An Introduction to Cybersecurity Ethics

MODULE AUTHOR:
Shannon Vallor, Ph.D.
William J. Rewak, S.J. Professor of Philosophy, Santa Clara University

TABLE OF CONTENTS

An Introduction to Cybersecurity Ethics

MODULE AUTHOR:
Shannon Vallor, Ph.D.
William J. Rewak, S.J. Professor of Philosophy, Santa Clara University

1. What do we mean when we talk about 'ethics'?

Ethics in the broadest sense refers to the concern that humans have always had for figuring out *how best to live*. The philosopher Socrates is quoted as saying in 399 B.C. that "the most important thing is not life, but the good life."[1] We would all like to avoid a bad life, one that is shameful and sad, fundamentally lacking in worthy achievements, unredeemed by love, kindness, beauty, friendship, courage, honor, joy, or grace. Yet what is the best way to obtain the opposite of this – a life that is not only *acceptable*, but even excellent and worthy of admiration? How do we identify a *good* life, one worth choosing from among all the different ways of living that lay open to us? This is the question that the study of ethics attempts to answer.

Today, the study of ethics can be found in many different places. As an academic field of study, it belongs primarily to the discipline of philosophy, where it is studied either on a **theoretical** level ('what is the best theory of the good life?') or on a **practical, applied level** as will be our focus ('how should we act in this or that situation, based upon our best theories of ethics?'). In community life, ethics is pursued through diverse cultural, political and religious ideals and practices, through which particular social groups give their members guidance about how best to live. On a personal level, it can be found in an individual's self-reflection and continual strivings to become a better person. In work life, it is often formulated in formal codes or standards to which all members of a profession are held, such as those of medical or legal ethics. Professional ethics is also taught in dedicated courses, such as business ethics. Ethics can also be infused into courses such as this one.

2. What does ethics have to do with *technology*?

There is a growing international consensus that ethics is of increasing importance to education in technical fields, and that it must become part of the language that technologists are comfortable using. Today, the world's largest technical professional organization, IEEE (the Institute for Electrical and Electronics Engineers), has an entire division devoted just to **technology ethics**.[2] In 2014 IEEE began holding its own international conferences on ethics in engineering, science, and technology practice. To supplement its overarching professional code of ethics, IEEE is also working on **new ethical standards** in emerging areas such as AI, robotics, and data management.

What is *driving* this growing focus on technology ethics? What is the reasoning behind it? The basic rationale is really quite simple. Technology **increasingly shapes *how* human beings seek the good life**, and with what degree of success. Well-designed and well-used technologies can make it easier for people to live well (for example, by allowing more efficient use and distribution of essential resources for a good life, such as food, water, energy, or medical care). Poorly designed or misused technologies can make it harder to live well (for example, by

[1] Plato, *Crito* 48b.

[2] https://techethics.ieee.org

toxifying our environment, or by reinforcing unsafe, unhealthy or antisocial habits). **Technologies are not ethically 'neutral'**, for they reflect the values that we 'bake in' to them with our design choices, as well as the values which guide our distribution and use of them. Technologies both reveal and shape what humans value, what we think is 'good' in life and worth seeking.

Of course, this always been true; technology has never been separate from our ideas about the good life. We don't build or invest in a technology hoping it will make no one's life better, or hoping that it makes all our lives worse. **So what is new, then?** Why is ethics now such an important topic in technical contexts, more so than ever?

The answer has partly to do with the unprecedented **speeds and scales** at which technical advances are transforming the social fabric of our lives, and the inability of regulators and lawmakers to keep up with these changes. Laws and regulations have historically been important instruments of preserving the good life within a society, but today they are being outpaced by the speed, scale, and complexity of new technological developments and their often hard-to-predict social impacts.

Additionally, many lawmakers lack the **technical expertise** needed to guide effective technology policy. This means that technical experts are increasingly called upon to help anticipate those social impacts and to think proactively about how their technical choices are likely to impact human lives. This means making ethical design and implementation choices in a dynamic, complex environment where the few legal 'handrails' that exist to guide those choices are often outdated and inadequate to safeguard public well-being.

For example: face- and voice-recognition algorithms can now be used to track and create a lasting digital record of your movements and actions in public, even in places where previously you would have felt more or less anonymous. There is no consistent legal framework governing this kind of data collection, even though such data could potentially be used to expose a person's medical history (by recording which medical and mental health facilities they visit), their religiosity (by recording how frequently they attend services and where), their status as a victim of violence (by recording visits to a victims services agency) or other sensitive information, up to and including the content of their personal conversations in the street. **What does a person given access to all that data, or tasked with keeping it secure, need to understand about its ethical significance and power to affect a person's life?**

Another factor driving the recent explosion of interest in technology ethics is the way in which 21st century **technologies are reshaping the global distribution of power, justice, and responsibility**. Companies such as Facebook, Google, Amazon, Apple, and Microsoft are now seen as having levels of global political influence comparable to, or in some cases greater than, that of states and nations. In the wake of revelations about the unexpected impact of social media and private data analytics on 2017 elections around the globe, the idea that technology companies can safely focus on profits alone, leaving the job of protecting the public interest wholly to government, is increasingly seen as naïve and potentially destructive to social flourishing.

Not only does technology greatly impact our opportunities for living a good life, but its **positive and negative impacts are often distributed unevenly** among individuals and groups. Technologies can generate widely disparate impacts, creating 'winners' and 'losers' in the social lottery or magnifying existing inequalities, as when the life-enhancing benefits of a new technology are enjoyed only by citizens of wealthy nations while the life-degrading burdens of environmental contamination produced by its manufacture fall upon citizens of poorer nations. In other cases, technologies can help to create fairer and more just social arrangements, or create new access to means of living well, as when cheap, portable solar power is used to allow children in rural villages without electric power to learn to read and study after dark.

How do we ensure that access to the enormous benefits promised by new technologies, and exposure to their risks, are distributed in the right way? This is a question about technology ***justice***. Justice is not only a matter of law, it is also even more fundamentally a matter of *ethics.*

3. What does ethics have to do with cybersecurity?

Cybersecurity practices have as their aim the securing—that is, the *keeping safe*—of data, computer systems and networks (software and hardware). While those data, systems, and networks might have some economic or other value in and of themselves, what cybersecurity practices *primarily* protect are the integrity, functionality, and reliability of human institutions/practices that *rely upon* such data, systems, and networks. And in protecting those institutions and practices, cybersecurity professionals in turn are protecting the lives and happiness of the human beings who depend upon them.

If you are a cybersecurity professional tasked with securing a hospital's network and critical data from invasion and attack, you are intimately involved in protecting sick patients, even if you have no medical training. Patients' privacy, health, even their survival can hinge upon your success or failure. In many cases the well-being of patients' families and caregivers is being shielded by your practice as well. This is a particularly stark example, but cybersecurity practices and professionals are also critical to the protection of credit users, students, power and water customers, voters, investors, inventors, drivers, train and airplane passengers—basically *all of us.*

This means that **ethical issues are at the core of cybersecurity practices**, because these practices are increasingly required to secure and shield the ability of human individuals and groups to live well. And given the increasing complexity and difficulty of securing online data and systems across a proliferating landscape of cloud computing services, WiFi-enabled mobile devices, and 'smart' objects—from a multiplicity of hostile actors exploiting lax or under-resourced security controls—the ethical responsibility to protect others that is borne by cybersecurity professionals is an increasingly *heavy* burden.

For example, which of these life-impacting events might result from cybersecurity practices?

A. Kent, a hard-working first-generation college senior, has just requested that copies of his university transcript be sent to the ten graduate schools to which he has applied. Kent does not know that he was recently the victim of a malicious and undetected intruder into his university's network; as a prank, the intruder changed a random selection of students' course grades to an 'F.'

B. Desiree, a middle-aged mother of two, applies for a loan to start a new small business. She has a promising and novel business plan, a nest egg of savings, and a few key investors who are ready to sign on. The bank checks her credit report on file with a major credit bureau, finds it excellent, and approves her startup loan; her investors commit and she launches what in ten years will have become a beloved and highly profitable franchise. Desiree never learns that an attempted theft of the sensitive personal data in her credit file was thwarted by the credit bureau's cybersecurity team five years prior.

C. Due to a massive network outage caused by DDoS attacks, the **Porters,** a Texas farming family, are unable to access critical weather updates, including evacuation orders, during an unusually intense hurricane that is takes an unexpected turn toward their local area. By the time the family turns on their emergency radio and learns of the imminent danger they are in, the local access roads to the highway have become impassable, and they have nowhere to go as the unprecedented floodwaters surround their farmhouse.

D. A phishing email opened by **Casey**, a mid-level manager at a subcontractor for a major aeronautics manufacturer, infects the internal company network with malware. The malware targets and modifies a particular kind of file used in updates to autopilot systems.

E. Dev and Katia, a pair of talented freelance hackers, identify a previously unknown but easily fixed vulnerability in the current operating system of a particular manufacturer's mobile phones, which allows the remote injection and execution of malicious code. As they discuss what they should do next—contact the affected the manufacturer via a backchannel, notify a popular tech media news site, or expose the vulnerability on their own cybersecurity blog—Dev and Katia are approached by a friend, who works for the phone manufacturer's primary competitor. The friend offers them both lucrative jobs, on the condition that they remain silent about the exploit they have found.

Which of these hypothetical cases raise ethical issues concerning cybersecurity? The answer, as you probably have guessed, is **'All of them.'** In each of these examples, one or more unsuspecting persons' chances of living good lives are profoundly impacted by what cybersecurity professionals and other actors in the information security space have or have not done—or by what they *will* or will *not* do.

