URL_DO=DO_TOPIC&URL_SECTION=201.html. Accessed December 2, 2016.

United States Patent and Trademark Office. 2005. *Piracy of Intellectual Property: Statement of Stephen Pinkos, Deputy Undersecretary of Commerce for Intellectual Property*. Washington, DC: United States Patent and Trade Office. May 25.

Urban, Gregor. 2015. "Complicity in Cyberspace: Applying Doctrines of Accessorial Liability to Online Groups." In Russell G. Smith, Ray Chak-Chung Cheung, and Laurie Yiu-Lau, Chung, eds. *Cybercrime Risks and Responses: Eastern and Western Perspectives*. New York: Palgrave Macmillan: 194–206.

Varelius, Jukka. 2014. "Do Patents and Copyrights Give Their Holders Excessive Control Over the Material Property of Others?" *Ethics and Information Technology* 16(4): 299–305.

Volodzko, David. 2015. "China's Addiction to Counterfeiting." *The Diplomat*. October 17. Available at http://thediplomat.com/2015/10/chinas-addiction-to-counterfeiting/. Accessed February 2, 2016.

Walker, Danielle. 2015. "Man, Pleads Guilty to Intellectual Property Theft Conspiracy Impacting Microsoft, Other Firms." *SC Magazine*. April 2. Available

at www.scmagazine.com/hacking-ring-member-pleads-guilty-to-st. Accessed March 8, 2017.

7 The problem of cyberwarfare

Learning objectives

At the end of this chapter, students will be able to:

1. Summarize the argument for applying conventional ethics of armed conflict to cyberspace and the argument against doing so
2. Define major military concepts – including deterrence, active defense, and balance of power that have been applied to cyberspace
3. Point to emerging ethical issues in conflict in cyberspace, including issues related to agency, autonomy and responsibility
4. Distinguish between cyber conflict and cyber espionage and describe ethical issues related to both, as well as those reserved for one type of actions only

As we consider the ethical problem of cyberwarfare in this chapter, we can consider five real-life situations involving the use of cyberwarfare or response to cyberwarfare by a government, corporation or individual:

- In 2008, the Russian Federation intervened against the Republic of Georgia in what had begun as a territorial skirmish between Georgia and the breakaway republic of Abkhazia. In August, Russia invaded Georgia using a combination of conventional ground, air and naval troops, augmented by coordinated cyber-attacks. "Cyberwarriors" took down 54 Georgian websites used in communication, finance and government activities. The coordinated cyberattacks made conventional attacks more powerful and efficient since Georgia's troops and government were unable to implement a coordinated response due to problems with their technology (Hollis, 2011).
- In December 2016, Russian hackers carried out 6500 hack attacks against the Ukrainian finance and defense ministries. They also attacked the state treasury and the power grid in Kiev, Ukraine's largest city. Ukraine's president accused Russia of "waging a cyberwar against our country" (Zinets, 2016, 1).
- In November 2015, the international hacker group Anonymous declared "digital war on ISIS" after the radical terrorist group carried out an attack against a nightclub in Paris which resulted in the deaths of 130 people. In the following months, Anonymous members reported Twitter accounts of suspected ISIS terrorists and also hacked into and defaced

social media sites purported to belong to ISIS. Anonymous sought to destroy ISIS's credibility and recruitment power through tweeting (altered) pictures of known ISIS members engaging in actions like flying a rainbow flag in support of gay rights or engaging in bestiality (Colarik and Ball, 2016).

- In January 2015, US Federal Bureau of Investigation Director James Comey presented the results of his agency's investigation into the hacks on US-based entertainment company Sony Pictures. The hacks resulted in the public release of embarrassing e-mails and photos of US celebrities and executives. The group, calling itself "Guardians of Peace," was found to be linked to the North Korean government, and hacks were seen as retaliations for Sony's refusal to withdraw a satirical film which portrayed North Korea's leadership in a negative light (Haggard and Lindsay, 2015).
- In November 2016, two bills were introduced in the United States' legislature – the Election Infrastructure and Security Promotion Act of 2016 and the Election Integrity Act of 2016. Both bills would require the US Department of Homeland Security to designate voting machines used in US elections as critical infrastructure. With this designation, the Department of Homeland Security would assume responsibility for securing these systems for hacking or tampering by internal US or outside actors. This legislation was passed in response to allegations that Russian government hackers may have targeted voting machines in the United States, in order to sow suspicion among American voters regarding the validity of election results (Newman, 2016).

What do these activities have in common and how do they differ? Is each of these activities described above an act of cyberwarfare? Why or why not?

Defining cyberwarfare

We can begin our discussion by looking at the US military's definition of cyberwarfare. **Cyberwarfare** has been defined as:

> Warfare waged in space, including defending information and computer networks, deterring information attacks, as well as denying an adversary's ability to do the same. It can include offensive information operations mounted against an adversary.
>
> (Hildreth, 2001, 3)

Cyberwarfare is thus regarded as part of a larger set of operations known as warfare, with 'cyber' referring to the fact that specific actions are thus carried out through the use of cyberweapons or cyber activity. One can conduct cyberwarfare independently or as part of a larger strategy in which a nation uses both cyber and conventional weapons and tactics to achieve a target. In some instances, cyber warfare is seen as a **force multiplier**. A nation uses cybertactics – such as taking down an enemy's communications infrastructure – in order to install disorder within the adversary's military or general population, thus facilitating the carrying out of traditional conventional (or kinetic) attacks. Similarly, Brey (2007, 21) defines **information warfare** as "an

extension of ordinary warfare in which combatants use information and attacks on information and information systems as tools of warfare." Finally, Rowe (2009, 5) defines cyber conflict as "the use of computational technologies in cyberspace for malevolent and destructive purposes in order to impact, change or modify diplomatic and military interactions between entities." He describes cyberconflict as a foreign policy tool used by states or individuals against states.

Attacks using cybermeans can in some circumstances be regarded as **acts of war**. In the guidance developed for military officers, decision makers and military personnel, an act of war is defined as:

> An action by one country against another with an intention to provoke a **war** or an action that occurs during a declared **war** or armed conflict between military forces of any origin."
>
> (USlegal.com, No date)

The uniqueness debate: is cyberwar really war?

View one: conventional military ethics apply to cyberspace

As you may have noticed already, the ethical framework which we utilize in talking about cyberwarfare is different from the ethical frameworks which we have used to think about issues like secrecy, surveillance and piracy. This is because our theorizing about cyberwarfare has different roots than the ethical theories which we have examined in previous chapters of this text (Lucas, 2017). In our other chapters, we looked at ethics of privacy, surveillance and intellectual property through referring to the work of moral philosophers. However, much of the work in cyberwarfare ethics has been carried out not by academics – including those in philosophy – but by practitioners. Many of the leading thinkers about cyberwarfare ethics have been not moral philosophers but military ethicists. These individuals start with the assumption that there is little that is unique or new about cyberspace as a field of conflict. Rather, they argue that just as we (as individuals and an international community) have rules for what constitutes ethical behavior at sea, on land or in the air – based on the established understandings and traditions which are codified in the international Law of Armed Conflict (LOAC) – so can we create understandings about what constitutes ethical behavior in cyberspace using this same body of legal and ethical understandings.

In arguing for the 'portability' of these ethical understandings into the territory of cyberspace, Gary Solis quotes the 2011 United States International Strategy for Operating in Cyberspace, which states that:

> The development of norms for state conduct in cyberspace does not require a reinvention of customary international law, nor does it render existing international norms obsolete. Long-standing international norms guiding state behavior – in times of peace and conflict – also apply in cyberspace.
>
> (White House, 2011, 2)

Many analysts today refer to the **Tallinn Manual on the International Law Applicable to Cyber Warfare** in discussing the legality and ethics of acts of cyberwarfare by nations and nonstate actors. This document was authored between 2009 and 2013 in a series of meetings between members of the North Atlantic Treaty Organization (NATO). Some analysts, like Solis, feel that it represents an international consensus regarding what actions are and are not legal and ethical in the conduct of cyberwarfare.

In this ethical view, ethics and laws are very tightly linked. Although we stated previously (in Chapter 1) that law and ethics may overlap but that they do not always do so, most military ethicists do not make a sharp distinction between law and ethics when discussing war and conflict. This is because traditionally, international law including the **Law on Armed Conflict (LOAC**) and the **Geneva Convention**, has provided the basis for talking about ethics in conflict – including what specific acts are deemed lawful or unlawful. International law is written at the level of the state and provides guidance on actions which states may take in prosecuting or carrying out war. It deems some actions to be lawful and legal while others are not, based on a set of ethical principles known as Just War. The Geneva Convention provides for the rights and safety of those who are not or who are no longer engaged in war – including civilians and those who have been taken as prisoners of war. Although these legal understandings state what actions a state might rightfully and ethically take during combat, they are also translated on a national level into policy guidance for uniformed, professional soldiers. Thus, an individual, like a state, can be prosecuted for a war crime, if they are judged guilty of having violated international laws and norms through engaging in an activity like torture of a prisoner, or conducting military aggression against unarmed civilians. In the field of cyberethics, of course, the challenge is to translate these understandings in such a way that they can be applied to judging the ethics of conducting operations in cyberspace. What might it mean, for example, to say that someone has conducted an act of aggression against an unarmed civilian in cyberspace? We will explore this issue in more depth in this chapter.

What is Just War?

However, it is necessary to begin by spelling out in greater specificity what is meant by the notion of 'Just War,' as well as how it is expressed through the Law of Armed Conflict, through examining its history, its sources and its provisions. Military ethicists and lawyers distinguish between two sets of moral and legal understandings: ***Jus in bello*** is a Latin phrase which refers to understandings regarding the prosecution or carrying out of war. Jus in bello provisions are codified in the Law of Armed Conflict. This set of legal and ethical understandings – derived largely from the legal framework of the United Nations – spell out the conditions under which the prosecution or fighting of a conflict is considered legal and ethical in international law.

It is important to note here that jus in bello – as described in the LOAC – is a set of understandings about what actions people can and cannot take **during wars**. Students are sometimes confused, since the LOAC provisions mean that if you behaved in accordance with these restrictions while engaged in combat then you cannot be prosecuted for your actions – regardless of the basis on which the war was fought, or whether or not someone thinks it was a

good or worthy cause. In other words, a legal war is one in which the combatants behaved in accordance with the rules of conduct for fighting their enemies; it has nothing to do with the rightness or the wrongness of the cause or the nation on whose behalf they fought. Theoretically, one could go to war representing an authoritarian dictatorship and still be described as acting legally and ethically – if one followed the Law of Armed Conflict.

Jus in bello questions are separated out, thus, from questions about the justification or reasons for war, which derive from a set of understandings known as ***jus ad bellum*** (Latin for 'right to war'). The body of work known as *jus ad bellum* describes the principles of what constitutes a Just War or one which is engaged in for the first reasons. Greek philosophers debated the conditions under which an army and a nation could be said to have behaved honorably in going to war, and in the non-Western tradition, scholars point to discussions in the Indian epic, *The Mahabharata*.

Within the Judaeo-Christian tradition, scholars point to the writings of **Augustine of Hippo** (who lived in the fourth and fifth century AD) and **Thomas Aquinas** (1225–1274) as providing the roots of *jus ad bellum*, or Just War thinking. Augustine's work addressed one's intent in going to war, suggesting that one should not, for example, go to war with the intent of punishing one's opponents or seeking revenge upon them for emotional reasons. Rather, for war to be practiced as statecraft, nations and groups should seek specific goals such as defending their territory from one who sought to trespass. A war fought for this reason was seen as ethical, while fighting merely because one disliked one's neighbors or wished to harm them was not. Aquinas sought to explain the ethics of the Crusades through examining, again, the conditions under which one could properly and ethically go to war. Aquinas contributed the understanding that "one should wage war to wage peace." That is, a nation's goal should be to end a conflict through going to war against a nation which upset the world's balance, to restore that balance and to check aggression. He suggested that one should not go to war merely to enrich one's nation or for territorial gain. Later analysts like **Hugo Grotius** (1583–1645) added provisions such as a ban on 'preemptive war,' in which one attempts to seek an advantage over one's opponents through attacking first or before an opponent is ready.

Today, jus ad bellum criteria for Just War are spelled out in customary international law by the international community. They include the following:

As you learn about these principles, you should be already asking yourself how one can distinguish between preemptive and defensive war, between punitive and defensive attacks or strikes, and between various types of intentions when one is fighting not a physical war over land, but a virtual war in cyberspace. As we will see in this chapter, analysts disagree as to whether ideas like those of Aquinas and Grotius can be neatly mapped onto war in cyberspace.

In addition to the provision of jus in bello, we need to consider the specifics of *jus ad bellum*, or the ethical and legal principles for the just prosecution or conduct of war. The Law of Armed Conflict, which rests on customary international law, or a set of legal understandings between states established and accepted historically, establishes four basic principles: Distinction; Proportionality; Military necessity; and Unnecessary suffering (LOACblog, No date).

Criteria	*Explanation*
Right Intention	The state can legitimately go to war for reasons of self-defense (i.e. if their territory has been attacked). Stated in United Nations Charter Article 51
Proper Authority	This means that only states can declare war and that doing so must be by the proper means, such as a written order
Public Declaration	The state initiating conflict also needs to publicly state that it is doing so – rather than engaging in a sneak attack
Just Cause or Right Intention	They may engage in war in order to stop their opponent's aggression and restore the previous order. States are not ethically and lawfully permitted to declare war for the purposes of extracting revenge or punishing an opponent, and they must not do so for reasons such as self-aggrandizement, such as wanting to increase their prestige or territory
Probability of Success	States must feel that there is some probability of success in responding to an attack, rather than undertaking a suicide mission or failing to secure allies who might help them to win the conflict
Proportionate Force	States must use only enough force to accomplish their objective. In other words, it would be inappropriate to kill all of an opponent's soldiers, or to destroy all of their equipment
Last Resort	States should only initiate conflict if all other means of solving the conflict have failed (such as diplomacy)

Figure 7.1 Criteria for initiating conflict

The **principle of distinction** in international law establishes that warfare is an activity carried out by states in which professional soldiers engage in combat with one another. When a state formally declares war on another state and meets the provisions for what constitutes lawful intervention against another state, then the soldiers of that state are permitted to go to war against the soldiers of the adversary state. However, there is never a case where a state is allowed to legally or ethically attack civilians of an adversary state. Rather, civilians as well as civilian infrastructure (like hospitals and schools) are regarded as protected from injury in war. Thus, states are required to practice distinction – practicing restraint in their targeting and taking measures to make sure that civilians are not injured in warfare.

The **principle of proportionality** means that states and those acting on behalf of states should apply only as much force as is necessary to achieve one's goal, which is to repel an adversary from one's territory. One's intent thus should be to repel an adversary, rather than to punish an adversary by, for example, destroying his village or his entire military company or battalion. The calculation about how much to attack should thus be a rational calculation rather than one motivated by emotions. The objective also should not be to gain an advantage against your opponent in future warfare by, for example, damaging his equipment and personnel to the point that he could never respond in the future, even in self-defense.

The **principle of military necessity**, again, limits the actions which a state can engage in in warfare – placing limits on activities which are not required in order to prevail in a conflict. Thus, one should never unnecessarily torture an opponent, or blind him or permanently injure him intentionally. This principle has also been interpreted to mean that certain categories of weapons should never be used, since there is no military necessity for doing so. For example, blinding agents and certain categories of weapons – such as biological and chemical weapons – are considered not military necessities.

Finally, the LOAC includes the **principle of avoiding unnecessary suffering**. Again, this is meant to limit the scope of warfare to only that which is actually necessary, through prohibiting actions like torture.