In some of these cases it is obvious how good cybersecurity practices might have prevented or limited the harm done to others; in other cases this is less clear. Cybersecurity professionals are challenged ethically on multiple levels. First, they are challenged by technical quandaries that have ethical *implications*: which security techniques are most likely to be effective, and what resources do they require? How can we keep up with an ever-escalating 'arms race' between network intruders and defenders? Since virtually no computer system can be made 100% secure, what levels and types of security risk are acceptable to tolerate? To what extent and in what ways must users of the system and other affected stakeholders be made aware of the risks?

In other cases the challenges are not technical at all, but *directly* ethical—can I ever justify exposing others to a greater risk of a breach for my own personal profit, or to avoid costs to my company? How do I balance competing duties to my employer, my nation, or the human family at large? What levels of care must I take to perform my role responsibly?

A broader and better understanding of cybersecurity ethics is therefore essential to promoting and protecting human flourishing in an increasingly networked society.

This free module, developed at the Markkula Center for Applied Ethics at Santa Clara University in Silicon Valley, is one contribution to meeting this growing need. It provides an introduction to some key issues in cybersecurity ethics, with working examples and questions for students that prompt active ethical reflection on the issues. Instructors and students using the module do not need to have any prior exposure to applied ethics or ethical theory to use the module. However, this is only an introduction; **thinking about cybersecurity ethics can begin here, but it should not *stop* here**. One big challenge for teaching cybersecurity ethics is the immense territory the subject covers, given the ever-expanding variety of contexts in which cybersecurity is needed. Thus **no single set of ethical rules, guidelines, or insights can provide guidance in all cybersecurity circumstances**; **such knowledge must always be actively and intelligently adapted and applied to particular cybersecurity contexts and problems 'in the wild.'**

This is why many companies, government institutions, universities, non-profit agencies, and professional societies whose members develop or rely upon cybersecurity practices are funding an increasing number of their own cybersecurity ethics-related programs and training tools. Links to many of these resources can be found in **Appendix A** to this module. **These resources can be used to build upon this introductory module and provide more detailed and targeted ethical insights for cybersecurity professionals.**

In the remaining sections of this module, you will have the opportunity to learn more about:

Part 1: Important ethical issues in cybersecurity

Part 2: Common ethical challenges faced by cybersecurity professionals

Part 3: Cybersecurity professionals' ethical obligations to the public

Part 4: General frameworks for ethical thinking and reasoning in cybersecurity contexts

Part 5: Ethical 'best practices' for cybersecurity professionals

In each section of the module, you will be asked to fill in answers to specific questions and/or examine and respond to case studies that pertain to the section's key ideas. This will allow you to practice using all the tools for ethical analysis and decision-making that you will have acquired from the module.

PART ONE

What are the important ethical issues in cybersecurity?

1. What makes an ethical issue 'important' or 'significant'?

In the Introduction we saw that the 'good life' is what ethical action seeks to protect and promote. We'll say more later about the 'good life' and why we are ethically obligated to care about the lives of others beyond ourselves.

But for now, we can **define an ethical issue as 'important' or 'significant'** when its associated harms or benefits have a substantial possibility of making a difference to certain individuals' chances of having a good life, or the chances of a group to live well: that is, to flourish in society together. Some harms and benefits are not ethically significant. Say I prefer Coke to Pepsi. If I ask for a Coke and you hand me a Pepsi, even if I am disappointed, you haven't impacted my life in any ethically significant way. Some harms and benefits are too trivial to make a meaningful difference to how our life goes. Also, **ethics implies human choice**; a harm that is done to me by a wild tiger or a bolt of lightning might be very significant, but won't be ethically significant, for it's unreasonable to expect a tiger or a bolt of lightning to take my life or welfare into account.[3]

In many technical contexts, such as the engineering, manufacture, and use of aeronautics, nuclear power containment structures, surgical devices, buildings, and bridges, it is very easy to see the ethically significant harms that can come from poor technical choices, and very easy to see the ethically significant benefits of choosing to follow the best technical practices known to us. All of these contexts present obvious issues of 'life or death' in practice; innocent people will die if we disregard public welfare and act negligently or irresponsibly, and people will generally enjoy better lives if we do things right.

Because 'doing things right' in these contexts preserves or even enhances the opportunities that other people have to enjoy a good life, **good technical practice in such contexts is also *ethical* practice.** A civil engineer who willfully or recklessly ignores a bridge design specification, resulting in the later collapse of said bridge and the deaths of a dozen people, is not just bad at his or her job. Such an engineer is also guilty of an *ethical failure*—and this would be true even if they just so happened to be shielded from legal, professional, or community punishment for the collapse.

In the context of cybersecurity practice, the potential harms and benefits are no less real or ethically significant, up to and including matters of life and death. But due to the fact that cybersecurity efforts are often carried out 'behind the scenes,' largely hidden away from customers, clients, and other users, the ethical nature of cybersecurity practice can be harder to recognize. This part of the module seeks to make these issues more visible.

[3] Even acts performed without direct intent, such as driving through a busy crosswalk while drunk, or unwittingly exposing sensitive user data to hackers, can involve ethical choice (e.g., the reckless choice to drink and get behind the wheel, or the negligent choice to use outdated cybersecurity tools)

2. What significant ethical benefits and harms are linked to cybersecurity efforts?

One way of thinking about benefits and harms is to understand what our ***life interests*** are. Like all animals, humans have significant vital interests in food, water, air, shelter, and bodily integrity. But we also have strong life interests in our health, happiness, family, friendship, social reputation, liberty, autonomy, knowledge, privacy, economic security, respectful and fair treatment by others, education, meaningful work, and opportunities for leisure, play, entertainment, and creative and political expression, among other things.[4]

Cybersecurity practices can significantly impact each of these fundamental interests of human beings. In this respect, then, **cybersecurity has a broader ethical sweep** than some of the stark examples of technical practice given earlier, such as the engineering of bridges. Unethical design choices in building bridges can destroy bodily integrity and health, and through such damage make it harder for people to flourish, but unethical choices in cybersecurity contexts can cause many more *different* kinds of harm. While cybersecurity failures could in certain scenarios cost me my life, as we noted in the Introduction, they could also leave my body physically intact but my reputation, savings, or liberty destroyed. Effective cybersecurity practices can also generate a vast range of *benefits* for society at large, including safer infrastructure, reduced social and economic anxiety, and increased investment and innovation.

1. IMPORTANT ETHICAL ISSUES IN CYBERSECURITY

A. HARMS TO PRIVACY: Thanks to the ocean of sensitive data that persons and organizations are generating today (or, to use a better metaphor, the many different lakes, springs, and rivers of data that are pooling and flowing across the digital landscape), most of us do not realize how exposed our lives and property are, or can be, by poor cybersecurity practices.

Some of the most common cyberthreats to privacy include **identity theft**, in which personally identifying information is stolen and used to impersonate victims in financial transactions (taking out loans in a victim's name or using their credit cards to make unauthorized purchases), or for other illegitimate purposes, such as providing criminals with stolen identities. Hacking and other network intrusions can also be used to obtain sensitive information about individuals and their activities that can be used for the purposes of **blackmail**, **extortion,** and other forms of unethical and/or illegal manipulation of people's will. Privacy violations of this sort are often used to get victims to harm the interests of third-parties, for example, using blackmail to pressure compromised employees to betray sensitive client information, trade secrets, or engage in other forms of **corporate or government espionage and misconduct**.

The risks of privacy harm created by poor or unethical cybersecurity practices are amplified further by the continued growth of a **chaotic global data ecosystem** that gives most individuals little to no ability to personally curate, delete, correct, or control the storage or release of their private information. Only thin, regionally inconsistent, and weakly enforced sets

[4] See Robeyns (2016) https://plato.stanford.edu/entries/capability-approach/) for a helpful overview of the highly influential capabilities approach to identifying these fundamental interests in human life.

of data regulations and policies protect us from the **reputational, economic, and emotional harms** that release of sensitive data into the wrong hands can cause. Even *anonymized* data can, when linked or merged with other datasets, reveal intimate facts (or in many cases, *falsehoods*) about us. **Privacy isn't just about our online activities, either.** Facial, gait, and voice-recognition algorithms, as well as geocoded mobile data, can now identify and gather information about us as we move and act in many public and private spaces.

It is important to note that privacy harms do not only threaten those whose sensitive information is directly exposed to cyberthreats; even those who try to live 'off the digital grid' cannot prevent sensitive data about them from being generated and shared by their friends, family, employers, clients, and service providers. For example, individuals who themselves practice stringent personal data security and encryption of their sensitive data might be targeted through their medical provider or law firm, where sensitive data about them may be stored less securely. In networked societies, **sensitive data rarely stays confined to the digital context in which it was originally created or shared**.

This puts an immense amount of pressure on cybersecurity professionals, who are increasingly **trusted to supply the critical line of defense against personal and organizational privacy harms.** Because personal control and containment of sensitive data is often virtually impossible to maintain in networked environments, especially without the benefit of highly specialized training and advanced cybersecurity tools, the ethical responsibility of preventing irreparable privacy harm falls increasingly upon cybersecurity professionals rather than the original 'owners' of sensitive data.

Therefore, poor cybersecurity practices, from lax patching efforts and outdated encryption tools to a lack of incident response planning, can be more than just ineffective—they can be *unethical*, insofar as they *unnecessarily* or *negligently* expose others to profound personal and organizational privacy harms. **In Part Two of this module, we'll discuss some of the specific challenges that avoiding privacy harms presents for cybersecurity practitioners, and explore possible tools and solutions.**

B. HARMS TO PROPERTY: We saw above that property can be indirectly threatened by violations of data privacy, through mechanisms such as extortion. However, often property is directly targeted through cyberintrusions that may seek to misappropriate electronic funds, steal valuable intellectual property such as trade secrets, obtain bank account numbers and passwords, or remotely cause damage or destruction to an individual or organization's digital or physical property. The motivations for such harms vary widely: such property may be targeted by profit-seeking criminal enterprises; by politically-motivated groups of non-state actors; by agents of corporate espionage; by hostile military or intelligence agents of foreign nations; or by the aggressive impulses of a lone hacker or collective seeking to demonstrate their own destructive power.

It is important to recognize that unauthorized harms to property are, *typically*, significant ethical harms; they injure *persons* who rely upon such property to secure good lives for themselves or others. Property may not be of intrinsic ethical value, as human lives are, but we frequently have good reason to consider unauthorized damage to property to be unethical—even in cases when it is not strictly or explicitly prohibited by law.

There are rare cases in which the unauthorized destruction of property might be argued by some to be ethically justified by a higher moral duty, such as national security interests. Presumably, for example, this is the kind of claim that was made by the agents of the nation state or states responsible for using the Stuxnet worm in 2010 to disable Iranian centrifuges being used as part of Iran's efforts to enrich uranium. In other cases, defenders of a network under cyberattack might assert an ethical right to 'hack back' in ways that aim to damage the systems of the cyberattacker.

Even in such cases, however, cyberintrusions that target property generate significant ethical concerns; for example, consider the fact that the release of the Stuxnet worm also infected hundreds of thousands of *other* computers of individuals and organizations unrelated to the Iranian nuclear program. Likewise, 'hacking back' has been challenged as creating an unacceptable risk to innocent parties, since its collateral effects are usually unknown and since cyberattacks often involve 'spoofing' strategies that make it easy to misidentify the system responsible for the attack. Regardless of the validity of arguments for and against so-called 'defensive' cyberattacks on property, **professionals tasked with cybersecurity have a default ethical obligation to protect their organization's networks, or those of their clients, from any and all property-targeting intrusions and attacks.**

C. CYBERSECURITY RESOURCE ALLOCATION: Another ethical issue that must always inform cybersecurity practice is the inevitably high *cost* of cybersecurity. Cybersecurity efforts consume considerable individual and organizational resources: time, money, and expertise. They also impose considerable costs on system resources: cybersecurity efforts can negatively impact data storage capacity, network and download speeds, power efficiency, and system usability/reliability. Of course, *not* having effective cybersecurity measures in place typically imposes even *higher* and more unacceptable costs. Still, a network that is maximally secure but as a result is practically unusable, or economically unsustainable, can normally not be justified—just as it would *normally* not be reasonable or justifiable to secure a bank by boarding up and padlocking all of the doors.

That said, in *some* cases, even usability/product viability concerns can't justify weakening security standards. If, for example, my company wants to make a Wi-Fi enabled pacemaker, but simply lacks the resources necessary to make that product both effective *and* reasonably secure from hackers, then there is a strong ethical argument that my company should not be in the business of making Wi-Fi enabled pacemakers. In that case, a cybersecurity professional who signed off on or otherwise enabled lax security controls on such a device would also be violating ethical standards, since he or she would be well aware of the unacceptable risk of grave harm to others that his or her action creates.

If it's not clear how the issue of resource allocation can be an *ethical* issue, consider the stakes involved in getting the right balance between security and other competing resource needs. If a hospital network security administrator gets spooked by a suspicious port scan of the network and decides to respond to the possible threat by immediately instituting a new and extremely time-consuming security logon procedure, without first considering the core function and interests of users of the network, they could be endangering patient's lives, especially in departments where quick network access is needed in order to use life-saving medicines or equipment.

Thus the task of identifying a justifiable balance between well-resourced cybersecurity and other kinds of functionality is an *ethical* one, since it requires reflecting carefully upon the harms, benefits, rights and values involved in such a decision, and the likely impact of the decision on the ability of others to seek and lead good lives.

D. TRANSPARENCY AND DISCLOSURE: Another set of ethical issues in cybersecurity practice has to do with our general but limited obligations of *transparency* in practices that affect the well-being of other people. Because cybersecurity is a form of risk management, and because those risks significantly impact other parties, there is a default ethical duty to disclose those risks when known, so that those affected can make informed decisions. For example, it is *generally* agreed to be the case that if an organization discovers a critical vulnerability in its software, it should notify its customers/clients of that discovery in a timely fashion so that they can install a patch (if available) or take other defensive measures.

Yet in many cases the appropriate mode and extent of the disclosure, and what counts as a 'timely' notification, is subject to considerable debate. For example, in a case where a vulnerability would be very challenging to discover and exploit by a third party, cannot yet be patched by the security team, and involves a critical network of high utility to customers, a delay in notification until a patch is available may be ethically defensible, since premature disclosure would potentially invite an attack that would otherwise not be forthcoming, creating a *higher* risk of harm to others.

Although there are some *general* transparency and disclosure guidelines that can be helpful to consider, as articulated in Section V, it remains the case that because each cybersecurity scenario involves different facts, and places different goods and interests at stake, there is no 'one-size-fits-all' rule or instruction that one can follow to guarantee appropriately transparent cybersecurity practice. This means that typically, what is required in each case is careful ***ethical reflection*** on the particular scenario and the specific risks, benefits, tradeoffs, and stakeholder interests involved, followed by a well-reasoned **ethical *judgment*** about what is best to do, given the particular facts and options.

E. CYBERSECURITY ROLES, DUTIES, AND INTERESTS: Cybersecurity practices involve a number of distinct roles and interests, some of which are in tension with one another. In such cases it can be unclear what our ethical duties are, to whom we owe the greatest ethical concern, and whose interests we should be most invested in protecting. The variety of roles and subcultures of cybersecurity practice can also generate confusion about the ethical standards of the cybersecurity community. Careful ethical reflection is necessary to sort through such confusions and arrive at justifiable decisions in particular cases.

For example, there has long been a debate about the ethical standards of the 'hacker' community, a debate amplified by the divergent subcommunities of those who identify as 'white-hat,' 'black-hat,' or 'gray-hat' hackers. The joint origin of hacking and security practices among individual computer hobbyists and informal collectives makes the need to develop clear community standards within an emerging cybersecurity *profession* especially complicated. Many cybersecurity professionals have occupied multiple and competing roles in the development of their own security skillset and knowledge base; they may feel conflicting loyalties to the interests of the public, government agencies, their employers or clients, and to particular subcultures and interest groups within the security community, not to mention their own personal interests. The market for 'zero-day' exploits perfectly embodies the complex ethical landscape of cybersecurity, in which financial incentives are given both for creating *and* exposing potentially harmful cybertools.

Illustrations of tensions among different roles and interests in the cybersecurity community are easy to come by. One cybersecurity researcher may have a strong desire to publish a formerly unknown method of undermining a popular encryption key management system, for the sake of improving the community's knowledge base and spurring research into countermeasures. Yet the same researcher may also have clients of his or her cybersecurity consulting firm who would be placed at greater risk by such a disclosure. Or consider a chief information security officer (CISO) who wishes to hire for his or her 'Red Team' of penetration testers a brilliant young hacker whose skills are unparalleled, but whose professionalism and ethical values are still underdeveloped; the CISO hopes to mentor this person fully into the culture of 'white-hat' cybersecurity practice, giving more ammunition to the 'good guys,' but knows there is a real risk of failure—one that could expose his or her employer to an internal breach. How should the CISO make this call?

All of the issues outlined above in Part One involve ethical choices that must be made by cybersecurity professionals, choices that significantly impact the lives and welfare of others. **All of these ethical issues are highly complex and variable, although this does *not* mean that they are therefore *subjective*.** There are many responses to cybersecurity issues that are clearly ethically *wrong*. Others are clearly ethically dubious, or fall short of what we would expect from any respected cybersecurity professional. Still, finding cybersecurity solutions that are clearly *right* or *justifiable* by reasonable professional standards can be challenging, and requires careful ethical reflection, analysis, and problem-solving. The function of this module is to illustrate the critical need for those skills in cybersecurity, and to give students some initial practice in using them.

Finally, the range of ethical issues in cybersecurity is by no means *limited* to those we have focused on in Part One. **Cybersecurity professionals need to be attentive to the many ways in which their practices can significantly impact the quality of people's lives**, and must learn to better anticipate their potential harms and benefits so that they can be effectively addressed.

On the next page, you will get some practice in doing this yourself.

Case Study 1

Leslie is a cybersecurity consultant approached by a new startup, BioHack, which plans to develop a revolutionary but controversial new consumer product: a subdermal implant that will broadcast customers' personally identifying information within a 10-foot range, using strong encryption that can only be read and decrypted by intended receivers using special BioHack-designed mobile scanning devices. Users will be able to choose what kind of information they broadcast, but two primary applications will be developed and marketed initially: the first will broadcast credit card data enabling the user to make purchases with the wave of a hand. The second will broadcast medical data that can notify emergency first responders of the users' allergies, medical conditions, and current medications. The proprietary techniques that BioHack has developed for this device are highly advanced and must be tightly secured in order for the company's future to be viable. However, BioHack's founders tell Leslie that they cannot presently afford to hire a dedicated in-house cybersecurity team, though they fully intend to put one in place before the product goes to market. They also tell Leslie that their security budget is limited due to the immense costs of product design and prototype testing, so they ask her to recommend FOSS (free open-source software) solutions for their security apparatus and seek other cost-saving measures for getting the most out of their security budget. They also tell her that they cannot afford her full consulting fee, so they offer instead to pay her a more modest fee, plus a considerable number of shares of their company stock.