As we can see here, although it is written at the state level, international law also provides a basis for judging the ethics of specific parties to a conflict, including individual soldiers and civilian decision makers who can be prosecuted for **war crimes** or violations of international law during a time of war. War crimes are actions carried out during a conflict which violate international law. Such acts would include violations of either the LOAC or the Geneva Conventions, including willful killing, or causing great suffering or serious injury to body or health, and torture or inhumane treatment.

As we see in the five examples we began this chapter with, some of the actions described appear to violate international law – since the attacks affected both professional soldiers engaged in military combat and civilians. An attack on a power grid of a city, as occurred in Kiev in 2016, has the potential to cause "unnecessary suffering" to civilians, as it might result in individuals in hospitals, nursing homes and other facilities being deprived of lifesaving procedures or equipment. In addition, during a cold winter, depriving people of power raises the issue of potential deaths from hypothermia. Hacking attacks into another nation's electoral systems are also a violation of international law, since nations agree to respect other nation's **sovereignty** through non-intervention in the domestic affairs of another nation (Wood, No date).

However, as you read through these examples, you may find yourself remembering the uniqueness debate which we have encountered throughout this text. And you may ask yourself, "Is it really appropriate to call someone who uploads a virus which crashes an electrical grid a war criminal? Doesn't that seem a bit harsh? Isn't a war criminal someone who serves as a guard at a concentration camp in Nazi Germany, not an individual who writes a program or alters a script?" Here we are really asking whether cyberspace constitutes a new and unique terrain for ethical, moral and social thinking – or whether preexisting ethical, moral and social understandings can be imported and applied to cyberterritory and cyberinteractions. Here we can ask: Is cyberwarfare really even war? Is a cyberattack really the same as an armed attack? And what does it mean to talk about a cyberattack on unarmed civilians? Can we really distinguish between who will be affected by a cyberaction – civilians or only professional military personnel – and how might we do so?

Principle	*Explication*	*Restrictions*
Distinction	War is between professional combatants only. Civilians are not to be targeted or involved in military conflicts.	Restrictions on attacking hospitals, schools; use of aerial bombardment; avoiding situations which would create refugee streams
Proportionality	States should only use enough force to repel an attack on their territory. Once they have achieved that objective, they should cease military actions.	Restrictions on use of nuclear weapons
Military Necessity	Actions should only be undertaken in war out of military necessity – not out of a desire for revenge or punishment.	Restrictions on torture and actions of a punitive nature
Unnecessary Suffering	States should strive to avoid inflicting unnecessary suffering, including refraining from using weapons and practices described as cruel or inhumane.	Restrictions on use of chemical and biological weapons, blinding agents, torture

Figure 7.2 Major provisions for law of armed conflict

Those who believe that there is such a thing as "Just War in cyberspace," point to steps which the United States has already taken towards the regulation of cyberwarfare as simply another type of combat. First, it has established the US Cyber Command as part of the United States Strategic Command. This organization is located along with the National Security Agency's Threat Operations Center in Fort Meade, Maryland. Beginning with the 2011 Department of Defense Strategy for Operating in Cyberspace, the United States has established that nations have a right to react with military force to attacks on their national cyber infrastructure – both military and civilian. This document notes that The Department of Defense will "oppose those who would seek to disrupt networks and systems dissuade and deter malicious actors and reserves the right to defend these vital national assets as necessary and appropriate" (United States Department of Defense, 2011, 4).

Next, they point to the specific provisions established in the Tallinn Manual which have attempted to codify key issues – such as the role of civilians in the prosecution of cyberwar, the conditions under which it is lawful to respond to a cyberattack, and the ways in which one can practice discrimination in cyberwarfare through not targeting civilians. The Tallinn Manual notes that nations can respond to cyberattacks with conventional force if the intensity of a cyberattack is such that it meets the definition of an armed attack (according to Article 51 of the United Nations Charter). It also notes that civilians can participate in cyberactivity during wartime alongside military personnel. However, when they do so, they lose the protection normally provided to civilians and may instead be treated as combatants. The Tallinn Manual also acknowledges that while one cannot specifically target civilians during a cyberattack, it is permissible to carry out attacks which might nonetheless inconvenience citizens through – for example – taking a banking system offline (Schmitt, 2014).

In addition, information ethics experts like Taddeo (2016) and Dipert (2014) have both made the claim that destroying an information object is the goal of cyberwarfare, and that such actions can indeed be managed and judged according to traditional Just War precedents.

Those who believe that a framework of laws and norms of ethical behavior in cyberspace can be created paint an optimistic picture of the international system as a place which could include a safe, secure cyberspace, which is predictable and rule-governed (Broeders, 2016). In this view, cyberwarfare can provide an even better, more ethical alternative to conventional warfare for two reasons: First, analysts like Denning suggest that cyberwarfare could cause less harm and be more easily reversible, particularly if it does not cascade or escalate to encompass conventional warfare as well (Stewart, 2013, 1). At the same time, some analysts argue that just as the presence of nuclear weapons actually makes the world a safer place because states are cautious about entering into conflicts where the results might be so deadly (creating a situation of Mutually Assured Destruction), that the presence of cyberweapons which have the potential to disrupt our electrical grids, air control towers and other vital services like heat and water may be sufficient to establish a situation where states are willing to practice restraint in order to avoid Mutually Assured Cyber Disruption. Valeriano and Maness suggest that thus far, states seem to be creating a system of cyberdeterrence, at least informally. They argue that as long as states are able to engage in restraint through not using cyberweapons to attack their opponents, the more likely it is that such restraint will become a norm within the international system. They write:

> The longer this remains the case, the more likely it is that states will set up normative rules to govern cyber behaviors. This could include institutional restraints, international consultations or legal standards … cyber actions are a sacred taboo that must not be violated. There remain red lines that no one has yet crossed. There is a chance they will be crossed, but for now we have observed states being limited in cyber actions.
>
> (2015, 63)

Here, we can identify the virtue of restraint at work, as we did in Chapter 4 on privacy. Powerful actors may decide that even though they have the ability to carry out an action, they will engage in self-control through choosing not to pursue the action. However, others might argue that if states are indeed practicing restraint through choosing not to deploy cyberweapons, it is likely occurring only for utilitarian reasons. Here Valeriano and Manness suggest that states may engage in a calculation whereby they conclude that "If I attack him via cyber, there is at least a chance that he will attack me conventionally with far greater force" (2015, 64).

Finally, Gvosdev makes an ethical argument related to the characteristics of the cyberweapons themselves. He suggests that cyberweapons could be created which were more precise – better able to discriminate against targets, and thus less likely to lead to indiscriminate killing. He writes that:

> Whereas a generation ago a nation might still have to use munitions to cripple strategic targets such as command-and-control facilities, power stations or communications center – running the risk of killing employees and personnel in those areas, a cyber weapon offers the prospect of a bloodless strike, of being able to take infrastructure off line without having to permanently destroy it… . A cyber weapon might be seen as a more ethical choice than deploying an explosive.
>
> (Gvosdev, 2014, 1)

However, Gvosdev notes that one might need to plant a cyberweapon on an enemy's computer during peacetime, leaving them there to deploy in the event of a war. However, as we know, doing this would violate international ethical and legal standards, which do not permit moving weapons into place – onto another state's territory – during a time of peace and without a declaration of war. Thus, Gvosdev argues that the use of cyberweapons could easily lead to a merging of the boundaries between peacetime and wartime and create a situation where even when nations were at peace, it was only because they were passively threatening their opponents with the threat that they could destroy them at any time. He also notes that it is unclear what we should call the people who create these weapons and place them upon other's servers during peacetime. Are they combatants, noncombatants or someone else? It appears in many ways that cyberwarfare is creating a new type of war which raises many new (and unique) ethical questions.

Box 7.1 Application: defining cyberweapons

On any given day, your home computer (or smart phone) may upgrade its settings multiple times – downloading patches and fixes for existing programs, upgrading software and even exchanging information with other computers about problems that might arise in your system. Every time, your computer is vulnerable to the threat of attack by cyberweapons. But what exactly is a cyberweapon, and how do we distinguish between a cyberweapon and other types of threats – like those related to cybercrime or nuisance activities?

It's important to have a specific definition of cyberweapon for three reasons: First, most policymakers agree that computer programs which are classified as cyberweapons should be treated differently than other programs. Companies should be required to exercise greater security in terms of who they share and sell such programs to. In some instances, the government should intervene in order to make sure that cyberweapons are not sold to a nation's adversaries or groups which may have hostile intents towards one's nation. International and domestic laws regulate arms trafficking in relation to traditional (kinetic) weapons. Arms dealers must be registered and they must obtain export licenses before trading in certain devices. If they do not, they are subject to criminal penalties both domestically and internationally.

Next, it is useful to know what a cyberweapon is when deciding whether or not to accuse an adversary of having launched a cyberattack. As noted in this chapter, some activities of one's adversaries might properly be classified as cyberespionage while others might be defined as cyberattacks. Here, a useful determinant may be the type of device or program which an adversary used in carrying out activities on a host nation computer.

Finally, some analysts have called for cyber arms control and a halting of the cyber arms race which they see developing amongst developed nations. In order to formulate binding international agreements regarding the conditions under which one can create and stockpile cyberweapons, as well as to verify whether nations are adhering to such agreements, a definition of cyberweapon is an important first step.

But the taxonomy of cybersecurity issues does not always lend itself to the most accurate definitions. The use of the term cyber, while academically vague, acts as a catchall adjective in the industry for digital communications and activities. The term cyberweapon still has contentious definitions. It could be defined as any digitally based method of attack, ranging from the oft-used DDoS attack to spear-phishing schemes. However, this perspective is unintuitive for academic purposes, because it lumps together ontologically separate concepts.

The North Atlantic Treaty Organization (NATO) has developed a definition for cyberweapons which appears in the "Tallinn Manual on the International Law Applicable to Cyber Warfare". This definition focuses on the intent of the attacker, stating that "cyber weapons are cyber means of warfare designed, used or intended to cause either injury or

death of people or damage to or destruction of objects" (North Atlantic Treaty Organization, 2017).

In contrast, academic analyst Trey Herr (2014) has outlined a more specific definition which looks for three elements. A program which contains these elements is thus defined as a cyberweapon. Herr defines a cyberweapon as a digital object, and a form of malware that follows a specific pattern of behavior for a specific set of purposes. According to Herr, malware includes three elements: a *propagation* method or a way of reproducing; a technique for *exploiting* weaknesses in digital spaces and delivering a *payload* to either steal or destroy data or disrupt digital or physical properties. (These elements are abbreviated as PrEP.)

Herr's definition departs from the NATO definition in stating that a cyberweapon is meant to target digital objectives with physical consequences as an extension of the weapon's capability. Herr's definition also allows for the term cyberweapon to be attached to a program which degrades and destroys data, rather than looking only at the destruction of physical infrastructure. His definition also excludes other programs from being labeled as cyberweapons. A cyberweapon degrades, damages or destroys its target. A tool for stealing data or observing network activity is a tool of espionage, not a weapon. While it could be that these tools of espionage are perceived as being damaging, this does not make them cyberweapons. External perceptions do not change intrinsic properties.

Sources

Ford, S. 2014. "Warfare, Cyberweapons and Morality." In *Cybersecurity: Mapping the Ethical Terrain*, eds. M. Keelty, A. Henschke, N. Evans, S. Ford, A. Gastineau, and L. West. National Security College Occasional Paper No 6 June 2014. Australia: Australian National University. Available at http://nsc.anu.edu.au/documents/ocassional-paper-6-cyber-ethics.pdf. Accessed April 4, 2017.

Herr, Trey. 2014. *PrEP: A Framework for Malware and Cyber Weapons*. Washington, DC: George Washington University Cybersecurity Policy and Research Institute. Available at https://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/54ee0d97e4b0621e861ba345/1424887191756/PreP+paper.pdf. Accessed March 15, 2017.

Infosec Institute. 2015. *Cyberwarfare and Cyberweapons, a Real and Growing Threat*. Madison, WI: Information Security Institute. Available at http://resources.infosecinstitute.com/cyber-warfare-cyber-weapons-real-growing-threat/#gref. Accessed March 19, 2017.

View two: cyberwar is a unique new form of conflict

Thus, some philosophers disagree about whether one can certainly "import" ethics and norms from conventional war into thinking about cyberwarfare. In a recent analysis, Matthew Waxman (2011), a lawyer, describes a hypothetical situation in which the United States "goes to war" against Iran. He suggests that they might undertake four different types of actions: conducting military strikes against the physical infrastructure of Iran's banking system; disconnecting Iranian

banks from the US financial system through passing legislation and sanctioning them; flooding their economy with counterfeit currency or uploading malware to corrupt the computer infrastructure of their banking system. He describes one strategy which is a conventional war strategy (destroying physical infrastructure); one which is actually an economic strategy (passing legislation to sanction an opponent economically); one which is actually a type of covert activity (passing counterfeit currency) and one which is a cyber activity (uploading malware). He then asks the reader to consider which of these would be legal, and which would be considered a "**use of force**" as defined in the United Nations Charter.

Analysts who come down on the 'uniqueness' side of the uniqueness debate point to specific properties of cyberspace and internet technology which create new ethical challenges for warfare. As we can observe in the examples provided here, cyberattacks can vary in their intensity and their targets. In addition, participants in cyberhostilities may be states or nations or nonstate actors like a terrorist organization, and targets may include commercial entities like corporations. Thus, analysts disagree about such basic questions as: what constitutes an act of war in cyberspace? When is an attack illegal under international law? When is it permissible – legally and ethically – to hack back at an adversary, and what constitutes direct participation in hostilities in cyberspace?

Defining cyberattack

In US military parlance, a **computer network attack (CNA.)** – is any attack carried out against 'critical national infrastructure.' A computer network attack is thus an action aimed at destroying someone else's computers. The attack designation refers to the consequences of the action rather than the means used.

In designating a computer network attack, Solis (2014, 12) distinguishes between cyberintrusion and cyberattack. He notes that an intrusion is smaller in scale; an intrusion may be a covert operation against a specific computer or individual target which might be valuable (such as a government's nuclear command and control system, or a civilian hospital or banking system). A computer network attack, in contrast, is aimed at critical infrastructure. Critical infrastructure means military and civilian networks which carry out functions like transportation, energy supply (electrical systems, natural gas, oil), banking and finance – essentially any system which the disruption of which would cause profound social, economic and legal consequences. In fall 2016, voting systems were added to this list of critical national infrastructure.

Despite the significance of the target in a computer network attack, it may nonetheless be difficult to distinguish whether or not an attack is actually occurring. As Solis (2014, 11) writes:

> An armed attack by frontal assault, naval gunfire or aerial bombing makes clear that a kinetic attack … is underway. Cyberwarfare, however, sometimes allows room to question if an attack is even occurring and whether the Laws of Armed Conflict and International Humanitarian Law even apply.

Furthermore, he notes that it may be very difficult to know who is actually carrying out the attack, and the status of that individual or group. He notes that international laws would apply in

a situation where the attack was carried out by a state's armed forces, intelligence services or even a private contractor working for the state (2014, 15). However, in recent years, it has often been difficult for analysts to tell whether the group that attacked their system belonged to a volunteer hacker collective which supported a state's policy (i.e. a group of Chinese or North Korean computer hobbyist hackers) or whether the group was in fact working on behalf of the government.

It is important to know who originated the attack in this instance since it would be legal under international law for a state to 'hack back' or retaliate if it felt that it had been the subject of an armed attack by another state. However, the matter is more complicated if a state suspects that it has been attacked by civilians acting as a nonstate actor. In addition, Solis writes that at the moment of attack it may be difficult for a military target, for example, to know if he is being attacked by a hostile nation intent of harming his system, or if he is being attacked by a hobbyist who is merely exploring the system without intending to cause any harm. He notes that in the UN Charter, both 'attack' and 'act of violence' are very specific legal terms which are clearly defined. However, he argues that these terms can be applied to talking about cyberattacks – since one can show that an act was aggressive or hostile in nature, and that it was intended to harm an adversary. He writes:

> For either international or non-international armed conflicts, one excellent definition of cyber-attack is a trans-border cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons, or damage or destruction to objects.
>
> (2014, 11)

Here he notes that the specific military definition is much more limited than the way the term is used in the media, where almost anything might be termed a 'cyber-attack' (2014, 11–12).