Question 1.1:
What risks of ethically significant *harm*, as defined in Part One, are involved in this case? *Who* could be harmed if Leslie makes poor choices in this situation, and *how*? What potential *benefits* to others should she consider in thinking about BioHack's proposal?

Question 1.2:
Beyond the specific harms noted in your answer to 1.1, what are some ethical *concerns* that Leslie should have about the proposed arrangement with BioHack? Are there any ethical 'red flags' she should notice?

Question 1.3:
What are three *questions* that Leslie should ask about the ethics of her involvement with BioHack before deciding whether to accept them as clients (and if so, on what terms?)

Question 1.4:
Can you think of any specific *conditions* that Leslie should ask BioHack's founders to agree to before she can ethically accept this arrangement? What are they?

PART TWO

Common ethical challenges for cybersecurity professionals

We saw in Part One that a broad range of ethically significant issues are associated with cybersecurity practices. Here in Part Two, we will see how those issues generate ten types of common ethical challenges encountered by cybersecurity professionals.

It is important to note that **even when a cybersecurity practice is legal, it may not be *ethical.*** Unethical or ethically dubious cybersecurity practices can result in significant harm and reputational damage to network users, clients, companies, the public, and cybersecurity professionals themselves.

These are the just *some* of the common ethical challenges that we must prepared to address through the ethical 'best practices' we will summarize in Part Five. They have been framed as ***questions***, since these are the questions that cybersecurity professionals will frequently need to ask themselves in real-world contexts, in order to ensure ethical and effective cybersecurity practice.

1. Ethical Challenges in Balancing Security with Other Values:

Have we struck an ethically acceptable balance, all things considered, between the value of cybersecurity and other values that may be in tension with it, including network/device usability, reliability, speed, and other resource needs of the organization and its stakeholders?

Have we had honest conversations with our clients/customers/employers/users about how this balance will be struck? Or have we given these stakeholders a false sense of security, or made promises about security/system functionality that we cannot keep?

If there is a serious breach of our system or other security violation leading to significant harm, will we be able to justify our security resource allocations to affected stakeholders (system users, clients, customers, investors, the Board, the media, members of the general public)? Or will we be rightly judged as having been unprepared and negligent in our provisions for cybersecurity?

Do our actions reflect consistency, sincerity, and transparency in our value commitments, or upon inspection will they reveal arbitrary, inconsistent, insincere, or deceptive professions of value? For example, if our organization or team takes a strong public stand on privacy protection of user emails from third-party requests by law enforcement, have we fully committed to the implications of that stand? Are we also willing to forgo, for example, our own internal monitoring of user emails for security purposes? Can any apparent disparities in value commitment be justified and explained with compelling ethical reasoning from principles that will withstand public critique?

2. Ethical Challenges in Threat/Incident Response:

Do we have an appropriate *incident response plan,* for each type of threat or incident that we anticipate facing? Do these include *concrete action plans for the worst-case-scenarios,* including mitigation strategies to limit or remedy harms to others if our best efforts at preventing a breach/attack fall short?

Do we have adequate resources and systems in place to successfully *implement* our incident response plan? Or does our plan only reflect what we'd *like* to be able to do in response to a threat or security breach, not what we actually *can* and *are prepared* to do? How much of a gap between these is ethically acceptable?

What are the ethical gray areas we face in our incident response practice? How aggressive can we justifiably be in repelling and discouraging attacks? Have we adequately considered the risks of 'collateral damage' to innocent parties, or reputational damage to ourselves and our organization, if our response steps over the ethical line?

How will we respond to ransomware attacks affecting our network or users? When, if ever, is it ethically right to pay ransoms to attackers to restore system functionality or access? How much burden should be put on users/clients to protect and consistently backup their own data on other devices, as a way of limiting ransomware vulnerability?

3. Ethical Challenges in Security Breach/Vulnerability:

Do we have an ethically sound plan for when and how to notify network/software users and other stakeholders of security incidents, including breaches and vulnerabilities? What ethical conditions must be met in order to justify a delay of notification, or a notification that is selective and not made public?

How do we meet the need for reporting that is *accurate*, *timely*, and *helpful*? Do we have an efficient system in place for rapidly investigating and planning an effective response to an incident, or is our response likely to be slowed down by internal confusion, disorder, and disagreement about what has really happened and what needs to be done? Do we have good protocols in place for communicating to affected stakeholders how they can obtain more information and assistance, or what measures they should take to protect themselves from further risk of harm?

Have we considered not only our own perspective, but the likely perspective of other stakeholders? Is a delay or selective notification of a breach or vulnerability likely to cause damage downstream to public, client, or user trust in our services, our product, or our organizational values, even if at the time we think our reasoning is ethically sound?

Have we identified the ethically appropriate balance between *overreaction* to breaches and vulnerabilities and *underreaction*? Is our team predisposed to dismiss signs of a possible breach as false positives, or to discount the true risk to others posed by a vulnerability? When we disclose a critical security flaw, is it labeled as 'critical', or do we often downgrade it to 'moderate'? Do we exaggerate security risks to get more resources? Or do we fully and appropriately weigh the actual risks and avoid 'wishful thinking' in our security environment?

4. Ethical Challenges in Network Monitoring and User Privacy:

How can we monitor our network effectively without ourselves making unjustifiable intrusions upon users and their privacy? Should users of the network have their emails read, or their keystrokes logged, or their physical locations or website visits tracked? Or are these measures excessively intrusive and unjustifiable, all things considered?

How should we monitor and control network activity on personal devices such as laptops and cell phones not owned by our organization and legitimately used for many other purposes, as opposed to devices that are the business property of the organization?

To what extent should users of the network be made aware of our security monitoring activities? How does this change depending on who the users are (employees, customers, members of the general public, or clients bearing their own privacy duties to others, such as lawyers and health care professionals)?

5. Ethical Challenges with Competing Interests & Obligations:

Have we adequately *reflected on the ethical harms* that may be done by a security breach, both in the short-term and long-term, and to whom? Are we taking into account the significant interests of *all* stakeholders who may be affected, or have we overlooked or discounted some of these impacts in favor of the interests of others?

What should we do if asked by an employer or client to grant someone a level of system access privileges that we have good reason to think are inappropriate, or that place the security of other parties at undue risk?

What should we do if asked by an employer or client to put off disclosure of a serious or critical system vulnerability, or to delay a patch, in order to protect the company's reputation, stock price or investor commitment?

What will we do if we are asked to violate a professional duty of cybersecurity practice in the interests of national security, or some other non-professional ethical interest? How will we evaluate such requests to determine the ethically acceptable response? What costs must we be willing to bear to carry out our highest ethical duties to others?

What sorts of compensation arrangements for cybersecurity services might create a conflict of interest between myself and those I am professionally bound to protect, or the appearance of such a conflict?

6. ETHICAL CHALLENGES IN DATA STORAGE AND ENCRYPTION:

How can we responsibly and safely store and transmit sensitive information? Are data subjects, customers and clients given clear and accurate information about our encryption, key management and data storage practices?

Do we take adequate care in contracting with third parties (for encryption tools, security audits, cloud services or physical servers, etc.), considering not simply cost but reputation and reliability of third party services, especially those located in countries where stability of infrastructure or political and legal protections may be an issue?

What are the ethical risks and benefits associated with various forms and strengths of encryption we might use? Are our encryption practices well-aligned with industry standards? Are those standards themselves adequate/ethically defensible?

How will we respond to requests from law-enforcement or intelligence agencies to weaken our encryption practices or decrypt specific devices? Do we have a policy in place regarding such requests, and have we made that policy public or otherwise available to those who have entrusted the security of their information and systems to us? Or are we addressing such challenges in an ad-hoc and arbitrary fashion?

What are the *ethical risks of long-term data storage*? How long we are justified in keeping sensitive data, and when/how often should it be purged for security purposes? Do we have an end-to-end security plan for the *full lifecycle* of the data we store, and do we regularly examine that plan to see if it needs to be improved or updated?

7. ETHICAL CHALLENGES IN IOT, SMART GRID, AND PRODUCT DESIGN:

Have we adequately considered and justified the increased security risks of any wireless-enabled devices or products we design or develop? Is, for example, the health-preserving function of a medical device enhanced *enough* by the addition of wireless capability to justify that added risk of tampering or intrusion? Do Bluetooth-enabled door locks *make sense* from a security perspective? Or are our product design strategies informed more by a desire to exploit 'Internet of Things' hype than by our customers/users' genuine interests?

Have we been sufficiently *imaginative* in conceiving how a network, product or feature might be abused, exploited, or misused? Or have we narrowly restricted our security design and practice to the idealistic scenario of the benign and rational user operating in a benign and rational social environment? Have we fully confronted the prospect of those who may exploit a smart grid, network, device or feature *simply to demonstrate their power to do harm*, as opposed to having a conventional criminal motive?

For networked utilities and wireless devices that could cause significant harm if exploited, have we employed added/upgraded security measures, including end-user training and instruction for safe and secure operation? For example, have we suggested allowing a device to communicate only with a local server rather than be connected directly to the Internet? Have we designed the device software to require strong password practices, or have we left this up to the user, exposing them to greater harm?

For 'Smart Grid' technologies and other systems involving critical public functions (such as health care, voting, or education) or utilities (such as power and water), has the public interest been adequately protected? Do the professionals involved in securing those systems fully understand the far higher ethical stakes involved in such enterprises?

8. Ethical Challenges with Accountability for Cybersecurity:

In a cybersecurity team, who is designated as responsible for each aspect of cybersecurity practice? How will we avoid a scenario where ethical cybersecurity practice is a high-level goal of the team or organization, but no specific individuals are tasked with specific actions to achieve that goal?