However, one grey area that still exists is the question of whether one could respond to an offensive cyberattack with a conventional attack, or whether one could respond to a conventional attack with an offensive cyberattack.

The problem of attribution

In addition, analysts point to the problem of **attribution**. They note that unlike conventional hostilities where it is often quite easy to identify the perpetrator of an attack, cyberhostilities raise certain challenges. It is often difficult to determine whether an attack has occurred, who carried out the attack and when. Thus, it may be difficult to figure out if an actor did indeed attack preemptively – since states have thus far not issued formal declarations of war before engaging in cyberhostilities.

Furthermore, it is unclear whether or not international law provisions which were drawn up to cover the actions of states can actually be used to judge the legality and morality of actions carried out by nonstate actors. The traditional Law of Armed Conflict makes several assumptions that may not hold in cyberspace: It assumes that we can clearly identify the attacker and trace an attack order through a chain of command, making it possible to attribute both ethical and legal

responsibility for an attack. It is not always possible to establish a chain of command in the same way in the cyberenvironment; this becomes particularly challenging now because of things like bots and automated attacks. In a recent case, researchers at Oxford University have alleged that someone manipulated the results of Britain's "Brexit vote" in which the United Kingdom's citizens voted to leave the European Union. These researchers suggest that an individual or group created "**ballot bots**" – describing social media accounts which were utilized to sway voter's opinions on the June 2016 referendum. The researcher describes this type of social media manipulation as a threat to a healthy democracy (Baraniuk, 2016).

Alternate frames for considering cyberwarfare ethics

Given the difficulties in applying – or importing – the Just War framework into talking about cyberwarfare, some scholars have suggested abandoning this framework altogether, instead asking questions about the ethics of cyberattacks using a framework of criminality, terrorism or espionage, rather than by referring to military war ethics.

These analysts note that carrying out acts of violence or destruction in cyberspace are much cheaper than carrying out similar 'attacks' using conventional forces. For this reason, many of those who carry out such acts are not actually nations but might instead be smaller, less formal groups known as **nonstate actors**. In our five cases with which we began this chapter, four of them feature traditional state or national actors. We can name Georgia, Russia, the United States, Ukraine and North Korea as nations involved in cyberwarfare. However, the third case here involves no traditional national actors. Rather, the participants in cyberwarfare – the Islamic State of Iraq and Syria (ISIS) and Anonymous – are both nonstate actors, acting on behalf of their own interests and not on behalf of a particular state. If we look back at our definition of an 'act of war,' we see that it refers only to the actions of 'one country against another.' Therefore, the actions of Anonymous would not be considered an act of war, nor would its actions be subject to international law.

For this reason, some analysts thus suggest that the actions of groups like Anonymous – and ISIS – are better understand not within the framework of international humanitarian law (IHL) but rather within criminal law. We might define the actions of nonstate actors, as well as certain actions by state actors, thus as acts of cybervandalism, cyberterrorism or cyberespionage, rather than cyberwarfare. Here, we can consider several different definitions, including the definition of cyberterrorism, espionage, cyberespionage, psychological operations and **propaganda**.

Defining cyberterrorism

Just as cyberwarfare is often treated as an unconventional variant of warfare in general, the term cyberterrorism is often used to denote a subset of terrorist activities with the caveat that such activities occur through or on the internet. Cyberterrorism can thus encompass a number of activities: A terrorist group might overtake means of communication to put out false reports about, for example, a large-scale chemical spill in a major urban area, leading to social disruption as millions of people attempted to evacuate the area. A terrorist group might also engage in data

mining to get information about a prominent individual in order to engage in assassination or kidnapping, as well as blackmail the individual through threatening to release embarrassing or compromising personal information. Finally, a terrorist group might actually create widespread civilian casualties by, for example, tampering with equipment which regulated food safety or tampering with equipment at an air traffic controller station, leading to plane crashes and collisions. Terrorists might also use the internet to carry out activities as a force multiplier, increasing the efficacy of conventional attacks which might be occurring at the same time.

In general, terrorism is regarded by the international community as both illegal and unethical for a variety of reasons: First, terrorists violate Just War criteria through engaging in surprise attacks outside of a conventional battlefield, with no formal declaration of war, and failing to distinguish between civilian and military targets. In fact, terrorism is often carried out for the purposes of intimidation. The aim is to solicit an emotion of terror through carrying out one action which can inspire fear in many others, causing them to change their behavior as a result. The aim is political, but unlike conventional warfare, the terrorist is not aiming to kill all of his opponents. Rather, the aim is to carry out an act which is injurious enough (physically or economically) that others will rethink their actions. The element of surprise is key in creating this emotion, since anyone anywhere could be the target of a terrorist attack at any time – since terrorists respect neither battlefields nor the civilian/soldier distinction.

Terrorists themselves have no legal status within the international community because they are not uniformed combatants fighting on behalf of a state. That is, terrorism differs from warfare in that it is not regulated by international law. It is always illegal and unethical, because it does refer to activities carried out outside of formally declared war and because it does not distinguish between civilians and military personnel as targets.

The cyberterrorism label is useful in referring to the actions of terrorists on the internet since it emphasizes the fact that both civilian and military infrastructure may be targeted by these actors, and that the effects of these attacks may be felt by civilian and military actors alike, without warning, at any time and in any circumstances.

Defining psychological operations

Others have suggested that many cyberattacks today should be understood not as acts of war, but rather as a facet of psychological operations. Psychological Operations or PSYOP are planned operations to convey selected information and indicators to audiences to influence their emotions, motives, objective reasoning and ultimately the behavior of organizations, groups and individuals (Rouse, No date). Psychological operations refers to a set of activities which can be performed both during war itself and in the stages leading up to a conflict. Here, the aim is often to 'prepare the battlefield' by confusing actors as participants in war, through supplying false information. Psychological operations are aimed at eliciting an emotion such as confusion or fear. Psychological operations may not involve any actual physical force or any intentional injuring of targets.

Psychological operations are thus a form of what Brey (2007, 27) calls information warfare. He defines information warfare as "an extension of ordinary warfare in which combatants use

information and attacks on information and information systems as tools of warfare." Information warfare might include using the media to spread propaganda, and it might also include disrupting, jamming or hijacking the communication infrastructure or propaganda feeds of the enemy and hacking into computer systems that control vital infrastructure.

Information warfare relies on the use of deception, which is legal according to the Laws of Armed Conflict which permits deceiving one's enemy through stratagems and ruses. Indeed, the history of warfare contains many examples of situations in which a nation successfully used propaganda as part of its arsenal of tools in warfare. In the US military, propaganda refers to "any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes or behavior of any group in order to benefit the sponsor, either directly or indirectly" (Garrison, 1999, 4).

However, while the use of deception in warfare is not considered illegal, ethicists often describe it as unethical. Psychological operations frequently aim to destroy the credibility of an organization, a corporation or an individual – including a political figure – or a process (like the electoral process). Thus, one can list objections to the use of cyber psychological operations within warfare from both a virtue ethics and a deontological perspective. A virtue ethics perspective might suggest that while warfare is honorable under certain circumstances (Vallor, 2013), it is dishonorable to engage in deceit and deception as part of one's wartime activities. A deontologist would instead focus on the ways in which acts of deception frequently seek to humiliate or embarrass an opponent, harming him psychologically if not physically. Such actions require treating an adversary (and his information) as a means to an end, rather than as an end in itself.

Defining cyberespionage

Another lens for considering the ethics of cyberwarfare treats these acts not as acts of war, or of psychological warfare, but rather as a type of covert activity or cyberespionage. Indeed, in their work, Valeriano and Maness (2015, 9) suggest that fully half of all interstate cyberincidents which have occurred in the last 20 years might be more properly described as cyberespionage or cybertheft, rather than cyber conflict. Brown (2016) notes that the Department of Defense designates much of their cyberactivity not as acts of war but rather as "computer network exploitation" – which is defined as "enabling operations and intelligence collective capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks." That is, the vast majority of the time, Department of Defense "cyberwarriors" are not 'fighting in cyberspace,' but are instead exploring and mapping cyberspace, in preparation for future battles. In legal terms, we can suggest that they are engaged in 'covert activity,' much as spies working on behalf of intelligence agencies are. Covert activities – including surveillance and trespass – are not part of any nation's official foreign policy, and are not publicly claimed by the states since such actions violate international law principles of sovereignty.

Such activities thus create a 'grey area' since as Brown notes, espionage and covert activity are not regulated under international law. Cyberespionage is therefore, in his words, "neither lawful nor unlawful under international law" (2016, 3). Here Brown explains that states, to some degree,

accept that espionage is the price of doing business in the international system. Those accused of espionage are frequently expelled from a host nation but are not usually charged. If they are charged, it is under domestic host nation laws.

However, within the cyberarena, it can often be difficult for those who are the subject of such reconnaissance missions to distinguish between whether they have been explored or whether they have been attacked. Here it is important to distinguish between two types of exploratory missions, or acts of cyberespionage. The United States has frequently been the subject of economic cyberespionage by China in particular. Both government and civilian (corporate) computers have been visited by cyberspies who were attempting to steal economic secrets, such as research and development, schematics for new products and information about their adversary's strengths and weaknesses. In considering acts of economic espionage, we can return to our discussion in Chapter 6 about theft of intellectual property, including the ethical reasoning behind why such activities are wrong. From a virtue ethics standpoint, it represents a failure to respect one's adversary and his property. From a utilitarian standpoint, it decreases a company's incentive to innovate and may weaken the United States economically as a result. From a deontological standpoint, it treats an adversary as a means to an end, and is clearly not something which would be acceptable as a general rule, or in a situation of reversibility. Such acts are considered both unethical and unlawful, and the United States has pressed charges against Chinese citizens accused of engaging in economic espionage in the United States (which may be against a private enterprise); and the United States and China have an agreement aimed at prohibiting cyber economic espionage for commercial gain (Brown, 2016, 3).

However, as Brown notes, "traditional espionage" or the stealing of national security information presents a more complicated set of ethical challenges. In addition, this type of cyberespionage violates several Just War principles. First, it violates the requirement that one must declare war against one's adversary before attacking him. Cyberespionage involves accessing an adversary's system during peacetime and placing cybermunitions to be deployed at a later date. It also violates the injunction against preemptive war, or the understanding that one should not attack in order to achieve an advantage now or in the future, rather than for reasons of self-defense or in response to an act of aggression or imminent attack. That if cyberespionage enables one to carry out reconnaissance for a future act of war, to have an advantage in that situation, it would also be both unlawful under international law as well as being unethical.

Perhaps most importantly, cyberespionage violates the injunction that conflicts are to occur only between professional soldiers acting on behalf of legitimate governments. For in 'breaking and entering' in an enemy's computer systems, the spy may '**masquerade**' as an ordinary citizen. As Rowe (2013) states, the actions of such cyberattackers thus often closely resemble **perfidy**, which is a war crime outlawed by international law (Article 27 of the 1977 Protocol I Additional to the Geneva Conventions). He writes: "Perfidy is attackers masquerading as a legitimate civilian activity, such as soldiers pretending to be Red Cross workers. Perfidy is considered unacceptable because it blurs the distinction between combatants and noncombatants, and encourages attacks on civilians" (2009, 3). Ross describes activities like tampering with routers and TCP/IP protocols as acts of perfidy.

Perfidy is thus a particular kind of deception – in which one impersonates someone else – more specifically a civilian, in order to gain access to a target for the purposes of harming the target. Terrorists thus engage in perfidy when they enter a civilian space for the purposes of harming civilians. Roff (2016) describes military hacking practices which rely on social engineering as acts of perfidy when, for example, a military cyberwarrior impersonates someone else in order to gain a target's trust and establish a relationship which is then used to gain access to passwords and information. Here, we can identify a number of ethical violations that have occurred: The hacker has engaged in lying or deception in masquerading as a civilian. Further, the hacker has harmed another individual through violating their trust. A Kantian deontologist would state further that the hacker has treated the subject as a means to an end, through exploiting the relationship in order to gain access to passwords or information.

If we go back to our chapter on ethical hacking (Chapter 3), we see that this type of masquerading or social engineering is an act which needs to be clearly identified and regulated by an agreement before activities like penetration can occur – in order to preserve the rights and trust of those who will be targeted by social engineering and other practices. As Roff points out, the protocols for the conduct of lawful or ethical warfare do not rule out ever engaging in acts of deception or masquerading – but they do rule out ever pretending to be a civilian when one is actually a combatant. This may include "feigning civilian computer software, hardware or data as a step towards doing harm to an adversary" (2016, 1).

In his work, Ross (2016) makes an analogy – using deception and masquerading to attack civilian computer infrastructure without warning and as a result harming civilians would be similar to poisoning a well in a village. He points out that if the well were the only source of clean water and the poisoning was not announced in advance, and as a result many villagers died, then this would violate several facets of Just Warfare principles. One would have launched an indiscriminate attack on unarmed civilians without warning. Similarly, using masquerading (by, for example, sending an attack from a computer without a "dot mil" address) in order to harm civilian computer infrastructure could have a similar set of effects.

Term	*Definition*	*Source*
Cyberterrorism	"The execution of politically motivated hacking operations intended to cause grave harm that is, resulting in either loss of life or severe economic loss or both."	Tavani (2004, 121)
Espionage	"The act of obtaining, delivering, transmitting, communication or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation." (Department of Defense, 2011, 2)	Brown (2016)
Cyberespionage	"Computer network exploitation" – defined as "enabling operations and intelligence collective capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."	Brown, (2016, 9)
Psychological Operations	Planned operations to convey selected information and indicators to audiences to influence their emotions, motives, objective reasoning and ultimately the behavior of organizations, groups and individuals. Used in all aspects of war, it is a weapon whose effectiveness is limited only by the ingenuity of the commander using it.	Rouse

Figure 7.3 Actions related to cyberwar

Masquerading presents specific ethical issues in any case – but these issues are magnified in cases where military personnel and civilians are involved. In such an instance, masquerading presents the opportunity not only to engage in ethical violations but also to engage in violations of international law. Ross thus distinguishes between attacks on civilian infrastructure and attacks on legitimate targets such as weapons systems, military command and control systems, web pages on military or government web servers and the like.

Thus, as Figure 7.3 indicates, one can identify a set of overlapping ethical issues associated with conflict in cyberspace – whether the activity is waged by states or nonstate actors. Each lens – Just War; Virtue Ethics; Utilitarian Ethics; and Deontological Ethics – highlights particular ethical issues which arise when fighting in cyberspace. The deontological ethics lens focuses on the ways in which practices like psychological operations, social engineering and deception can harm the subject of an attack, while virtue ethics suggests that such practices are not in keeping with the character or moral virtues which one should strive to cultivate. The utilitarian ethical lens suggests that such practices might ultimately generate more harm than good, since in the final analysis they could create a riskier international environment which would also pose more risks to the state engaged in cyberdefense. Finally, whether one refers to cyberactivities through the lens of cyberespionage, cyberterrorism, psychological operations or psychological warfare, one can identify violations of international humanitarian law and the Law of Armed Conflict.

One final issue: machines and the problems of attribution and responsibility

One final ethical issue to consider in our discussion of cyberwarfare ethics relates to the growing use of automated programs and automated weapons in the conduct of cyberhostilities. Miller et al. (2015) note that today cyberhostilities may be carried out through the actions of 'soft bots,' programs which can carry out activities on someone's behalf. Bots could be deployed to carry out a Dedicated Denial of Service (DDos) attack, in which an entity like the Pentagon could find its computers shut down as they are contacted by thousands of computers from around the world all attempting to reach them simultaneously. And computers could be programmed to automatically 'hack back' if they sense that they are being accessed as part of a cyberattack by a hostile entity, in a military protocol known as Active Cyber Defense.