Who should and will be held accountable for various risks or harms that might be imposed on others by our cybersecurity practice? How will we avoid the 'problem of many hands,' where no one is held accountable for the harmful outcomes of a problematic cybersecurity practice to which many contributed?

What organizational/team policies and routines must we establish in advance and enforce, in order to safeguard and promote ethical cybersecurity practice? (For example, regularly scheduled security audits, incident reports, reviews of access policies, privilege levels, password management and supervision routines).

Do we have effective processes for subpar aspects or results of our cybersecurity practice to be surfaced and investigated? **Is there an established process for correction, repair, and iterative improvement of our cybersecurity efforts?** (For example: 'premortem' and 'postmortem' exercises as a form of 'cybersec disaster planning' and learning from mistakes). Or do our procedures, norms, incentives, and organizational/team culture make it likely that such weaknesses will be ignored or swept under the rug?

Have we placed cybersecurity efforts in appropriately skilled and responsible hands, with appropriate levels of instruction, training, and guidance? Or do we offload too much responsibility for sound security practice to employees, customers, or members of the public who are not adequately-informed, motivated or equipped to do what we expect them to do?

What harms can result from our inadequate instruction and training (of data users, clients, customers, etc.), or from our giving stakeholders too much control (over password strength, choice to patch and update firmware, choice of scan frequency, etc.)?

9. Ethical Challenges in Security Research and Testing:

When is it ethical to publish information about previously unknown security techniques, tools, or vulnerabilities for the benefit of security researchers, when there is a risk of these techniques or vulnerabilities being exploited by malicious actors?

What are the ethical implications of developing and releasing automated security tools, especially those intended to spread 'in the wild'? Can this ever be justified by the need to block the spread of a destructive worm or other malware, even if it may have unintended effects on systems that end up being 'infected' with and altered by the security tool, without the consent of the owner of that system?

How should we balance the different ethical interests and timescales of security research, considering both longer-term interests, which may often favor an aggressive publication strategy to keep the field at the cutting-edge of security practice, and the short-term interests, in which publication may create new risks of malicious action?

How should hiring in our security research team balance the need for top talent and a shared ethical commitment to responsible and professional security practice? How can we promote a culture of moral growth and maturity in security research and testing?

What are the ethical implications of participating in the private market for 'zero-day' exploits, either as an exploit seller, buyer, or developer? How are these ethical implications amplified by the fact that companies such as Hacking Team and VUPEN often sell the exploits they buy to repressive governments, who seek them for use against dissidents and political activists? What if any justifications can be given for participating in such a market?

10. Understanding Broader Impacts of Cybersecurity Practice

Overall, have we fully considered how our cybersecurity practices today may impact others, now *and* well down the road? Is our cybersecurity team sufficiently diverse to understand and anticipate these effects? Does our cybersecurity plan take into account how its impact might vary across a variety of individuals, identities, cultures and interest groups? Or might we be ignoring or minimizing the effects of our practice on people or groups unlike ourselves?

Has sufficient input on our security practice been gathered from stakeholders outside of the organization (for example, privacy advocates, privacy law experts, civil rights advocates, political groups and demographic minorities, who each might represent very different interests/values/experiences from those known in-house)?

Do our cybersecurity practices violate anyone's legal or *moral* rights, **limit their fundamental human *capabilities***, or otherwise **damage their fundamental *life interests*?** Do our cybersecurity practices in any way **impinge on the *autonomy* or *dignity*** of other moral agents? Are our cybersecurity practices likely to **damage or interfere with the *moral and intellectual habits, values,* or *character development*** of any affected parties?

Would information about our cybersecurity practices be morally or socially controversial, or damaging to the professional reputations of those involved, if widely known and understood? Are they consistent with the organization's image and professed values? Or are they a PR disaster waiting to happen, and if so, why are *these* our practices, and not better ones?

CASE STUDY 2

In the summer of 2017 it was revealed that Equifax, a massive credit reporting bureau managing the credit rating and personally identifying information of most credit-using Americans, had suffered a severe security breach affecting 143 million Americans.[5] Among the data stolen in the breach were social security and credit card numbers, birthdates, addresses, and information related to credit disputes. The scale and severity of the breach was nearly unprecedented, and to make things worse, Equifax's conduct before and after the announcement of the breach came under severe criticism.

For example, the website created by a PR consulting firm to handle consumer inquiries about the breach was itself riddled with security flaws, despite requesting customers submit personally identifying information to check to see if they were affected. The site also told consumers that by using the site to see if they were affected, they were waiving legal rights to sue Equifax for damages related to the breach. The site, which gave many users inconsistent and unclear information about their status in the breach, offered to sell consumers further credit protection services from Equifax, for a fee.[6]

Soon it was learned that the Equifax had known of the May 2017 breach for several months before disclosing it. Additionally, the vulnerability the attackers exploited had been discovered by Equifax's software supplier earlier that year; that company provided a patch to all of its customers in March 2017. Thus Equifax had been notified of the vulnerability, and given the opportunity to patch its systems, two months before the breach exposed 100 million Americans to identity theft and grievous financial harm.

Later, security researchers investigating the general quality of Equifax's cybersecurity efforts discovered that on at least one of Equifax's systems in Argentina, an unsecured network was allowing logons with the eminently guessable 'admin/admin' combination of username and password, and giving intruders ready access to sensitive data including 14,000 unencrypted employee usernames, passwords and national ID numbers.[7]

Following the massive breach, two high-ranking Equifax executives charged with information security immediately retired, and the Federal Trade Commission launched an investigation of Equifax for the breach. After learning that three other Equifax executives had sold almost two billion dollars of their company stock before the public announcement of the breach, the Department of Justice opened an investigation into the possibility of insider trading related to the executives' prior knowledge of the breach.[8]

[5] https://www.theatlantic.com/business/archive/2017/09/equifax-cybersecurity-breach/539178/

[6] https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/

[7] https://krebsonsecurity.com/2017/09/ayuda-help-equifax-has-my-data/

[8] https://www.engadget.com/2017/09/18/equifax-stock-sales-doj-investigation-insider-trading/

Below, you'll answer some questions about this case study. Your answers should highlight connections between the case and the content of Part Two.

Question 2.1: Of the ten types of ethical challenges for cybersecurity practitioners that we listed in Part Two, which of those types does the Equifax case study potentially involve? Explain your answer.

Question 2.2: What significant ethical harms are involved in the Equifax case, both in the short-term and the long-term? Who are some of the different stakeholders who may be harmed, and how?

Question 2.3: What do you imagine might be some of the *causes* of Equifax's failure to adopt more stringent cybersecurity protections and a more effective incident response? Consider not just the actions of individuals but also the larger organizational structure, culture, and incentives.

Question 2.4: If you were hired to advise *another* major credit bureau on their information security, in light of the Equifax disaster, what are three questions you might first ask about your client's cybersecurity practices, and their ethical values in relation to cybersecurity?

Question 2.5: In what ways could an organizational culture of thinking about the *ethics* of cybersecurity, as described so far in this module, potentially have *prevented* the Equifax breach, or reduced its harmful impact?

CASE STUDY 3

Security researchers often use conference platforms such as DefCon and RSA to announce newly discovered security tools or vulnerabilities; often these are controversial, and invite careful ethical reflection on the harms of benefits of such disclosures, and the competing interests involved. Here are two examples to compare and consider from an ethical standpoint:

A. At DefCon 2016, security researcher Anthony Rose presented the results of his testing of the security of products in the emerging market for Bluetooth-enabled door locks.[9] He found that of 16 brands of locks he purchased, 12 had profoundly deficient security, including open transmission of plain-text passwords, the ability to easily change admin passwords and physically lock out users, and vulnerability to replay attacks and spoofing. Some of the locks could be remotely opened by an attacker a half-mile away. Of the manufacturers Rose contacted, only one responded to his findings. Another shut down its website but continued to sell its product on Amazon.

B. At Defcon 2017, two members of Salesforce's "Red Team" of offensive security experts were scheduled to present (under their Twitter handles rather than their professional names) details of their newly developed security tool, Meatpistol. Meatpistol is an automated 'malware implant' tool designed to aid security red teams in creating malware they can use to use to

[9] https://www.engadget.com/2016/08/10/researcher-finds-huge-security-flaws-in-bluetooth-locks/

attack their own systems, so that they might better learn their own systems' vulnerabilities and design more effective countermeasures. It functioned more or less as any malware tool does, able not only to generate code to infect systems but to steal data from them, except that it reduced the time needed to create new forms of such code from days to mere seconds. The two members of Salesforce's offensive security team planned to make Meatpistol's code public after the event, with the view that making Meatpistol an open source tool would allow the community of security researchers to improve upon it further. As with any malware implant tool, however, making it open source would have inevitably invited other hackers to use it for malicious purposes. Just prior to the event, an executive at Salesforce instructed the team not to release Meatpistol's code, and shortly thereafter, instructed them to cancel the previously-approved presentation altogether. The team presented on Meatpistol at DefCon anyway, after which they were summarily fired by Salesforce. Meatpistol's code was not released.

Below, you'll answer some questions about these cases. Your answers should make connections between the cases and the content of Part Two.

Question 2.6: Of the ten types of ethical challenges for cybersecurity practitioners that we listed in Part Two, which three types do you think are *most* relevant to these studies? Briefly explain your answer.

Question 2.7: Who are the different stakeholders whose interests Anthony Rose needed to consider in giving his DefCon presentation, and what potential harms/benefits to those various stakeholders did he need to consider and weigh?

Question 2.8: Who are the different stakeholders whose interests the Salesforce red team needed to consider in giving their presentation, and what potential harms/benefits to those various stakeholders did he need to consider and weigh?