Activity	*LOAC Ethics Issues*	*Virtue Ethics Issues*	*Utilitarian Ethics Issues*	*Deontological Ethics Issues*
Cyberwar	Preemption Lack of Declaration of War Targeting Civilians Participating in Conflict as a Civilian		Destruction of Infrastructure	
Cyberterrorism	Targeting Civilians Preemption Lack of Declaration of War Participating in conflict as a civilian Perfidy	Deception	Destruction of Infrastructure Creation of Risk, Instability	Perfidy/Deception
Cyberespionage	Perfidy Target Civilians	Deception	Destruction of Infrastructure Creation of Risk, Instability	Perfidy/Deception Instrumental Treatment of Others
Psychological Operations	Perfidy	Deception	Destruction of Infrastructure Creation of Risk, Instability	Perfidy/Deception Instrumental Treatment of Others

Figure 7.4 Actions and ethical violations according to ethical frameworks

In Chapter 2, we noted that all three of the ethical models – Virtue Ethics, Utilitarian Ethics, and Deontological Ethics – were created based on certain assumptions, including the assumption that there is an identifiable decision maker making the moral decision, and that the decision maker was aware that he or she was doing so. That is, an individual human was ultimately responsible for deciding to deploy the virus, to engage in the social engineering activity, or to attack the critical infrastructure. But we see in this chapter that this assumption may not hold true when we begin to theorize about the ethics of cyberwarfare.

The use of automated technologies in cyberwarfighting raises a number of ethical issues. First, it raises the issue of deception. Analysts like Miller et al. (2015) suggest that it is unethical to dupe an opponent who might believe that he is interacting with a human when in fact he might not be. Here, we can use the deontological lens to suggest that such a practice violates the principle of reciprocity. If I would not like to find myself in a situation where I was duped, believing that I was battling with a human when in fact I was battling with a machine, then my opponent would similarly oppose such a practice. Furthermore, traditional military codes of conduct rest on a principle developed in the Middle Ages called chivalry. In this view, combat is ethical when it is reciprocal, when both sides are equally likely to be injured or killed in the combat of hostilities. It is the willingness to place one's own self at risk that renders combat honorable. It is a meeting of equals between two skilled warriors. Thus, in recent years, some analysts have suggested that there is something cowardly about 'hiding behind the technology,' through relying on automated warfighting programs and devices. They question how it is possible to call warfare honorable or ethical when it no longer represents a process of reciprocal injury (Manjikian, 2014).

Next, many analysts have suggested that reliance upon programs like algorithms when engaged in combat raises issues of both legal and moral accountability. The analyst Luciano Floridi distinguishes between moral accountability and **moral responsibility**. He notes that a nonhuman entity – like a corporation – can be held morally accountable. For example, one could censure a company which produces a dangerous product which leads to people being injured.

However, he argues that the corporation could not be seen as morally responsible, since only humans are morally responsible (101). In considering who, then, is morally responsible for the actions of a robot or a drone, one might instead choose to give that role to the person who developed the technology, the person who deployed the technology; the person who gave the order to deploy the technology, or the person assigned to be the robot's 'minder.' However, Matthias (2004) calls our attention to a responsibility gap – or the possibility that a situation could develop in which the robot is not considered morally responsible for its decisions, but neither are the human operators. She argues that there may be situations where a machine is able to act autonomously or independently change its behavior during operation in response to changed circumstances, thus creating a vacuum in responsibility.

And Noorman (2014) notes that we tend to have ethical conversations which proceed from the assumption that there is one actor making moral decisions, when in reality most of us exist in webs of social ties. We may carry out tasks with others, and carry out tasks where our actions are dependent upon the actions of others. Thus, autonomy may look very different in practice then it looks in a hypothetical scenario. She gives the example of a plane crash and the sorts of investigations that take place after a plane crash. Investigators try to reach a conclusion regarding who is responsible for the action – but often an explanation might reference a failure to properly inspect a part, an operator or group of operators who created the faulty part to begin with, the person who designed the part or the system into which the part might fit, as well as an action by a pilot or air traffic controller which somehow made the part's failing more important than it might otherwise have been. In such a situation, it becomes difficult to assign responsibility, in order to hold people legal and ethically accountable. She also notes that within military communities, the usual way of attributing responsibility has been to follow a chain of command, asking who gave the order for a particular activity to take place. However, as Noorman points out, today those at the highest echelons of command may not have the same knowledge as a practitioner; while they are commanding those who serve, leaders are not always fully informed as to the technical limitations of the weaponry which is being used, or the nuances involved in their use (2014, 812).

A final issue in the debate about machines as actors in cyberwarfare relates to self-awareness. In their work on moral responsibility, the ethicists Fischer and Ravizza suggest that an individual need to be able to reflect on the morality of his or her own actions, and to see him or herself as capable of acting in a situation requiring moral discernment.

Box 7.2 Critical issues: should we ban cyberweapons?

As you have seen throughout this chapter, warfare is not always unethical nor is it always unlawful. However, not all forms of warfare are ethical and lawful, and international law and ethics has much to say about the specific conditions under which war must be declared and fought.

While one can specify the conditions under which a nation can lawfully declare and participate in war, there are still very specific restrictions on the types of activities which a nation may undertake in the prosecution of that conflict. In recent years, the international community has come together several times under the auspices of the United Nations to clarify which specific types of combat are deemed unlawful and unethical under the international system, as well as which specific types of weaponry are deemed unlawful and unethical. In many instances, this body has enacted specific legislation to outlaw particular types of warfare (such as genocide – the planned destruction of a group of people based on ethnicity, race or religion; or the use of aerial bombardment against civilian targets). It has also acted to implement international bans on the development, creation and deployment of particular types of weapons (including land mines and chemical, nuclear and biological weapons, including blinding agents).

In instances where a specific type of weaponry has been deemed unlawful and unethical, the claim usually rests on one of two grounds. First, some weapons may be deemed unnecessarily cruel and punitive in nature. International law states that an army should use enough force to stop an enemy from achieving a target, but that it should not go beyond the use of that force. Thus, a weapon would be deemed lawful if it succeeded in stopping an attacker from achieving a target, but it should not aim to either cause unnecessary suffering nor should it aim for long-lasting impacts – such as those affecting future generations. States have come together to restrict the development and stockpiling of nuclear weapons, for example, based on the claim that the force of this weapon is almost always disproportionate to the aims which a state may wish to achieve. Similarly, states have worked to ban chemical and biological weapons, due to fears that a global pandemic caused by a biological agent is out of proportion to a specific military aim, as well as an understanding that the suffering caused by such weapons, particularly on civilians, is cruel and punitive in nature.

Recently, states have begun asking whether the international community needs to come together to consider a similar ban on the development, stockpiling and deployment of cyberweapons. Here, one can claim that a cyberweapon which fundamentally altered the international communications infrastructure globally through, for example, destroying the internet, could inflict a long-lasting impact far beyond anything required in order to win a specific conflict.

Alternately, the international community could place specific restrictions on the types of cyberweapons which could be created. Neil Rowe (2009) argues that it is possible to create 'ethical cyberweapons' through placing four conditions on the development of new weapons. He argues that any new cyberweapons need to be "controllable." Weapons should be capable of focusing on specific targets, rather than propagating through means like viruses and worms, which allows them to be indiscriminate in their targeting and aims. He notes that all weapons should be easily stoppable, such that an attack could immediately cease once an enemy surrenders (Rowe, 2009, 10). Currently, some weapons cannot be stopped once they are deployed. He argues as well that there must be a means of identifying the provenance of cyberweapons, through embedding a signature in their code or data, so that attribution can take place. Finally, he suggests that the results of a

cyberweapon should be reversible, so that at the end of a conflict the damage could be prepared. Thus, for example, a weapon might take a target's data hostage and hold it for ransom rather than permanently destroying it. Once the enemy surrenders, he could then be given the keys to decrypt his data and restore his system.

Source

Rowe, Neil C. 2009. "The Ethics of Cyberweapons in Warfare." *International Journal of Cyberethics* 1(1). Available at http://faculty.nps.edu/ncrowe/ethics_of_cyberweapons_09.htm. Accessed April 6, 2017.

A contrasting view, put forth by Wallach and Allen (2010), among others, suggests that a machine can be described as engaged in moral or ethical work if it is merely applying a formula, or choosing from a series of laws to determine whether or not an action breaks a law or violates an ethical principle. They suggest that a machine can be programmed to 'think morally' if, for example, it can calculate the utility of various actions using an algorithm fed to it by programmers and if it can then rank actions from the most to least harmful, and then take actions to either avoid or pursue these ends. In "The Ethics of Driverless Cars," Neil McBride (2015) looks at a future situation of full autonomy – where a car could decide what route to take, fill itself with gas, bid for its own insurance, and learn from its environment without any human inputs. He argues that from a utopian perspective, this allows the machine to go beyond human fallibility and human error. Eventually, he argues your car will be a much better driver than you ever were – since it will be able to do things like interface with other cars in order to 'choreograph' a crash. Both cars would provide technical specifications including their speed and then a program could decide the 'best' impact for the crash in terms of preventing property loss and the loss of human life. From a utilitarian perspective, then, one might argue that the car is capable of acting morally, since it could choose to behave in such a way as to reduce human casualties. McBride asks, "Who wouldn't want that?" However, he then begins to sound like a deontologist when he asks questions about what sorts of impacts this scenario might have on a community. Would humans feel displaced or ashamed when a car takes their job or their source of expertise? In such a scenario is the human merely a means to an end, the source of inputs like gas money or money for insurance? He argues that humans should not be viewed as "a dangerous annoyance to be removed from the system," concluding that there are limits to the degree to which a computer or algorithm might act as a moral decision maker.

But Fischer and Ravizza (1998) would concede that while the driverless car is perhaps displaying judgment, it is not truly thinking morally, since doing so involves seeing oneself as able to make an independent judgment, and also weighing the various reactions that might arise from making a particular decision, including the reactions of other people. Thus, they would oppose the outsourcing of any sort of moral decision making – including moral decision making in warfare, including cyberwarfare – to a machine or a bot.

Chapter summary

- Cyber warfare may be considered both legal and illegal, both moral or ethical or immoral, depending on how it is waged and whether certain conditions are met.
- Cyber warfare is not the same as cybercrime – even though both cybercrimes and cyberwars may involve use of the same techniques – including spoofing, phishing, and social engineering – and the same tactics – like use of deception, espionage, DDoS attacks, etc.
- Some analysts believe that Just War thinking can be 'imported' from conventional war to thinking about cyberconflict. Others, however, disagree.
- There are two ways to approach cyberwarfare ethics. Some analysts focus on **ethical conduct of cyberwar**, through establishing conditions for the deployment and use of cyberweapons in combat. Others focus on the development of the weapons themselves, rather than the conditions of their use – aiming for the **development of 'ethical cyberweapons**.'

Discussion questions

1 Given that international humanitarian law grants nations the right to act in order to secure their own self-defense, and by extension, grants soldiers the right to act on behalf of that nation, could a robotic warfighting device (robot soldier) be legally and ethically granted that right? What ethical issues does this present?

2 "Doxing" is revealing someone's personal information publicly, without their knowledge or consent. But some analysts say that "political doxing" should be considered an act of war, since revealing information about a public figure could destabilize a country. In your opinion, should political doxing be considered an 'act of war'? Make sure you reference the definitions explored in this chapter.

3 Analyst Sanghamitra Nath argues that powerful states should not have weapons that less powerful nations might not have access to – like nuclear or cyber weapons, since this allows powerful nations to threaten weaker nations and creates issues of equity. How might you respond to this ethical argument? Do you agree or disagree and why?

4 Moral philosopher Peter Asaro (2008) worries about a situation in the future where humans might be killed during warfare by a machine or an algorithm acting autonomously, without a 'human in the loop.' Think about the models we have explored in this book – virtue ethics, utilitarian ethics and deontological ethics. How might each model be used to respond to his concern?

Recommended resources

International Committee for Robot Arms Control. Website available at http://icrac.net/statements/. Accessed March 31, 2017.

LOACBlog.com . No Date. "The Law of Armed Conflict (LOAC)." *LOAC Blog*. Available at https://loacblog.com/loac-basics/what-is-the-loac/. Accessed March 31, 2017.

Manjikian, Mary. 2014. "Becoming Unmanned: The Gendering of Lethal Autonomous Warfare Technology." *International Feminist Journal of Politics* 16: 48–65.

North Atlantic Treaty Organization. 2017. "Tallinn Manual on the International Law Applicable to Cyber Conflict." Available at https://ccdcoe.org/tallinn-manual.html. Accessed March 31, 2017.

Powers, Rod. "Law of Armed Conflict: The Rules of War." *The Balance*. September 15, 2016. Available at www.thebalance.com/law-of-armed-conflict-loac-3332966

Rainey, Stephen. 2015. "Friends, Robots, Citizens?" *SIGCAS Computers & Society* 45(3): 225–237.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Singer, Peter, and Friedman, Allan. 2014. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford: Oxford University Press.

United States Computer Emergency Readiness Team (US-CERT). No Date. "NCCIC Cyber Incident Scoring System." Available at www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System. Accessed March 31, 2017.

Chapter 7 sources

Ackerman, Spencer. 2012. "Pentagon: A Human Will Always Decide When a Robot Kills You." *Wired*. November 26. Available at www.wired.com/2012/11/human-robot-kill/. Accessed April 14, 2017.

Asaro, Peter. 2008. "How Just Could a Robot War Be?" In Philip Brey and Adam Briggle, eds. *Current Issues in Computing and Philosophy*. Amsterdam, Netherlands: IOS Press.

Baraniuk, Chris. 2016. "Beware the Brexit Bots: The Twitter Spam Out to Swing Your Vote." *Daily News*. June 21. Available at www.newscientist.com/. Accessed April 14, 2017.

Brey, Philip. 2007. "Ethical Aspects of Information Security and Privacy." In M. Petkovic and W. Jonker, eds. *Security, Privacy, and Trust in Modern Data Management*. Heidelberg: Springer: 21–36.

Broeders, Dennis. 2016. "The Public Core of Internet: Towards an International Agenda for Internet Governance." *Digital Frontiers*. October 19. Observer Research Foundation. Available at www.orfonline.org/expert-speaks/the-public-core-of-internet/. Accessed April 14, 2017.

Brown, Gary. 2016. "Spying and Fighting in Cyberspace: What Is Which?" *Journal of National Security Law and Policy*. Available at http://jnslp.com/wp-content/uploads/2016/03/Spying-and-Fighting-in-Cyberspace.pdf. Accessed April 14, 2017.

Charvat, J.P. 2009. "Cyber Terrorism: A New Dimension in Battlespace." In C. Czosseck and K. Geers, eds. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Amsterdam, Netherlands: IOS Press: 77–87.

Colarik, Andrew, and Ball, Rhys. 2016. "Anonymous vs. ISIS: The Role of Non-State Actors in Self-Defense." *Global Security and Intelligence Studies* 2(1): 20–34.

Department of Defense. 2011. "US DOD Strategy for Operating in Cyberspace." July. Available at www.slideshare.net/DepartmentofDefense/department-of-defense-strageggy-for-operating-in=cyberspace. Accessed April 14, 2017.

Dipert, Randall. 2014. "Distinctive Ethical Issues of Cyberwarfare." In Liles, Sam, ed. 9th International Conference on Cyber Warfare & Security: ICCWS 2014 (Purdue University, West Lafayette, IN on March 24–25, 2014).

Fischer John Martin, and Ravizza, Mark. 1998. *Responsibility and Control. A Theory of Moral Responsibility (Cambridge Studies in Philosophy and Law)*. Cambridge: Cambridge University Press.