Question 2.9: Do you think the 2016 Rose presentation was ethical, all things considered? Why or why not? What about the 2017 Meatpistol presentation (including its planned code release) – was it ethical? Was Salesforce right to try to stop it, and to block the code release?

Question 2.10: What are the most important ethical similarities *and* differences between the two examples in Case Study 3?

Question 2.11: How do you think the two presentations shaped the professional reputations of Rose and the Salesforce Red Team, respectively? For example, if you were looking to hire a security researcher for your red team, might you be *more* or *less* likely to hire Rose after his presentation? What about the two members of the Salesforce team? What ethical considerations would need to be weighed in your decision?

Question 2.12: How might members of the general *public* look at each of these presentations, and judge the moral character of the researchers themselves, in a different light than would other members of their security research community?

PART THREE

What are cybersecurity professionals' obligations to the public?

To what extent are cybersecurity professionals—information security officers, cryptographers, digital forensic scientists, penetration testers, security engineers, analysts, consultants, auditors, developers, and administrators—obligated by **ethical duties to the public**? **Where do those obligations come from**? And **who is 'the public'** that deserves a cybersecurity professional's ethical concern?

1. WHY DO CYBERSECURITY PROFESSIONALS HAVE OBLIGATIONS TO THE PUBLIC?

One *simple* answer is, 'because cybersecurity professionals are human beings, and all human beings have ethical obligations to one another.' The vast majority of people, upon noticing a small toddler crawling toward the opening to a deep mineshaft, will feel obligated to redirect the toddler's path or otherwise stop to intervene, even if the toddler is unknown and no one else is around. If you are like most people, you just accept that you have some basic ethical obligations toward other human beings.

But of course, our **ethical obligations to an overarching 'public' always co-exist with ethical obligations to one's family, friends, employer, local community, and even oneself**. In this part of the module we highlight the public obligations because **too often, important obligations to the public are ignored in favor of more familiar ethical obligations** we have to specific known others in our social circle—even in cases when the ethical obligation we have to the public is objectively much ***stronger*** than the more local one.

If you're tempted to say 'well of course, I *always* owe my family/friends/employer/myself more than I owe to a bunch of strangers,' consider that this is ***not*** **how we judge things when we stand as an objective observer.** If the owner of a school construction company knowingly buys subpar/defective building materials to save on costs and boost his kids' college fund, resulting in a school cafeteria collapse that kills fifty children and teachers, we don't cut him any slack because he did it to benefit *his* family. We don't excuse his employees either, if they were knowingly involved and could anticipate the risk to others, *even* if they were told they'd be fired if they didn't cooperate. We'd tell them that keeping a job isn't worth sacrificing fifty strangers' lives. If we're thinking straight, we'd tell them that keeping a job doesn't give them permission to sacrifice even *one* strangers' life.

As we noted in Part One, **some cybersecurity contexts *do* involve life and death risks** to the public. If my recklessly negligent cost-cutting on security penetration testing results in an attack on an autonomous vehicle's navigation system that causes one, or fifty, or a hundred strangers' deaths, it's really no different, morally speaking, than the reckless negligence of the school construction. Notice, however, that it may take us longer at first to make the connection, since the cause-and-effect relationship in the cybersecurity case can be harder to identify at first.

Other **risks of harm to the public that we must guard against** include those we described in Part One, from reputational harm, economic damage, and psychological injury, to reinforcement of unfair or unjust social arrangements.

However, it remains true that **the nature and details of our obligations to the public as cybersecurity professionals can be unclear.** How *far* do such obligations go, and *when do they take precedence* over other obligations? To what extent and in what cases do I *share* those obligations with others on my team or in my company? **These are not easy questions**, and often, the answers depend considerably on the details of the specific situation confronting us. But there are some ways of thinking about our obligations to the public that can help dispel some of the fog; Part Three outlines several of these.

2. CYBERSECURITY PROFESSIONALS AND THE PUBLIC GOOD

Remember that if the good life requires making a positive contribution to the world in which others live, then it would be perverse if we accomplished none of that in our professional lives, where we spend many or most of our waking hours, and to which we devote a large proportion of our intellectual and creative energies. Excellent doctors contribute health and vitality to the public. Excellent professors contribute knowledge, skill and creative insights to the public domain of education. Excellent lawyers contribute balance, fairness and intellectual vigor to the public system of justice. **Cybersecurity professionals of various sorts contribute goods to the public sphere as well.**

What is a cybersecurity *professional*? You may not have considered that the word 'professional' is etymologically connected with the English verb 'to profess.' What is it to profess something? It is to stand publicly for something, to express a belief, conviction, value or promise to a general audience that you expect that audience to hold you accountable for, and to identify you with. When I *profess* something, I say to others that this is something about which I am serious and sincere; and which I want them to know about me. So when we identify someone as a professional *X* (**whether 'X' is a lawyer, physician, soldier, data scientist, or cybersecurity analyst**), we are saying that being an 'X' is not just a job, but a vocation—a form of work to which the individual is committed and with which they would like to be identified. If I describe myself as just having a 'job,' I don't identify myself with it. But if I talk about '*my work*' or '*my profession*,' I am saying something more. This is part of why most professionals are expected to undertake **continuing education and training in their field**; not only because they need to benefit from the most current expertise available, but also because this is an important sign of their continuing investment in and commitment to the field. Even if I leave a profession or retire, I am likely to continue to identify with it—an ex-lawyer will refer to herself as a 'former lawyer,' an ex-soldier calls himself a 'veteran.'

So how does being a professional create special ethical obligations for the cybersecurity practitioner? Consider that members of most professions enjoy an elevated status in their communities; doctors, professors, scientists and lawyers generally get more respect from the public (rightly or wrongly) than retail clerks, toll booth operators, and car salespeople. But why? It can't just be the difference in skill; after all, car salespeople have to have very specialized skills in order to thrive in their job. The distinction lies in the perception that **professionals secure a vital public good**, not something of merely private and conditional value. For example, without doctors, public health would certainly suffer – and a good life is virtually impossible without some measure of health. Without good lawyers and judges, the public would have no formal access to justice – and without recourse for injustice done to you or others, a good life is much harder to come by. So each of these professions is supported and respected by the public precisely because they deliver something vital to the good life, and something needed not just by a few, but by us all.

Of course, basic cybersecurity practices (such as safely backing up data, keeping passwords strong and secure, being wary of phishing emails and insecure websites, and keeping security/antivirus software up-to-date) can be employed by any professional, in any field. But many cybersecurity practices are turning into new professions *of their own*, and these will continue to gain more and more public recognition and respect. **What do cybersecurity professionals do to earn that respect?** How must they act in order to continue to earn it? After all, special public respect and support are not given for free or given unconditionally—they are given in recognition of some service or value. That support and respect is also something that translates into real power: the power of consumer loyalty and public trust, the power to influence how safe people, organizations, and infrastructure are from cyberthreats, and the power to defend the viability and growth of information societies. And as we are told in the popular Spiderman saga, "With great power comes great responsibility." This is a further reason, even above their general ethical obligations as human beings, that cybersecurity professionals have special ethical obligations to the public they serve.

Question 3.1: Why is *security* an ethically significant public good?

Question 3.2: Besides security, what *other* ethically significant goods can cybersecurity professionals help to preserve or contribute to the public sphere?

Question 3.3: What kinds of character traits, qualities, behaviors and/or habits do you think mark the kinds of cybersecurity professionals who will contribute *most* to the public good? (Answer as fully/in as many ways as you are able):

3. JUST WHO *IS* THE 'PUBLIC'?

Of course, one can respond simply with, 'the public is everyone.' But the public is not an undifferentiated mass; the public is composed of our families, our friends and co-workers, our employers, our neighbors, our church or other local community members, our countrymen and women, and people living in every other part of the world. To say that we have ethical obligations to 'everyone' is to tell us very little about how to actually work responsibly as in the public interest, since **each of these groups and individuals that make up the public are in a unique relationship to us and our work, and are potentially impacted by it in very different ways**. And as we have noted, we also have special obligations to some members of the public (our children, our employer, our friends, our fellow citizens) that exist alongside the broader, more general obligations we have to all.

One concept that ethicists use to clarify our public obligations is that of a ***stakeholder***. A stakeholder is anyone who is potentially impacted by my actions. Clearly, certain persons have ***more*** at stake than other stakeholders in any given action I might take. When I consider, for example, how much effort to put into penetration testing the software for an infusion pump that will be used to measure and deliver precise doses of anesthesia, it is obvious that the surgical patients to whom this anesthesia will be delivered are the primary stakeholders in my action; their very lives are potentially at risk in my choice. And this stake is so ethically significant that it is hard to see how any other stakeholder's interest could weigh as heavily.

4. DISTINGUISHING AND RANKING COMPETING STAKEHOLDER INTERESTS

Still, in most cybersecurity contexts there are a **variety of stakeholders** potentially impacted by my action, whose **interests are not always aligned**. For example, my employer's interests in cost-cutting and an on-time product delivery schedule may be in tension with the interest of other stakeholders in having the most secure app or operating system on the market. Yet even such **stakeholder conflicts** are rarely as stark as they might first appear. In our example, the consumer also has an interest in an *affordable* and *timely* product, and my employer also has an interest in earning a reputation for product excellence and safety in its sector, and maintaining the profile of a responsible corporate citizen. Thinking about the public in terms of *stakeholders*, and **distinguishing them by the different 'stakes' they hold in what we do as cybersecurity practitioners**, can help to sort out the tangled web of our varied ethical obligations to one amorphous 'public.'