Garrison, W.C. 1999. *Information Operations and Counter-Propaganda: Making a Weapon of Public Affairs*. Carlisle Barracks, PA: US Army War College.

Gewirtz, David. 2013. "DDOS: Terrorism, or Legitimate Form of Protest?" February 26. Available at www.zdnet.com/article/ddos-terrorism-or-legitimate-form-of-protest/. Accessed April 14, 2017.

Gvosdev, Nikolas. 2014. "The Ethics of Cyberweapons." *Ethics and International Affairs*. January 30. Available at www.ethicsandinternatioanlaffairs.org/2014/the-ethics-of-cyber. Accessed April 14, 2017.

Haggard, Stephen, and Lindsay, Jon. 2015. "North Korea and the Sony Hack: Exporting Instability Through Cyberspace." *Asia-Pacific Issues, No. 117*. Washington, DC: East-West Center.

Available at https://scholarspace.manoa.hawaii.edu/bitstream/10/25/36444/1/api117.pdf. Accessed May 2, 2017.

Hildreth, Steven A. 2001. "Cyberwarfare." *Congressional Research Service, RL30735, 16*. Available at https://fas.org/sgp/crs/intel/RL30735.pdf. Accessed April 14, 2017.

Hollis, David. 2011. "Cyberwar Case Study: Georgia 2008." *Small Wars Journal*, January 2. Available at http://smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008. Accessed May 2, 2017.

Lucas, George. 2017. Cyberwarfare: *The Quest for Responsible Security in the Age of Digital Warfare*. Oxford, UK: Oxford University Press.

Matthias, Andreas. 2004. "The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata" *Ethics and Information Technology*, September 2004 6(3): 175–183. Available at: "*https://link.springer.com/journal/10676*" *Ethics and Information Technology*, September 2004 6(3): 175–183.

McBride, Neil. 2015. "The Ethics of Driverless Cars." *ACM SIGCAS Computers and Society* 45(3): 179–184.

Mele, Alfred R. 2006. "Fischer and Ravizza on Moral Responsibility." *The Journal of Ethics* 10(3): 283–294.

Miller, Keith, Wolf, Marty, and Grodzinsky, Frances. 2015. "Behind the Mask: Machine Morality." *Journal of Experimental and Theoretical Artificial Intelligence* 27(1): 99–107.

Newman, Lily Hay. 2016. "Officials Are Scrambling to Protect the Election From Hackers." *Wired*. September 21. Available at www.wired.com/2016/09/elections-loom-officials-debate-protect-voting-hackers/. Accessed May 2, 2016.

No Author. 2016. "Alan Mathison Turing." In *Columbia Electronic Encyclopedia*, 6th Edition, 1.

Noorman, Merel. 2014. "Responsibility Practices and Unmanned Military Technologies" *Science and Engineering Ethics*, 20 (3): 809–826. Available at: https://philpapers.org/asearch.pl?pub=1158.

Picard, Rosalind. 2001. "What Does It Mean for a Computer to 'Have' Emotions?" *MIT Media Laboratory Technical Report #534*. To appear in R. Trappl, P. Pett and S. Payr "Emotions in Humans and Artifacts."

Roff, Heather. M. 2016. "Cyber Perfidy, Ruse and Deception." In Fritz Allhooff, Adam Henschke, and Bradley Strawser, eds. *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press.

Rouse, Ed. No Date. "Psychological Operations/Warfare" Available at: http://www.psywarrior.com/mybio.html

Ross, Alec. 2016. *Industries of the Future*. New York: Simon and Schuster.

Rowe, Neil C. 2009. "The Ethics of Cyberweapons in Warfare." *International Journal of Cyber Ethics* 1(1): 20–31.

Rowe, Neil C. 2013. "Cyber Perfidy." In N. Evans, ed. *Routledge Handbook of War and Ethics*. Abingdon: Routledge.

Schmitt, Michael. 2014. "International Law and Cyberwar: A Response to the Ethics of Cyberweapons." *Ethics and International Affairs*. February 10, 2014. Available at

www.ethicsandinternationalaffairs.org/2014/international-law-and-cyverwar-a-response=-to-the=ethicds-of-cyberwaepons/. Accessed April 14, 2017.

Schneier, Bruce. 2015. "The Meanest E-mail You Ever Wrote, Searchable on the Internet." *The Atlantic*. September 8. Available at www.theatlantic.com/technology/archive/2015/09/organizational-doxing. Accessed January 5, 2017.

Solis, Gary D. 2014. "Cyber Warfare." *Military Law Review* 219: 1–52.

Stewart, Kenneth. 2013. "Cyber Security Hall of Famer Discusses Ethics of Cyber Warfare." *Naval Postgraduate School*. Available at www.navy.mil/submit/display.asp?story_id=74613. Accessed April 14, 2017.

Taddeo, Mariarosario. 2016. "Just Information Warfare." *Topoi* 35(1): 213–224.

Tavani, Herman. 2004. *Ethics and Technology: Ethical Issues in an Age of Information and Communication Technology*. Hoboken, NJ: Wiley Publishing.

USLegal.com. No Date. "Act of War." Available at http://definitions.uslegal.com/9/act-of-war. Accessed May 1, 2017.

Valeriano, Brandon, and Maness, Ryan. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford: Oxford University Press.

Vallor, Shannon. 2013. "The Future of Military Virtue: Autonomous Systems and the Moral Deskilling of the Military." In Karlis Podins, Markus Maybaum, and Jan Stinissen, eds. *2013 5th International Conference on Cyber Conflict*. Norfolk, VA: NATO Cooperative Cyber Defense Center of Excellence.

Wallach, Wendell, and Allen, Colin. 2010. *Moral Machines: Teaching Robots Right From Wrong*. Oxford: Oxford University Press.

Waxman, Matthew. 2011. "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)." *Yale Journal of International Law* 36(5): 421–458.

White House. 2011. "International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World." May 9. Available at www.slideshare.net/DepartmentofDefense/department-of-defnese-straegty-for-operating-in-cybersapce. Accessed April 15, 2017.

Wood, Michael. "Non-Intervention (Non-interference in domestic affairs)" The Princeton Encyclopedia of Self-Determination (Encyclopedia Princetonienis). Available at: https://pesd.princeton.edu/?q=node/258.

Zinets, Natalia, and Prentice, Alessandra. 2016. "Ukraine's Defense Ministry Says Website Hit by Cyber Attack." *Reuters*. December 13. Available at www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN1421YT. Accessed May 2, 2017.

Part III

8 The way forward

Learning objectives

At the end of this chapter, students will be able to:

1. Describe the ways in which the development of professional conduct can be impacted by institutions and organizations
2. Assess the social responsibilities of the cybersecurity professional
3. Define anticipatory ethics and describe challenges associated with proactively planning for future ethics challenges
4. Use notions of professionalism to respond to hypothetical situations regarding one's participation in ethically desirable or unpalatable activities

Throughout this text, you have been introduced to many of the most important ethical issues which cybersecurity professionals will encounter today. We have considered the role of the cybersecurity professional and the ethical responsibilities which professionals encounter in areas as diverse as privacy, surveillance, intellectual property and cyberwarfare. In this final chapter of the text, we will pause and consider the professional code of the computer science professional and we will also look forward, identifying some ethical challenges which may arise in the future. Although the emphasis throughout this text has been on applying the models – virtue ethics, utilitarianism, and deontological ethics – at the individual level, in this chapter we will also think about the status of the profession as a whole, and

the ethics of the profession on a group level. Finally, we will consider the sorts of constraints which the computer science professional may encounter in doing ethics in the real world.

Codes of ethics

The moral significance of one's work

What does it mean to be an ethical cybersecurity professional? In his characterization of the profession of engineering, Schmidt (2014, 1001) asks readers to ask "What is it about this profession that makes it a morally significant endeavor? What is it that we do, and that we strive to do that has moral and ethical significance?" In asking this question, he suggests that we are compelled to go beyond the understanding of an ethical professional as simply one who refrains from performing certain actions (like stealing information) that harm others. To be an ethical engineer, in his view, is something more than simply avoiding harmful, illegal or destructive behaviors. Instead, he argues that an ethical professional is someone who has a vision for his profession, and who understands the ethical significance of his profession – the responsibilities which members of his profession have to each other, to the profession and to society. An ethical professional is one who uses his skills as a builder to build not simply a product, but a better world. His work is a realization of those underlying values.

Thus, Schmidt's work illustrates the two competing views regarding what specifically is expected of the professional. The first view is more limited. It suggests that the builder or the engineer or the scientist is ethical if he engages in practices based on a desire to avoid creating or passing on risks or harms to users and society. Here Schmidt suggests that both deontological and consequentialist ethics are largely 'preventive' – or aimed at minimizing or avoiding harm. Thus, they can be used to provide a blueprint for what unethical actions the individual should avoid, in order to avoid harming others. However, they do not establish an ideal set of behaviors regarding what it means to be an ethical person or professional. In contrast, he argues,

virtue ethics provides a view of what actions, practiced consistently, may lead the individual to a higher state of existence in which they develop and perfect their character.

View one: avoiding harm

On the corporate level, as well as on the individual level, we can identify this vision of the 'ideal' professional. This view suggests that the professional should not merely strive to avoiding harm others or creating harm, but should instead evince a commitment to the project of improving people's lives and to creating a more just, fair or free society. Here, we can look at the statement of medical corporate ethics, the Hippocratic Oath, which we were introduced to in Chapter 1. If we consider this oath, we see that it both prescribes specific limits on the medical professional's behavior such that he doesn't harm the patient, but also suggests a broader commitment to 'health' which all practitioners should subscribe to. In this view, doctors are not ethical merely because they refrain from certain practices (like prescribing drugs in order to bring about the end of life) but also because they engage in certain practices – like giving aid to victims of an accident without thinking about economic remuneration and even undertaking personal health risks through providing care to individuals in a situation like the recent Ebola outbreak. In evincing a commitment to health as a social project, then, the physician has both an ethical commitment to his own patient and also a broader commitment to society as a whole.

In describing the job of an engineer, Schmidt identifies three virtues for the profession as a whole. He notes that practitioners should value safety – including the protection of people and their property. That is, a primary ethical commitment should be the commitment to reduce risks – to society and to users, through the creation of safe products. However, he argues that they should also value sustainability – including a commitment to improve the environment and conserve resources. Finally, they should value efficiency – or the ability to perform functions while minimizing costs. Among computer scientists, we see similar corporate ethical commitments

voiced by groups like the Privacy Enhancing Technologies Seminar, which has engaged explicitly and politically with the implications of surveillance in society. In some cases, professionals have suggested that an ethical commitment may (and perhaps even must) be translated into activism or political engagement. In many academic and professional fields, scholars have suggested that academic work and activism may be successfully linked, and that those who work in a field should not simply be privately engaged with their own work but that instead they should consider how such work fits into the "project" of encryption, of engineering, or of cybersecurity.

View two: cultivating a moral imagination

For engineers, this second view establishes a broader moral vision for those in the computer science and engineering professions. The first view – that the professional's job begins and ends with limiting harm to one's clients or the users of one's products – would cause practitioners to focus mostly on the private and corporate consequences of engineering decisions, with an emphasis on limiting risk and harm to a user of technology. However, the second view suggests that practitioners need to be aware not just of the safety and risk implications of their engineering decisions, but also of the broader social implications of those decisions. They need to ask not just immediate questions about the risks currently being created, but need also to have a bigger picture, in which they gaze into the future and consider the long-run implications of the decisions they are making today. Obviously, this second task is more complicated and wide-ranging than the first. There is a greater likelihood of failure, since as we have seen in this text, it is not always easy to predict how a technology may ultimately end up being used and indeed there are limits upon the degree to which the designer can affect the ideology which may come to accompany his product.

The analysts Busby and Coeckelbergh (2003) also suggest that this second task is more challenging since it requires the engineer to consider a research problem from a greater variety of angles. He needs to consider a problem – like the development of encryption technologies – from the viewpoint of a

scientist who seeks to solve a technical problem. But he also needs to consider the problem from the viewpoint of the end user, considering how he or she will relate to the technology and how her life will be affected by the technologies available, as well as the possibilities for their use. They argue that the engineer should be able to imagine what it would feel like as a user to be subjected to that risk. Here we might consider, for example, the recent introduction by Samsung of a cell phone with an engineering flaw which caused some phones to burst into flames – in homes and even on airplanes. The 'empathy' approach would ask us to consider not just what sorts of psychological harms people might sustain as a result of purchasing a faulty cell phone, but also how it might affect their overall feeling of well-being, if they were therefore more worried about being stranded or unable to call for help in an emergency. Swierstra (2015) calls these consequences the 'soft' impacts of new technologies.

Some soft impacts of new technologies will be positive while others will be negative, and the outcomes may be ambiguous. Swierstra (2015) argues that engineers thus need to be cognizant of the societal impact of their work, as well as being capable of thinking about 'big picture' issues. His work prompts us to ask questions like: Where are the limits – can computers nudge people to engage in behaviors without their knowledge or consent? When should individuals allow AI to make decisions on their behalf – i.e. ordering their groceries, screening their phone calls – and when should individuals themselves undertake those decisions?

Here Coeckelbergh (2006, 237) refers to the 'moral imagination' of the engineer – suggesting that a professional should be able to discern the moral and ethical relevance of design problems within a larger context. However, as he points out, a new professional who is just beginning a career may not immediately possess all of the skills described above. He suggests that professionals undergo a process of moral development (similar to the stages of moral development described by Kohlberg in Chapter 1 of this text) throughout their careers as they encounter new situations and practice their ethical decision-making skills. A mature professional, thus, might move beyond merely applying ethical rules and frameworks towards making his

or her own decisions in a situation where he or she may encounter two or more conflicting rules or norms.

Looking forward: anticipatory ethics and cybersecurity

The task of the cybersecurity professional is also complicated since ethical challenges associated with technology are dynamic, rather than static. That is, new ethical issues will undoubtedly arise as technologies advance and improve, and changes in the international system may also necessitate changes in terms of how practitioners think about issues like ownership of data, their duties to customers who may not be citizens of their country but may reside anywhere in the globe and their obligations as both national and global citizens.

Thus, the skilled professional needs to be able to anticipate new ethical challenges, to think critically through these challenges, and to decide based on their core values which should not change. Analysts use the term **emerging technologies** to refer to new technological developments which differ radically from those which preceded them. Roto et al. (2015, 1830) describe an emerging technology as one which is "radically novel and relatively fast growing, characterized by a certain degree of coherence persisting over time and with the potential to exert a consider impact on the socioeconomic domain." An emerging technology is one where it is often difficult to predict the impact it will have in the future. Since the long-term effects of a technology may be unclear or ambiguous, it's difficult to think about the ethics challenges which might emerge, as well as the social, economic and political issues which might arise. Halaweh (2013) includes cloud computing, ambient intelligence and virtual reality social networking websites among emerging technologies – describing them as technologies which may be significant and socially relevant in 10 to 15 years.

And while anticipatory ethics are important to individual practitioners, they are also important to the profession as a whole. Metcalf (2014) describes

the ways in which epistemic communities may come together to update ethical codes as new issues arise. Indeed, the Association for Computing Machinery's Code of Ethics makes reference to a set of supplementary guidelines that would be regularly updated to keep up with technological and social changes. Here, Metcalf (2014) states that the process of having conversations within a community about these difficult ethical issues is ultimately as important as the creation of a product – an updated professional ethical code. As members get together and talk about what the standards should be, the problems they foresee in the profession, the ways in which they conceptualize of themselves as a community and their mission, they can identify new information, take steps towards educating themselves and members; clarify important issues such as who their client is, and how they can create mechanisms of accountability to that client.

Unfortunately, communities of professionals have more commonly come together to address ethical breaches in their profession once they have occurred, rather than working proactively. In the field of biomedicine, practitioners came together to address issues of professional responsibility in the wake of scandals involving the prescription of the prenatal drug Thalidomide, which led to the birth of children with birth defects. We can also point to the emergence of the Belmont Report, which details the rights of those who participate in medical trials; this report was written in the wake of revelations about medical experiments which had been carried out on prisoners during the mid-20th century.

We can see some indicators that professionals in cybersecurity have begun to undertake these conversations about anticipatory ethics. Shilton (2015, 15) points to the current NSF Future Internet Architecture (FIA) program – noting that the call for proposals asked participants to identify architectural requirements "clearly informed by the legal, ethical and social contexts in which the future internet will exist." In Europe, the European Commission Project of Ethical Issues of Emerging ICT Applications considers similar issues, while the European Commission educational research and development project on Future and Emerging Technologies is attempting to predict what will be necessary for information technology in 2020, as well as

to think through the implications of future developments. Such projects represent a preemptive approach, then, where practitioners do not wait until issues – including ethical issues – present themselves but rather plan for them in advance.

Comparing codes today

In evaluating both new and old ethics challenges, the practitioner's starting point will always be the professional codes adopted by professional associations associated with cyber security. In this section, we will consider the ways in which the models introduced earlier in this text are reflected in the professional codes of the Association for Computing Machinery's Code of Ethics and Professional Conduct, adopted in 1992. In addition to the International ACM Code of Ethics, we can also identify codes of ethics which are specific to disciplines within information technology (such as the Association of Information Technology Professionals AITP Code of Ethics and Standards of Conduct, adopted in 2002). We can also identify codes specific to a single country such as the Australian Computer Society's Code of Ethics or the Code of Ethics of the British Computer Society.

The professional codes which you encounter may thus differ in terms of specificity, universality (whether they are seen as country specific or international); what they see as the role of the designer versus the role of the user; and in their emphasis on individual ethical responsibilities versus the responsibility of the profession as a whole. Nonetheless, common themes pervade them all – including the responsibilities of the computing and engineering professional to the public and to the public good. Ethical codes address issues of conflicts of interest, scope of competence, objectiveness and truthfulness, deception and professional conduct.

Today we can also note that some codes are bottom-up, having been written by practitioners themselves, acting as an epistemic community. In addition, some have changed over time, with subsequent drafts being issued. Others have been imposed upon the industry, often by a governing or legislative body, with certain facets of the codes being formally incorporated into legislation. Here, we can consider the efforts of the Cloud Infrastructure

services Providers in Europe (CISPE), which adopted a formal data protection code of conduct in alignment with European Union standards regarding the responsibilities of internet service providers to secure user data and safeguard user privacy in regard to data storage. This detailed code reads less as a set of aspirational ideals for those who will work in the field, than as a specific set of professional requirements that employees and managers should adhere to.

The ACM code

Students are advised to become familiar with the Association of Computing Machinery's Code of Ethics. This fairly detailed set of regulations (available in Appendix A) can be seen as containing all three of the perspectives we have examined in this text – virtue ethics, utilitarian ethics and deontological ethics.

The Code lays out the responsibility of the professional to prevent specific harms, reflecting the more limited view of ethical responsibility. Article 1.1 notes that computer experts should strive to "Protect fundamental human rights and respect the diversity of all cultures," as well as "minimize threats to health and safety." And Article 3.5 notes that "It is ethically unacceptable to either deliberately or intentionally demand individuals or groups, but instead personal dignity should be enhanced by an information system." Similarly, the Institute of Electrical and Electronics Engineers (IEEE), the world's largest professional society for electronics engineers, with 400,000 members, provides a minimal code of ethics which largely reads as general advice for professional behavior. We see this same emphasis on citing minimal standards for ethical behavior (basically a list of what people should not do) in the ethical code provided by the Institute for Certification of Computer Professionals (ICCP). This organization provides certificates for core competencies in computing, and acts to fulfill a licensing function since people can lose their certification if a panel determines that they have violated their professional obligations.

But the ACM code also lays out a larger vision of what it means to be a computer professional in Article 1.1 which notes that professionals "contribute to society and human well-being" and in article 3.5 which notes that ACM professionals "articulate and support policies that protect the dignity of users and others affected by a computing system."

Wheeler (2003, 5) identifies both the Kantian categorical imperative, along with elements of virtue ethics in the ACM Code of Conduct. She points to Article 1.4 which notes "be fair and take action not to discriminate," as emphasizing values like equality, tolerance and respect for others. She also notes that overall the ACM Code contains language which emphasizes values like honor, loyalty, wisdom and understanding.

Enacting cybersecurity in the real world

As noted throughout this text, the three models which we have presented for thinking through ethical issues – virtue ethics, utilitarian ethics and deontological ethics – are all predicated upon the assumption that there is a sole decision maker who is making an ethical decision in isolation. His or her decision is not influenced by others, nor is it related to other decisions which he or she might have made in the past or will make in the future. However, in the real world, we often do not have the luxury of making ethical decisions in isolation from one another, nor do we always have free rein to make the best (or ideal) ethical decision – divorced from the pressure of thinking about costs, time frames, organizational policies or other factors which might affect our decisions.

Thus, we will briefly consider some of the constraints that the cybersecurity professional may encounter in attempting to determine the most ethical course of action in a given situation. They include: the constraints of one's profession and professional standards; organizational constraints – such as money, time, and one's own position within an organizational hierarchy; constraints based upon previous decisions made by others, since one often is not engineering a new technical solution from

scratch; the constraints imposed by user expectations; and even political constraints.

First, as Didier (2010, 162) points out, each profession may have its own set of constraints which regularly affect decision making in their field of practice. For example, an emergency room physician may routinely find that time is of the essence in dealing with a patient in severe trauma, and therefore every ethical decision he makes occurs within a preexisting set of temporal limits. He may not have the luxury of waiting to see if a problem resolves on its own. In addition, each profession has its own hierarchy. The physician cannot, in actuality, do whatever he or she wants within a situation, without consulting with the hospital administrator, with legal professionals who safeguard the rights of the patient and with bodies like law enforcement if the patient has, for example, been the victim of a crime. Furthermore, he is constrained by ideals like the Hippocratic Oath, as well as the codes of his profession and the licensing mechanisms of the American Medical Association.

Thus, a professional may have an ideal solution in mind – an ideal technical solution, an ideal ethical solution or an ideal financial solution – but he or she is also called upon to exercise judgment, which may mean forgoing the best possible ethical solution in order to meet multiple important goals through making trade-offs. Physicians might thus be concerned about whether patients truly understand the medical information they are being given or the procedures which they are consenting to, and may thus need to consider their role in providing this information and guidance while still respecting patient autonomy. A lawyer may express concern about the ethics of defending a client when he knows that this client has committed a grave harm to someone else or society. He may consider the constraints of the legal system – not wanting to overburden the legal system with trivial matters, or expressing concerns about whether all clients are truly treated equitably within that legal system. An engineer may struggle with balancing missions like efficiency (creating the best solution within a reasonable time frame at a reasonable cost) and safety (deciding when a system is safe enough and when additional safeguards might

ultimately prove too time consuming or too costly). Didier (2010) describes the practice of weighing options as one of distinguishing between standards of professional practice and ideals which may be more abstract and sometimes unrealizable.

Similarly, computer science professionals dealing with cybersecurity will find that they too cannot simply do whatever they wish to do – even if they too have an ideal technological solution in mind. Shilton presents the example of a computer science professional who is involved in designing net networks including a new Named Data Network (NDN) which might redefine internet protocols. She notes that in 'building' a new system, computer engineers must make both technical and nontechnical choices. Engineers thus have to consider individual values like privacy, security and anonymity – as well as community values like democratization and trust (2015, 1).

Here, Busby and Coeckelbergh (2003) describe the ethics of engineering as coming not only from the engineers themselves and the problems which they must solve. In addition, they argue, engineers need to consider the expectations which technology users have. Here they note that an engineer (and by association, a cybersecurity expert) cannot merely do anything he or she wants. Instead, he or she operates within a web of obligations to a community, as well as a constraint which is created or placed by that community.

Here we can consider a situation where there is a technological solution which might perfectly solve a problem, but it is one which is ethically, politically or socially unpalatable – or at least questionable – to a large segment of the population. For example, one way to make sure that child abductions do not occur in society might be to attach a microchip or RFID tag to each child in America. Such a chip might be implanted in each child upon birth with a technology developed which allows parents to 'track' their child's whereabouts at all times for the rest of the child's life. Similarly, those suspected of terrorism, those released from prison or other members of groups which might be seen as presenting a risk could be similarly 'chipped.' In situations where customs and border enforcement personnel worried

about a visitor to the United States potentially overstaying his visa, the visitor could receive a temporary chip which would track his whereabouts, and which would be removed when he left the country. Clearly, very few people in America would support the imposition of such seemingly invasive controls upon citizens. Although 'chipping' people might be a technologically efficacious solution, it is one which is unlikely to be adopted due to longstanding cultural and historical understandings about what it means to be a citizen, to have autonomy and agency and to live in a democracy. People might be willing to 'chip' their pets, but would surely draw the line at 'chipping' humans.

Busby and Coeckelbergh (2003, 365) express this understanding, claiming that technologies – and a profession like engineering – are not morally neutral. They argue that "engineers are certain constrained by the prevailing culture, client relationships and subordination to managers in the firms for which they work. They clearly do not enjoy complete freedom. When their decisions or their conduct do have the potential for harm they are often quite rigidly constrained by the law." Here, they point to strict statues which exist in the United Kingdom, for example, which require engineering firms to carry out risk analysis studies before undertaking a particular path of action. Furthermore, they argue that engineers frequently have to make decisions regarding the order of priorities which they are pursuing. For example, they might have to choose between the most equitable solution and the safest solution, thus balancing the pursuit of two equally important and ethically compelling goals.

In addition, though our three models treat all ethical decision making as occurring individually, rather than as part of a series of ongoing decisions where later decisions are impacted by earlier ones, in the real world this is seldom the case. In the real world, there is often not merely one designer, but instead there may be multiple design units collaborating to produce a product. And they may be adopting or adapting a technology built earlier, which constrains their work since they are not building from the ground up. Shilton (2015, 5) thus argues that designers may inherit not only earlier technological limitations, but they may also inherit a particular mindset

which accompanied earlier design decisions. She notes that "affordances built into a technology may privilege some uses (and users) while marginalizing others, highlighting values as a critical if sometimes invisible influence on the design process."

And Schmidt (2014, 995) speaks of engineering practices which take place within institutions – and within institutional constraints. He notes that there may be decisions which engineers might like to make but which they cannot because of existing constraints (i.e. here we can think of something like wishing to completely reengineer a product for safety reasons rather than merely making adjustments). It may be that the most virtuous course of action is not always the most feasible.

All of these constraints illustrate the fact that decisions, including ethical decisions, are seldom 'clean.' Instead they are messy. There may be multiple overlapping goals and objectives, along with constraints.

Box 8.1 Application: US Cybercommand

What is the United States Cybercommand and how does it fit into the goals and objectives of the US military? The newest command, USCYBERCOM, was established in 2009. Its mission is to defend the Department of Defense's information networks, to support US commanders worldwide in the execution of their missions, and to act both reactively and proactively to defend "US cyberspace" and that of its allies against attempts at incursions by US adversaries. The US military views cyberspace as a domain of warfare. Just as the US Navy defends US territorial interests at sea, and the US Air Force does so in the air, the US Cybercommand defends America's interests in cyberspace.

CYBERCOM trains and utilizes information warriors who carry out activities such as cyberdefense and analysis of vulnerabilities, as well as participating in activities in new areas like social media. CYBERCOM

also establishes policies regarding US cyberactivities, engaging in questions as to the legality of cyberactivity both domestically and according to international law; jurisdictional issues related to cyberwarfare as well as the conditions under which cyberdefensive and cyberoffense activities (such as '**active cyberdefense**') are ethically and politically justified. The Command also looks at questions like what a force posture should look like for cyberspace, what types and amounts of cyberweapons a state should create and utilize, and how cyberweapons should be used in concert with traditional kinetic weapons.

USCYBERCOM is headquartered at Ft. Meade, Maryland, adjacent to the US National Security Agency. Currently, USCYBERCOM works in conjunction with the Department of Homeland Security to provide cybersecurity to government networks. Each has their respective focus; the former leading the defense of military networks while the latter leads the defense of civilian networks.

Furthermore, there is the problem of interdisciplinarity. Richard Bowen, a fellow of the UK Royal Academy of Engineering, talks about the ways in which engineering and engineering problems in the future are going to be increasingly interdisciplinary, and how that will require an interdisciplinary ethics. He describes an 'entanglement' of different fields, and different ethical stances within those fields (2011, 205).

Today, cybersecurity experts might be asked to develop and test systems for safeguarding the security of patient's radiology x-rays in a system where data might be transferred to another country, as the job of reading x-rays has been outsourced to technologists in another country. They might be asked to design and test systems established so that parents can visually monitor their children while they are in a daycare facility. They might design systems for tracking and monitoring elderly people with dementia so that they do not wander off and become lost or confused. In each of these cases,

the ethical issues will overlap with other fields – including issues of children's rights to privacy, the rights of the elderly, or legal and ethical issues related to the transfer of data from one country to another. In each case, cybersecurity experts might work with professionals from fields like child development, hospital administration or gerontology – each of whom will have their own ethical priorities and ways of looking at a problem.

And as Coeckelbergh (2006) points out, decision making is also constrained by external controls, such as regulatory frameworks. Those who design surveillance systems for hospitals or schools will be constrained by laws governing the rights of children or hospital patients. Additional external controls which we can identify include factors like the wishes of the client (including their budget). Thus, decision makers can be influenced by their peers, by an organization and its organizational culture, as well as by their profession and society (Coeckelbergh,2006, 249–250).

Several codes of ethics reflect this perception – that in the real world, a practitioner may have to sort out the right or ethical action in a situation where he may be asked to fulfill multiple, conflicting roles (Wheeler, 2003, 2). Indeed, the preamble to the ACM Code of Ethics states that "any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations" (Association for Computing Machinery, 1992). It even states in Article 1.2 that at times the ethical action may involve acting as a whistleblower in relation to one's company or one's superiors. Similarly, the British Computer Society's Code of Code notes that members may need to use their own judgment in meeting standards. As Wheeler (2003, 3) notes, "Somehow the ethical information systems practitioner has to balance the ethical requirements of his or her profession, culture, nation and global perspective." Figure 8.1 provides a schematic for thinking through the multiple constraints which a cybersecurity professional may encounter in making an ethical decision.

Defining the scope of professional responsibility

In considering the Code of Ethics put forth by the ACM and the models proposed in this book, it may sound as though the job of behaving as an ethical practitioner is daunting, particularly for a beginner. However, the cybersecurity professional is often not solely responsible for the consequences of every situation which may arise. Although the designer's priority should be to minimize the harm to the user, at least some of the blame for negative consequences, and some of the responsibility for safeguarding against them also belongs to the user. In addition, in situations where a computer engineer designs a technology and then finds that a user has used it inappropriately (such as using a surveillance technology to deprive others of their dignity or human rights), the ethical breach should not be attributed to the designer.

Pols (2010) argues that when a technological artifact is produced (such as a piece of equipment, or code or software), the responsibility for how that artifact is used belongs both to the architect or engineer who designed the technology, as well as to **the user** who also makes decisions about the appropriate use of that technology. That is, ethics are a shared responsibility. However, the original creators of the technology are also in a position to guide would-be users into using technology in ethical ways. For example, we might consider the example of the plastic rings that have been developed to hold together the cans in a six-pack of soda or another beverage. A user might decide to toss this device into the water where it can injure wildlife. Recently, designers have begun experimenting with new types of this technology, including a set of rings which are edible by wildlife, or biodegradable, thus guiding users – or helping them to engage in responsible behavior – by eliminating some of the risk or negative effects.