Of course, **I *too* am a stakeholder**, since my actions impact my own life and well-being. Still, my *trivial* or *non-vital* interests (say, in shirking a necessary but tedious security audit, or concealing rather than reporting and patching an embarrassing security hole in my app) *will never override a critical moral interest* of another stakeholder (say, their interest in not being unjustly arrested, injured, or economically damaged due to my professional laziness).
Ignoring the health, safety, or other vital interests of those who *rely* upon my cybersecurity practice is simply not justified by my own stakeholder standing. Typically, doing so would imperil my reputation and long-term interests anyway.

Ethical decision-making thus requires cultivating the habit of reflecting carefully upon the range of stakeholders who together make up the 'public' to whom I am obligated, and **weighing what is at stake for each of us** in my choice, or the choice facing my team or group. **On the**

next two pages is a case study you can use to help you think about what this reflection process can entail.

CASE STUDY 4

In 2015, just in time for the holiday season, Mattel released its WiFi-enabled Hello Barbie doll, which allowed the doll's microphone to record conversations with a child and send it via Wi-Fi to third parties for audio language processing, allowing the doll to then offer the child an appropriate natural language response. Because the conversations were stored in the cloud, parents were also able to monitor the child's conversations with the doll; parents can even share the audio clips of their children's conversations online on the website of ToyTalk, the maker of the third-party software.

The toy raised a broad range of ethical issues, including the appropriateness of allowing parents to spy on their children during imaginative play. Also, as one legal scholar noted, "In Mattel's demo, Barbie asks many questions that would elicit a great deal of information about a child, her interests, and her family. This information could be of great value to advertisers and be used to market unfairly to children."[10] However, security flaws were also prominent ethical concerns.

Security researchers quickly recognized significant security weaknesses in the doll that could be exploited by hackers for malicious purposes. One independent security researcher claimed that he was able to hack the device in such a way that he could access the user account information, stored audio files, and microphone for the doll, and potentially spoof ToyTalk's third party website server to assume control of the doll's speech. Somerset Recon, an organization devoted to security analysis and reverse engineering, eventually found 14 vulnerabilities in the system, including allowance for weak passwords, no protections against brute force password attacks (allowed unlimited password guesses), and exposure to URL redirect and phishing efforts. There was also the potential for malicious Javascript to be stored on ToyTalk's third party website, allowing "persistent backdoor access to a ToyTalk user account."[11] Somerset Recon acknowledged that some efforts to provide adequate security had been made by ToyTalk, but also noted that there appeared to have been "little to no pre-production security analysis" and that the company appeared to be "using their bug bounty program as a low-cost alternative" to an independent security audit that could have identified the vulnerabilities before the product was released, and before real-world users were exposed to a post-market "race between security researchers and malicious hackers" to find the system's flaws.[12]

[10] https://www.theguardian.com/technology/2015/mar/13/smart-barbie-that-can-listen-to-your-kids-privacy-fears-mattel

[11] http://www.somersetrecon.com/blog/2016/1/21/hello-barbie-security-part-2-analysis

[12] ibid.

Question 3.4: What specific, significant harms to members of the public did the initial release of the Hello Barbie toy risk? List as many potential types of harm from Hello Barbie's release as you can think of.

Question 3.5: How should those potential harms have been evaluated alongside the prospective *benefits* of the toy? Could a toy like this have benefits that would be significant enough to justify the risks of harm you identified above in 3.4? (Explain your answer)

Question 3.6: List the various *stakeholders* involved in the Hello Barbie case, and for each type of stakeholder you listed, identify what was *at stake* for them. Be sure your list is as complete as you can make it, including all possible affected stakeholders.

Question 3.7: What factors in this case suggest that Mattel/ToyTalk had an especially *strong* ethical duty to offer cybersecurity protections for users of their product? Did they fulfill that duty? Explain your answer.

Question 3.8: What public good was done by the actions of dedicated security professionals in this case?

Question 3.9: In what ways could Mattel/ToyTalk have made much *better* use of security professionals in this case? What factors might have influenced them *not* to use the best professional security practices and resources available?

Question 3.10: How do the ethical issues raised by this case study relate to questions of *public trust* in technology and the tech industry?

PART FOUR

What general ethical frameworks might guide cybersecurity practice?

We noted above that cybersecurity practitioners, in addition to their special professional obligations to the public, also have the same ethical obligations to their fellow human beings that we all share. What might those obligations be, and how should they be evaluated alongside our professional obligations? There are a number of familiar concepts that we already use to talk about how, in general, we ought to treat others. Among them are the concepts of rights, justice and the common good. But how do we define the concrete meaning of these important ideals? Here are three common frameworks for understanding our general ethical duties to others:

1. VIRTUE ETHICS

Virtue approaches to ethics are found in the ancient Greek and Roman traditions, in Confucian, Buddhist and Christian moral philosophies, and in modern secular thinkers like Hume and Nietzsche. Virtue ethics focuses not on rules for good or bad actions, but on the qualities of morally excellent persons (e.g., virtues). Such theories are said to be character based, insofar as they tell us what a person of virtuous character is like, and how that moral character develops. Such theories also focus on the habits of action of virtuous persons, such as the habit of moderation (finding the 'golden mean' between extremes), as well as the virtue of prudence or practical wisdom (the ability to see what is morally required even in new or unusual situations to which conventional moral rules do not apply).

How can virtue ethics help us to understand what our moral obligations are? It can do so in three ways. The first is by helping to see that we have a basic moral obligation to make a consistent and conscious effort to develop our moral character for the better; as the philosopher Confucius said, the real ethical failing is not having faults, 'but rather failing to amend them.' The second thing virtue theories can tell us is where to look for standards of conduct to follow; virtue theories tell us to look for them in our own societies, in those special persons who are exemplary human beings with qualities of character (virtues) to which we should aspire. The third thing that virtue ethics does is direct us toward the lifelong cultivation of practical wisdom or good moral judgment: the ability to discern which of our obligations are most important in a given situation and which actions are most likely to succeed in helping us to meet those obligations. Virtuous persons with this ability flourish in their own lives by acting justly with others, and contribute to the common good by providing a moral example for others to admire and follow.

Question 4.1: How would a conscious habit of thinking about how to be a better human being contribute to a person's character, especially over time?

Question 4:2: Do you know what specific aspects of your character you would need to work on/improve in order to become a better person? (Yes or No)

Question 4:3: Do you think most people make enough of a regular effort to work on their character or amend their shortcomings? Do you think we are morally obligated to make the effort to become better people? Why or why not?

Question 4:4: Who do you consider a model of moral excellence that you see as an example of how to live, and whose qualities of character you would like to cultivate? Who would you want your children (or future children) to see as examples of such human (and especially moral) excellence?

Question 4:5: What are three strengths of moral character (*virtues)* that you think are particularly important for *cybersecurity practitioners* to practice and cultivate in order to be excellent models for others in the profession? Explain your answers.

2. Consequentialist/Utilitarian Ethics

Consequentialist theories of ethics derive principles to guide moral action from the likely consequences of those actions. The most famous form of consequentialism is utilitarian ethics, which uses the principle of the 'greatest good' to determine what our moral obligations are in any given situation. The 'good' in utilitarian ethics is measured in terms of happiness or pleasure (where this means not just physical pleasure but also emotional and intellectual pleasures). The absence of pain (whether physical, emotional, etc.) is also considered good, unless the pain somehow leads to a net benefit in pleasure, or prevents greater pains (so the pain of exercise would be good because it also promotes great pleasure as well as health, which in turn prevents more suffering). When I ask what action would promote the 'greater good,' then, I am asking which action would produce, in the long run, the greatest net sum of good (pleasure and absence of pain), taking into account the consequences for all those affected by my action (not just myself). This is known as the hedonic calculus, where I try to maximize the overall happiness produced in the world by my action.

Utilitarian thinkers believe that at any given time, whichever action among those available to me is most likely to boost the overall sum of happiness in the world is the right action to take, and my moral obligation. This is yet another way of thinking about the 'common good.' But utilitarians are sometimes charged with ignoring the requirements of individual rights and justice; after all, wouldn't a good utilitarian willingly commit a great injustice against one innocent person as long as it brought a greater overall benefit to others? Many utilitarians, however, believe that a society in which individual rights and justice are given the highest importance is actually the kind of society most likely to maximize overall happiness in the long run. After all, how many societies that deny individual rights, and freely sacrifice individuals/minorities for the good of the many, would we call happy?

Question 4:6: What would be the hardest part of living by the utilitarian principle of the 'greatest good'? What would be the most rewarding part?

Question 4:7: What different kinds of pleasure/happiness are there? Are some pleasures more or less valuable or of higher or lower quality than others? Why or why not? Explain your intuitions about this:

Question 4:8: Utilitarians think that pleasure and the absence of pain are the highest goods that we can seek in life, and that we should always be seeking to produce these goods for others (and for ourselves). They claim that every other good thing in life is valued simply because it produces pleasure or reduces pain. Do you agree? Why or why not?

Question 4:9: A utilitarian might say that to measure a 'good life,' you should ask: 'how much overall happiness did this life bring into the world?' Do you agree that this is the correct measure of a good life, or not? Briefly explain.

Question 4:10: In what ways do you think cybersecurity practitioners can promote the 'greater good' through their work, that is, *increase* human happiness? In what ways could poor cybersecurity practice greatly *undermine* others' happiness?