Figure 8.1 Constraints on ethical decisions in cybersecurity

In cybersecurity, the issue of where the designer's responsibility ends and the user's responsibility to safeguard his or her own safety begins, is far from resolved. The issue here is "To what degree are cybersecurity professionals responsible in situations where the user may make a mistake, oversharing on social media, opening themselves up to social engineering or phishing attempts, choosing 'password' as their password, or sharing their passwords with others?" Here Michelfelder calls our attention to the fact that many computer users exhibit a high level of technological illiteracy. She writes:

> The vast majority of US citizens have little or no comprehension of basic concepts upon which technology is based … students rarely, if ever, take a course where they … are exposed to the design process, make ethical choices in the use and development of technology, or learn about how engineers and technologists use mathematical and scientific principles in the solution of society's problems.
>
> (2010, 64)

Here she argues that consumers and the public also have an ethical responsibility to consider the choices they are making in regard to embracing or discarding a technology, or developing a dependence on a technology. They should not simply depend on technological experts to make these decisions for them.

Political and economic constraints: a final thought

A final set of constraints within which computer scientists must operate today are political and economic constraints. In an interview with *The Atlantic* in 2015, well-known cryptographer Phillip Rogaway cautioned that many computer scientists view their work as esoteric and in many ways beautiful, as they wrestle with complex mathematical theorems inside the Ivory Tower of a university. However, he notes, they may not acknowledge the degree to which their work is also political. "Who funds your research?" he asks, noting that if the researcher is receiving funds from the United States Department of Defense or another government agency – as nearly 75 percent of academic cryptographers do – then the researcher is in some ways implicated in the policies of that agency. Rogaway argues that computer scientists are required to consider the long-run political consequences of their research, to think about who might use their knowledge and the products of that knowledge, and the ends to which that research product might be put to use (Waddell, 2015).

Box 8.2 Going deeper: Just War theorists

The body of ethical thought known as Just War Theory has a rich heritage. Here are a few of the major thinkers who can be described as Fathers of Just War Theory.

Augustine of Hippo (354–430) was born into a relatively upper-class family living in the North African provinces of the Roman Empire. As an adult, he converted to Christianity and moved to Rome. He set upon a critical exploration of Christianity, believing that reason and deduction could be appropriate tools for the study of spirituality. Much of his work asks how people can reconcile their political and spiritual duties, and whether being an ethical person means renouncing politics and political activity. In his work *Contra Faustus*, he explored the question of whether Christians could serve in the Roman Army. This work was a seminal step in the development of Just War Theory.

Thomas Aquinas (1225–1274) was a Catholic priest who worked to utilize both philosophy and theology to ask questions about morality and politics. He is known for his contributions in the areas of Natural Law and Just War. His greatest work was the *Summa Theologica*, a magnum opus that outlined and established Aquinas' theological arguments. One of his major contributions within the *Summa Theologica* was refining a set of warfare ethics created by Augustine of Hippo into what is now known as classical Just War Theory. Aquinas developed three main criteria for a Just War that a state must meet, creating an argument for how warfare could be used for the defense of a rightly ordered peace. These three criteria are sometimes referred to as the deontological criteria of *jus ad bellum*. This moniker is used to prioritize these criteria over prudential criteria that were developed later.

Hugo Grotius (1583–1645) was a Dutch philosopher and legal expert heralded as the father of international law. Much like Augustine before him, Grotius was born into an upper-class family, but his early life was one marked by war. The Dutch Republic was in an ongoing war of independence from the Hapsburg dynasty and in fierce competition to cement itself as a power in commerce. While Grotius made significant

contributions to the study of sovereignty and international commerce, he also contributed to the tradition of Just Warfare. He helped develop new concepts of sovereignty that broadened the scope of legitimate authority from the monarchical right of kings to the duly elected representatives of a democratic body. His work, *De Jure Belli ac Pacis*, was a significant contribution to the contemporary development of the Just War tradition.

Rogaway points to a historic precedent, noting that those scientists who worked on nuclear physics in the 1950s felt compelled to speak out against the nuclear arms race and the dangers that it presented. He suggests that professionals may want to go beyond merely contemplating the ethical consequences of their activities to becoming activists – if they are uncomfortable with how their work is being used and concerned for the future (Waddell, 2015). In 2014, the International Association for Cryptologic Research (IACR) adopted such an activist stance in passing the so-called "Copenhagen Resolution." This short statement notes that:

> The membership of the IACR repudiates mass surveillance and the undermining of cryptographic solutions and standards. Population-wide surveillance threatens democracy and human dignity. We call for expediting research and deployment of effective techniques to protect personal privacy against governmental and corporate overreach.
>
> (IACR, 2014)

Conclusion

As you complete this book, you will hopefully retain some knowledge of the models of ethical decision making which you encountered. It is possible that you have also developed an interest in thinking about technological ethics and that you will follow news stories about emerging topics in information ethics, including those related to surveillance, privacy, intellectual property

and cyberwarfare. But the biggest way to become an ethical cybersecurity professional will come from your professional experiences which will give you an opportunity to practice these skills. You may also have the opportunity to attend lectures and training about ethics in the course of your career, and to engage with other professionals who can show you how they have tackled ethics issues which have arisen in their own careers. As you continue on in this field, your professional community can continue to guide you in thinking ethically both with current issues and those which may arise in the future.

Chapter summary

- While ethical values are constant, ethical issues should be viewed as dynamic. A changing information environment has the potential to create new ethical issues, many of which the original creators of a technology may not have anticipated.
- Professionals often make ethical decisions within a web of constraints – like preexisting technological constraints; financial constraints; user constraints; legal constraints and organizational constraints.
- Today, many of emerging cyberissues are interdisciplinary. Such issues will require knowledge of cyberethics as well as related fields like military, medical or financial ethics.
- The community of computer practitioners has a responsibility to guide the development of their field and to think long-term about the project of computer science and information technology – to ensure that it is meeting the needs of its users and defining and adhering to its mission.

Discussion questions

1 Should a group like the ACM ever have more power to regulate computer activities? Should it have the ability to license computer professionals and to strip individuals of their licenses if they commit a breach?

2 Do you think it is reasonable for computer professionals to have an 'ideal' in mind in terms of cybersecurity? What might an ideal of perfect cybersecurity look like, if you believe that there is such a thing?

3 Think about the future, and consider some challenges which might arise in future computing environments. How can we best prepare for these challenges?

4 Have you ever experienced any constraints in your own work – related to the environment, finances, coworkers or other factors? How did you resolve these constraints and what lessons did you learn from the situation?

Recommended resources

Bowen, Richard. 2011. "Engineering Innovation in Healthcare: Technology, Ethics and Persons." *Human Reproduction and Genetic Ethics: An International Journal* 17(2): 204–221.

Busby, J.S. and Coeckelbergh, Mark. 2003. "The Social Ascription of Obligations to Engineers." *Science and Engineering Ethics* 9: 363–376. Available at https://doi.org/10.1007/s11948-003-0033-x.

Coeckelbergh, Mark. 2006. "Regulation or Responsibility? Autonomy, Moral Imagination and Engineering." *Science, Technology and Human Values* 31(3): 237–260.

Searle, Rick. 2016. "Algorithms Versus Hive Minds: A Premonition of Democracy's Future." *International Journal of Techno Ethics* 7(2): 48–63.

Waddell, Kaveh. 2015. "The Moral Failure of Computer Scientists." *The Atlantic*. December 11. Available at www.theatlantic.com/technology/archive/2015/12/the-moral-failure-of-computer-scientists. Accessed April 4, 2017.

Chapter 8 sources

Association of Computing Machinery. 1992. "ACM Code of Ethics and Professional Conduct." October 16. Available at: https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct.

Bowen, W. Richard. 2011. "Engineering Innovation in Healthcare: Technology, Ethics and Persons." *HRGE* 17(2): 204–221.

Busby, J.S. and Coeckelbergh, Mark. 2003. "The Social Ascription of Obligations to Engineers." *Science and Engineering Ethics* 9(3): 363–376 Available at https://doi.org/10.1007/s11948-003-0033-x.

Coeckelbergh, Mark. 2006. "'Regulation or Responsibility7?' Autonomy, Moral Imagination and Engineering." *Science, Technology and Human Values* 31(3): 237–260.

Dev Bootcamp. 2015. "Ethical Cybersecurity and Tech Inclusivity: Noah Kelley of Hack*Blossom." *Devbootcamp*. Available at https://devbootcamp.com/blog/ethical-cybersecurity-and-tech-inclusivity-noah-kelley. Accessed April 11, 2017.

Electronic Frontier Foundation. No Date. "About EFF." Available at www.eff.org/about. Accessed April 8, 2017.

Fisher, William. 2001. "Freedom of Expression on the Internet." *Harvard Law School, The Berkman Center for & Society*. Available at https://cyber.harvard.edu/ilaw/Speech/. Accessed April 8, 2017.

Halaweh, Mohamed. 2013. "Emerging Technology: What Is It?" *Journal of Technology Management and Innovation* 8(3): 108–115.

International Association for Cryptologic Research. 2014. "IACR Statement on Mass Surveillance." May 14. Available at www.iacr.org/misc/statement-May-2014.html. Accessed April 4, 2017.

Levy, Yair, Ramim, Michelle, and Hackney, Raymond. 2013. "Assessing Ethical Severity of e-Learning Systems Security Attacks." *The Journal of Computer Information Systems* 53(3): 75–84.

Metcalf, Jacob. 2014. "Ethics Codes: History, Context and Challenges." *Council for Big Data, Ethics and Security*. November 9. Available at http://bdes.datasociety.net/council-output/ethics-codes-history-context-and-challenges/. Accessed January 2, 2017.

Michelfelder, Diane. 2010. "The Philosophy of Technology When 'Things Ain't What They Used to Be.'" *Techne* 14(1): 60–68.

Paganini, Pierluigi. 2006. "Healthcare Industry Tops List of Hacker Targets: More Than 100 Million Medical Records Compromised in 2015." *Security Affairs*. Available at http://securityaffairs.co/wordpress/46554/cyber-crime/healthcare-industry-hackers.html. Accessed April 13, 2017.

Pols, Auke. 2010. "Transferring Responsibility Through Use Plans." In I. van de Poel and D.E. Goldberg, eds. *Philosophy and Engineering, Philosophy of Engineering and Tech*. New York: Springer Publishing: 189–203.

Roto, Daniele, Hicks, Diane, and Martin, Ben. 2015. "What Is an Emerging Technology?" *Research Policy* 44(10): 1827–1843.

Schmidt, Jon Alan. 2014. "Changing the Paradigm for Engineering Ethics." *Science and Engineering Ethics* 20: 986–1010.

Shilton, Katie. 2015. "Anticipatory Ethics for a Future Internet: Analyzing Values During the Design of an Internet Infrastructure." *Science and Engineering Ethics* 21: 1–18.

Swierstra, Tsjalling. 2015. "Identifying the Normative Challenges Posed by Technology's 'Soft' Impacts." *Nordic Journal of Applied Ethics* 9(1): 5–20.

UNESCO. No Date. "Freedom of Expression on Internet." Available at www.unesco.org/new/en/communication-and-information/freedom-of-expression/freedom-of-expression-on-the-internet/. Accessed on April 8, 2017.

Waddell, Kaveh. 2015. "The Moral Failure of Computer Scientists." *The Atlantic*. December 11. Available at www.theatlantic.com/technology/archive/2015/12/the-moral-failure-of-computer-scientists. Accessed April 4, 2017.

Wakunuma, Kutoma, and Stahl, Bernd. 2014. "Tomorrow's Ethics and Today's Response: An Investigation into the Ways Information Systems

Professionals Perceive and Address Emerging Ethical Issues." *Information Systems Frontiers* 16(3): 383–397.

Wheeler, Shirley. 2003. "Comparing Three IS Codes of Ethics – ACM, ACS and BCS." *Pacific Asia Conference on Information Systems* (PACIS 2003 Proceedings - 107) AIS Electronic Library (AISeL). Available at http://aisel.aisnet.org/pacis2003/107

Appendix A

Code of ethics, Association of Computing Machinery

Adopted by ACM council 10/16/92

Preamble

Commitment to ethical professional conduct is expected of every member (voting members, associate members, and student members) of the Association for Computing Machinery (ACM).

This Code, consisting of 24 imperatives formulated as statements of personal responsibility, identifies the elements of such a commitment. It contains many, but not all, issues professionals are likely to face. Section 1 outlines fundamental ethical considerations, while Section 2 addresses additional, more specific considerations of professional conduct. Statements in Section 3 pertain more specifically to individuals who have a leadership role, whether in the workplace or in a volunteer capacity such as with organizations like ACM. Principles involving compliance with this Code are given in Section 4.

The Code shall be supplemented by a set of Guidelines, which provide explanation to assist members in dealing with the various issues contained in the Code. It is expected that the Guidelines will be changed more frequently than the Code.

The Code and its supplemented Guidelines are intended to serve as a basis for ethical decision making in the conduct of professional work. Secondarily, they may serve as a basis for judging the merit of a formal complaint pertaining to violation of professional ethical standards.

It should be noted that although computing is not mentioned in the imperatives of Section 1, the Code is concerned with how these fundamental imperatives apply to one's conduct as a computing professional. These imperatives are expressed in a general form to emphasize that ethical principles which apply to computer ethics are derived from more general ethical principles.

It is understood that some words and phrases in a code of ethics are subject to varying interpretations, and that any ethical principle may conflict with other ethical principles in specific situations. Questions related to ethical conflicts can best be answered by thoughtful consideration of fundamental principles, rather than reliance on detailed regulations.

1 General moral imperatives

As an ACM member I will ...

1.1 Contribute to society and human well-being

This principle concerning the quality of life of all people affirms an obligation to protect fundamental human rights and to respect the diversity of all cultures. An essential aim of computing professionals is to minimize negative consequences of computing systems, including threats to health and safety. When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare.

In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.

1.2 Avoid harm to others

"Harm" means injury or negative consequences, such as undesirable loss of information, loss of property, property damage, or unwanted environmental impacts. This principle prohibits use of computing technology in ways that result in harm to any of the following: users, the general public, employees, employers. Harmful actions include intentional destruction or modification of files and programs leading to serious loss of resources or unnecessary expenditure of human resources such as the time and effort required to purge systems of "computer viruses."

Well-intended actions, including those that accomplish assigned duties, may lead to harm unexpectedly. In such an event the responsible person or persons are obligated to undo or mitigate the negative consequences as much as possible. One way to avoid unintentional harm is to carefully consider potential impacts on all those affected by decisions made during design and implementation.

To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others. If system features are misrepresented to users, coworkers, or supervisors, the individual computing professional is responsible for any resulting injury.

In the work environment the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk. However, capricious or misguided reporting of violations can, itself, be harmful. Before reporting violations, all relevant aspects of the incident must be thoroughly assessed. In particular, the assessment of risk and responsibility must be credible. It is suggested that advice be sought from other computing professionals. See principle 2.5 regarding thorough evaluations.

1.3 Be honest and trustworthy

Honesty is an essential component of trust. Without trust an organization cannot function effectively. The honest computing professional will not make deliberately false or deceptive claims about a system or system design, but will instead provide full disclosure of all pertinent system limitations and problems.

A computer professional has a duty to be honest about his or her own qualifications, and about any circumstances that might lead to conflicts of interest.

Membership in volunteer organizations such as ACM may at times place individuals in situations where their statements or actions could be interpreted as carrying the "weight" of a larger group of professionals. An ACM member will exercise care to not misrepresent ACM or positions and policies of ACM or any ACM units.

1.4 Be fair and take action not to discriminate

The values of equality, tolerance, respect for others, and the principles of equal justice govern this imperative. Discrimination on the basis of race, sex, religion, age, disability, national origin, or other such factors is an explicit violation of ACM policy and will not be tolerated.

Inequities between different groups of people may result from the use or misuse of information and technology. In a fair society, all individuals would have equal opportunity to participate in, or benefit from, the use of computer resources regardless of race, sex, religion, age, disability, national origin or other such similar factors. However, these ideals do not justify unauthorized use of computer resources nor do they provide an adequate basis for violation of any other ethical imperatives of this code.

1.5 Honor property rights including copyrights and patent

Violation of copyrights, patents, trade secrets, and the terms of license agreements is prohibited by law in most circumstances. Even when software is not so protected, such violations are contrary to professional behavior.

Copies of software should be made only with proper authorization. Unauthorized duplication of materials must not be condoned.

1.6 Give proper credit for intellectual property

Computing professionals are obligated to protect the integrity of intellectual property. Specifically, one must not take credit for other's ideas or work, even in cases where the work has not been explicitly protected by copyright, patent, etc.

1.7 Respect the privacy of others

Computing and communication technology enables the collection and exchange of personal information on a scale unprecedented in the history of civilization. Thus there is increased potential for violating the privacy of individuals and groups. It is the responsibility of professionals to maintain the privacy and integrity of data describing individuals. This includes taking precautions to ensure the accuracy of data, as well as protecting it from unauthorized access or accidental disclosure to inappropriate individuals. Furthermore, procedures must be established to allow individuals to review their records and correct inaccuracies.

This imperative implies that only the necessary amount of personal information be collected in a system, that retention and disposal periods for that information be clearly defined and enforced, and that personal information gathered for a specific purpose not be used for other purposes without consent of the individual(s). These principles apply to electronic communications, including electronic mail, and prohibit procedures that capture or monitor electronic user data, including messages, without the permission of users or bona fide authorization related to system operation and maintenance. User data observed during the normal duties of system operation and maintenance must be treated with strictest confidentiality, except in cases where it is evidence for the violation of law, organizational regulations, or this Code. In these cases, the nature or contents of that information must be disclosed only to proper authorities.

1.8 Honor confidentiality

The principle of honesty extends to issues of confidentiality of information whenever one has made an explicit promise to honor confidentiality or, implicitly, when private information not directly related to the performance of one's duties becomes available. The ethical concern is to respect all obligations of confidentiality to employers, clients, and users unless discharged from such obligations by requirements of the law or other principles of this Code.

2 More specific professional responsibilities

As an ACM computing professional I will ...

2.1 Strive to achieve the highest quality, effectiveness, and dignity in both the process and products of professional work

Excellence is perhaps the most important obligation of a professional. The computing professional must strive to achieve quality and to be cognizant of the serious negative consequences that may result from poor quality in a system.

2.2 Acquire and maintain professional competence

Excellence depends on individuals who take responsibility for acquiring and maintaining professional competence. A professional must participate in setting standards for appropriate levels of competence, and strive to achieve those standards. Upgrading technical knowledge and competence can be achieved in several ways: doing independent study; attending seminars, conferences, or courses; and being involved in professional organizations.

2.3 Know and respect existing laws pertaining to professional work

ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so. Policies and procedures of the organizations in which one participates must

also be obeyed. But compliance must be balanced with the recognition that sometimes existing laws and rules may be immoral or inappropriate and, therefore, must be challenged. Violation of a law or regulation may be ethical when that law or rule has inadequate moral basis or when it conflicts with another law judged to be more important. If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.

2.4 Accept and provide appropriate professional review

Quality professional work, especially in the computing profession, depends on professional reviewing and critiquing. Whenever appropriate, individual members should seek and utilize peer review as well as provide critical review of the work of others.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks

Computer professionals must strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Computer professionals are in a position of special trust, and therefore have a special responsibility to provide objective, credible evaluations to employers, clients, users, and the public. When providing evaluations the professional must also identify any relevant conflicts of interest, as stated in imperative 1.3.

As noted in the discussion of principle 1.2 on avoiding harm, any signs of danger from systems must be reported to those who have opportunity and/or responsibility to resolve them. See the guidelines for imperative 1.2 for more details concerning harm, including the reporting of professional violations.

2.6 Honor contracts, agreements, and assigned responsibilities

Honoring one's commitments is a matter of integrity and honesty. For the computer professional this includes ensuring that system elements perform

as intended. Also, when one contracts for work with another party, one has an obligation to keep that party properly informed about progress toward completing that work.

A computing professional has a responsibility to request a change in any assignment that he or she feels cannot be completed as defined. Only after serious consideration and with full disclosure of risks and concerns to the employer or client, should one accept the assignment. The major underlying principle here is the obligation to accept personal accountability for professional work. On some occasions other ethical principles may take greater priority.

A judgment that a specific assignment should not be performed may not be accepted. Having clearly identified one's concerns and reasons for that judgment, but failing to procure a change in that assignment, one may yet be obligated, by contract or by law, to proceed as directed. The computing professional's ethical judgment should be the final guide in deciding whether or not to proceed. Regardless of the decision, one must accept the responsibility for the consequences.

However, performing assignments "against one's own judgment" does not relieve the professional of responsibility for any negative consequences.

2.7 Improve public understanding of computing and its consequences

Computing professionals have a responsibility to share technical knowledge with the public by encouraging understanding of computing, including the impacts of computer systems and their limitations. This imperative implies an obligation to counter any false views related to computing.

2.8 Access computing and communication resources only when authorized to do so

Theft or destruction of tangible and electronic property is prohibited by imperative 1.2 – "Avoid harm to others." Trespassing and unauthorized use of a computer or communication system is addressed by this imperative. Trespassing includes accessing communication networks and computer

systems, or accounts and/or files associated with those systems, without explicit authorization to do so. Individuals and organizations have the right to restrict access to their systems so long as they do not violate the discrimination principle (see 1.4). No one should enter or use another's computer system, software, or data files without permission. One must always have appropriate approval before using system resources, including communication ports, file space, other system peripherals, and computer time.

3 Organizational leadership imperatives

As an ACM member and an organizational leader, I will ...

BACKGROUND NOTE: This section draws extensively from the draft IFIP Code of Ethics, especially its sections on organizational ethics and international concerns. The ethical obligations of organizations tend to be neglected in most codes of professional conduct, perhaps because these codes are written from the perspective of the individual member. This dilemma is addressed by stating these imperatives from the perspective of the organizational leader. In this context "leader" is viewed as any organizational member who has leadership or educational responsibilities. These imperatives generally may apply to organizations as well as their leaders. In this context "organizations" are corporations, government agencies, and other "employers," as well as volunteer professional organizations.

3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities

Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social responsibility. Therefore, organizational leaders must encourage full

participation in meeting social responsibilities as well as quality performance.

3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life

Organizational leaders are responsible for ensuring that computer systems enhance, not degrade, the quality of working life. When implementing a computer system, organizations must consider the personal and professional development, physical safety, and human dignity of all workers. Appropriate human-computer ergonomic standards should be considered in system design and in the workplace.

3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources

Because computer systems can become tools to harm as well as to benefit an organization, the leadership has the responsibility to clearly define appropriate and inappropriate uses of organizational computing resources. While the number and scope of such rules should be minimal, they should be fully enforced when established.

3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements

Current system users, potential users, and other persons whose lives may be affected by a system must have their needs assessed and incorporated in the statement of requirements. System validation should ensure compliance with those requirements.

3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system

Designing or implementing systems that deliberately or inadvertently demean individuals or groups is ethically unacceptable. Computer

professionals who are in decision making positions should verify that systems are designed and implemented to protect personal privacy and enhance personal dignity.

3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems

This complements the imperative on public understanding (2.7). Educational opportunities are essential to facilitate optimal participation of all organizational members. Opportunities must be available to all members to help them improve their knowledge and skills in computing, including courses that familiarize them with the consequences and limitations of particular types of systems. In particular, professionals must be made aware of the dangers of building systems around oversimplified models, the improbability of anticipating and designing for every possible operating condition, and other issues related to the complexity of this profession.

4 Compliance with the code

As an ACM member I will ...

4.1 Uphold and promote the principles of this Code

The future of the computing profession depends on both technical and ethical excellence. Not only is it important for ACM computing professionals to adhere to the principles expressed in this Code, each member should encourage and support adherence by other members.

4.2 Treat violations of this code as inconsistent with membership in the ACM

Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.

This Code and the supplemental Guidelines were developed by the Task Force for the Revision of the ACM Code of Ethics and Professional Conduct:

Ronald E. Anderson, Chair, Gerald Engel, Donald Gotterbarn, Grace C. Hertlein, Alex Hoffman, Bruce Jawer, Deborah G. Johnson, Doris K. Lidtke, Joyce Currie Little, Dianne Martin, Donn B. Parker, Judith A. Perrolle, and Richard S. Rosenberg. The Task Force was organized by ACM/SIGCAS and funding was provided by the ACM SIG Discretionary Fund. This Code and the supplemental Guidelines were adopted by the ACM Council on October 16, 1992.

Glossary

Active cyberdefense A military tactic in which defenders can launch an automatic counterattack against any suspected incursion or attack without waiting for authorization or permission.

Act of war An action by one country against another with the intention to provoke war or an action that occurs during a declared war or armed conflict between military forces of any origin.

Autonomy The ability to act as an individual with free will and without being coerced or controlled by another.

Authentication The use of encryption protocols to ensure that all users of a system or all participants in a transaction are who they say they are. Usually carried out through the issuance of certificates.

Ballot bots Automated programs that create social media accounts with which to disseminate information conforming to or promoting a certain political or agenda.

Black hat hacker Hackers who perform illegal or illicit operations with the intent to harm or destroy.

Bug bounty program A form of sanctioned hacking in which hackers carry out activities aimed at identifying flaws in computer systems, and are rewarded by defending systems for their efforts.

Categorical imperative An ethical standard proposed by Immanuel Kant. Defined as an objective, rationally necessary and unconditional principle that we must always follow despite any natural desires or inclinations we may have to the contrary. (Stanford Encyclopedia of Philosophy)

Computer ethics Normative ethics that are a branch of both practical and professional ethics. This field of ethics pertains to those who study and develop computing expertise and their use of computers and similar forms of technology.

Conventional morality Laws or rules that are viewed as the standard in a group or society because they conform to long-held beliefs and values.

Copyright A form of legal protection on artistic products, branding or labels.

Critical infrastructure Sectors whose assets, systems and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety or any combination thereof. (Department of Homeland Security)

Cybercrime A crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense. (Technopedia, 2017)

Cyberfraud The use of deception for personal gain in online business transactions by assuming a false online identity or by altering or misrepresenting data.

Cyberterrorism The execution of politically-motivated hacking operations intended to cause grave harm that is resulting in either the loss of life or severe economic damage.

Cybertrespass The use of information technology to gain unauthorized access to computer systems or password-protected sites.

Cybervandalism The use of information technology to unleash programs that disrupt the operations of computer networks or corrupt data.

Cyberwarfare Activities of warfare taking place in cyberspace or attacks on conventional targets waged through the use of cyber assets. May include both offensive and defensive operations, including deterrence activities, as well as information operations waged using social media.

Data localization Policies adopted requiring that user data uploaded or provided to the internet will be stored at a facility in the same nation that the user was located in while performing computer activities; this means that the laws regarding safeguarding of citizen information will be in conformity and compliance with the norms where the activity took place.

Data trustee A firm or agency which is legally and ethically responsible for storing and safeguarding personal and corporate user data and making decisions regarding the release and sharing of that data with others.

Deontology Developed by Immanuel Kant, an ethical system sometimes called rule-based ethics. Aims at identifying a universal set of actions which are morally right or wrong regardless of circumstances or intention.

Difference principle Developed by John Rawls, the Difference Principle holds that inequalities in the distribution wealth, responsibility, and power are permissible so long as they benefit the lowest strata of society. (Encyclopedia.com)

Differential surveillance The disparate application of surveillance primarily on the lower classes of society or some other minority group.

Doxing Revealing someone's personal information publicly, without their knowledge or consent.

Dual-use technology Technologies that have both a civilian commercial and military use.

Duty A moral or legal obligation.

Epistemic community A community of academics or professionals bound together through undergoing similar training, sharing specific sets of vocabulary and ideas and belonging to the same professional organizations.

Fair Use The principle that certain ideas or products can be used without payment or licensing fees provided certain limits are adhere to.

Grey area An area of uncertainty where the norms and laws are not yet clear or resolved, often because the problem which is being address is new and/or novel.

Hacktivism The use of computer technology to achieve or publicize a political or social agenda. Often requires the use of illegal or illicit means. Individuals who participate in this type of activity are called 'hactivists.'

Information ethics A system of ethics that pertains to the nature and use of information. (Luciano Floridi)

Informed consent Legal consent to an action with knowledge of possible consequences.

Intellectual property The notion that the originator of an idea owns that idea. He or she is entitled to determine how it is used and to be compensated for its use.

Jurisdiction The territory in which legal decisions can be said to be valid, and where legal authority can be extended and enforced.

Just War A philosophical tradition that posits warfare can be just or moral when in the defense or pursuit of a rightly ordered peace.

Licensing agreement A legal contract specifying the conditions under which a copyright or trademark can be reproduced.

Masquerading Using deception to hide your identity in order to perform an attack.

Moral responsibility The obligation a rational individual has to their moral code or system.

Objectivism An ethical stance which assumes that moral good is real and that it exists independently of culture or opinion. This stance posits that the most moral decision or outcome can be identified or discovered.

Passive defense Protocols for limiting incursions and damage caused by attacks without having an active counterattack protocol.

Philosophy An intellectual discipline which asks broad questions about the nature of knowledge, reality, values, mind, reason and logic.

Piracy Practices by which people upload, download, share, distribute or transmit media or data protected by copyright.

Piracy rate The number of pirated software units divided by the total number of software units put into use, or the percentage of software acquired illegally.

Plagiarism Claiming another person's ideas or intellectual property as your own.

Privacy calculus A theory which suggests that people can rationally decide to 'trade' privacy or their personal information in return for a specific payoff (such as a discount or convenience).

Privacy enhancing technologies (PET) Methods that allow online users to protect the privacy of their personal information. May include encryption or anonymizing protocols.

Propaganda A tool of psychological operations meant to demoralize or coerce enemy civilians and combatants.

Proportionality Applying only as much force as necessary to achieve a goal.

Ransomware Software designed to steal or encrypt data belonging to users, under threat of its destruction or dissemination if a ransom isn't paid.

Thought experiment A way of asking or considering questions in philosophy through creating a hypothetical situation which highlights the problem. It may or may not be realistic.

Trolley problem A thought experiment originally proposed by philosopher Philippa Foot. The problem is designed to present scenarios in which individual rights might be sacrificed for a greater social or communal good and the limits of this approach.

Ubiquitous computing The notion that individual and corporate users are surrounded by technologies which collect user data as these technologies are incorporated into more everyday devices. Users may be unaware of these activities which may occur without their knowledge or consent to data sharing.

Uniqueness debate A debate in computer ethics about the degree to which ethical theories, dilemmas and values can be transferred from real-world situations to those in cyberspace. Some argue that technology dilemmas are merely extensions of preexisting ethical problems while others argue that cyberspace creates a new class of ethical and moral phenomena, requiring the development of new tools and concepts to address them.

Use of force The ability of a state to wield violence as a coercive tool.

Utilitarianism A system of ethics where the utility of actions can be measured to determine their moral quality.

Veil of ignorance Developed by John Rawls, the 'veil of ignorance' is an approach to ethical decision making in which the decision maker is charged to act as though he does not know his or her own position in a scenario. Thus, he or she is charged with creating an outcome which benefits all, particularly the weakest and most vulnerable actors in a transaction.

Virtue ethics A philosophical approach which states that the most moral outcome is that which is in keeping with an individual's values. In this approach, the goal of ethics is to develop an individual's moral character.

Index