3. Deontological Ethics

Deontological ethics are rule or principle-based systems of ethics, in which one or more rules/principles are claimed to tell us what our moral obligations are in life. In Judeo-Christian thought, the Ten Commandments can be thought of as a deontological system. Among modern, secular forms of ethics, many deontological systems focus on lists of 'rights' (for example, the rights not to be unjustly killed, enslaved, or deprived of your property). Consider also the modern idea of 'universal human rights' that all countries must agree to respect. In the West, moral rights are often taken as a basis for law, and are often invoked to justify the making of new laws, or the revision or abolition of existing ones. In many cultures of East Asia, deontological systems may focus not on rights but on duties; these are fixed obligations to others (parents, siblings, rulers, fellow citizens etc.) that must be fulfilled according to established rules of conduct that govern various types of human relationships.

Another well-known deontological system is that of the 18th century philosopher Immanuel Kant, who identified a single moral rule called the categorical imperative. This principle tells us to only act in ways that we would be willing to have all other persons follow, all of the time. He related this to another principle that tells us never to treat a human being as a 'mere means to an end,' that is, as an object to be manipulated for our own purposes. For example, I might want to tell a lie to get myself out of trouble in a particular case. But I certainly would not want everyone in the world to lie every time they felt like it would help them avoid trouble. And if someone lies to me to get me to do something that benefits them, I am rightly upset about being treated as a mere object to be manipulated for gain. So, I cannot logically give myself permission to lie, since there is nothing about me that exempts me from my own general moral standards for human behavior. For if I am willing to give myself permission to act in this way for this reason, how could I logically justify withholding the same permission from others?

According to this principle, human lives are the ultimate sources of all moral value. I thus have a universal moral obligation to treat other human lives in ways that acknowledge and respect their unconditional value, and to not treat them merely as tools to manipulate for lesser purposes. And since I myself am human, I cannot morally allow even my own existence to be used as a mere tool for some lesser purpose (for example, to knowingly sell out my personal integrity for money, fame or approval). This principle highlights my duty to always respect the dignity of all human lives. This theory is also linked with a particular idea of justice, as treatment that recognizes the basic equality and irreplaceable dignity of every human being, no matter who they are or where they live. Such thinking is often considered to be at the heart of the modern doctrine of inalienable human rights.

Question 4:11: How often, when making decisions, do you think about whether you would willingly allow or support others acting in the same way that you are choosing to act? Does it seem like something you *should* think about?

Question 4:12: What are two cases you can think of in the cybersecurity context in which a person or persons were treated as a ‘mere means to an end’, that is, treated as nothing more than a useful tool to achieve another person or group’s goal? (Feel free to draw from any of the working examples in previous parts of the module).

Question 4:13: Do you agree that human lives are of the highest possible value and beyond any fixed 'price'? In your opinion, how well does our society today reflect this view on morality and justice? Should it reflect this view?

Question 4:14: While each of the 3 distinct types of ethical frameworks/theories reviewed in this section is subject to certain limitations or criticisms, what aspects of the good life/ethics do you think each one captures best?

PART FIVE

What are ethical 'best practices' in cybersecurity?

The phrase 'best practices' refers to known techniques for doing something that tend to work well, better than the alternative ways of doing something. It's not a phrase unique to ethics; in fact it's used in a range of corporate, technical, and government settings; but it's often used in contexts where it is very important that the thing be done *well*, and where there are significant costs or risks to doing it in a less than optimal way.

For cybersecurity practitioners, we describe two types of best practices. The first set focuses on **best practices for functioning ethically *in cybersecurity practice***; they are adapted specifically to the ethical challenges that we studied in Part Two of this module. **These are not best *technical* practices** in cybersecurity (such as using strong passwords and encryption, or employing adversarial security testing), though maintaining best technical practices is often a necessary part of being an ethical cybersecurity practitioner. Rather, what is offered here are best practices for ensuring appropriate ethical attention, reflection, and decision-making in cybersecurity contexts.

The second set identifies **best practices for living and acting ethically *in general***; these practices can be adopted by anyone, regardless of their career or professional interests. Cybersecurity practitioners can benefit from drawing upon both sets of practices in creative ways to manage ethical challenges wisely and well.

1. BEST PRACTICES FOR CYBERSECURITY ETHICS

No single, detailed code of cybersecurity ethics can be fitted to all contexts and practitioners; organizations and professions should therefore be encouraged to develop explicit internal policies, procedures, guidelines and best practices for cybersecurity ethics that are specifically adapted to their own activities and challenges. However, those specific codes of practice can be well shaped by reflecting on these 14 general norms and guidelines for ethical cybersecurity practice:

I. Keep Cybersecurity Ethics in the Spotlight—and Out of the Compliance Box: As earlier examples have shown, ethics is a *pervasive* aspect of cybersecurity practice. Because of the immense social power of information technology, ethical issues are virtually *always* in play when we strive to keep that technology and its functioning secure. Even when our work is highly technical and not directly client-facing, ethical issues are never *absent* from the context of our work. However, the 'compliance mindset' found in many organizations, especially concerning *legal* matters, can, when applied to cybersecurity, encourage a dangerous tendency to 'sideline' ethics as an external constraint rather than see it as an integral part of being good at what we do. *Law and ethics are not the same, and don't substitute for one another*. What is legal can be unethical (quite common), and what is ethical can (even if less commonly) be illegal. If we fall victim to the legalistic 'compliance' mindset when we are thinking about ethics, we are more likely to view our ethical obligations as a box to 'check off' and then forget about, once we feel we have done the 'minimum' needed to 'comply' with them. Unfortunately, this often leads to disastrous consequences, for individuals and organizations alike. Because cybersecurity is a practice for which ethical considerations are *ubiquitous* and *intrinsic*, not intermittent and external, our individual and organizational efforts must strive to keep the ethics of our security work in the spotlight.

II. Consider the Human Lives and Interests Behind the Systems: Especially in technical contexts, it's easy to lose sight of what most of the systems we work with *are*: namely, ways of improving human lives and protecting human interests. Much of what falls under the 'cybersecurity' umbrella concerns the most *sensitive* aspects of human lives: their reputations, opportunities, property, and freedoms; their physical and psychological well-being; and their social connections, likes and dislikes. A decent human would never handle another person's body, money, or mental condition without due care; but it can be easy to forget that this is often what we are doing when we are charged with securing cybersystems.

III. Consider Downstream (and Upstream and Lateral) Risks in Cybersecurity Practice: As noted above, often we focus too narrowly on whether *we* have complied with ethical guidelines and we forget that ethical issues concerning cybersecurity don't just 'go away' once we have performed our *own* particular task diligently. Thus it is essential to think about what happens to the sensitive device, software, hardware system, or data even after it leaves our hands. Even if, for example, I have done extensive security testing and auditing of a product before its release, there are always new threats, new vulnerabilities that can emerge, and new applications of the product that might create new security challenges. I should always therefore have a view of the security risks downstream from my practice, and maintain effective lines of communication with those persons in a position to keep the system or product secure at those stages. Communication with those 'upstream' and lateral to my security practice is also essential; if the reason that I struggle with keeping a system secure is that poor design and configuration choices upstream are tying my hands, or because someone in another department is continually ignoring or overriding the security practices I've instituted, then I need to be prepared to address that. If I am not paying attention to the downstream, upstream, and lateral risks, then I have not fully appreciated the ethical stakes of my *own* current security practice.

IV. Don't Discount Non-Technical Actors, Interests, Expectations, and Exposures: Most cybersecurity professionals are highly skilled in specific areas of technical practice and accustomed to interacting with others with similar levels of technical expertise. Even their adversaries are often hackers with comparable technical skillsets and interests. This can lead to a dangerously insular mindset when it comes to considering the interests and risks to which non-technical actors are exposed (and which cybersecurity professionals are often duty-bound to protect.) For example, cybersecurity professionals know that no system is 100% secure from intrusion or attack, and that, for example, installing antivirus software is just one (modest and limited) tool for reducing security risk, not a magic security genie that makes any additional security practices unnecessary. But an ordinary, untutored user may well operate with inflated expectations and unrealistic beliefs about cybersecurity. Likewise, a cybersecurity professional is unlikely to fall for an unsophisticated phishing attempt, or to use an easy-to-guess password, or to insert a USB flash storage device received from a random stranger into their networked laptop. But many others will, and it can be tempting to adopt an ethically callous attitude toward people whose exposure to security risks results from technical incompetence or naïvete. This attitude is important to resist, for two reasons. First, because it leads to missed opportunities to implement basic risk prevention and mitigation strategies, increasing the overall risk to the network/organization and third parties. Second, because being technically naïve is not, in fact, something that makes a person any more deserving of harm or injury, or any less deserving of security. Maintaining appropriate empathy for non-technical actors and their interests will ultimately make you a better cybersecurity professional, not just in terms of your moral character, but also in terms of being more effective in cybersecurity work.

V. Establish Chains of Ethical Responsibility and Accountability: In organizational settings, the 'problem of many hands' is a constant challenge to responsible practice and accountability. To avoid a diffusion of responsibility in which no one on a team may feel empowered or obligated to take the steps necessary to ensure effective and ethical cybersecurity practice, it is important that clear *chains of responsibility* are established and made explicit to everyone involved in the work, at the earliest possible stages of a project. It should be clear who is responsible for each aspect of security risk management and prevention of harm. It should also be clear who is ultimately *accountable* for ensuring an ethically executed security project or practice. Who will be expected to provide answers, explanations, and remedies if there is a failure of ethics or significant breach allowed by the team's work? The essential function of chains of responsibility and accountability is to assure that individuals *take explicit ownership of cybersecurity work and its ethical significance.*

VI. Practice Cybersecurity Disaster Planning and Crisis Response: Most people don't want to anticipate failure, disaster, or crisis; they want to focus on the *positive* potential of a project or system. While this is understandable, the dangers of this attitude are well known, and have often *caused* failure, disaster, or crisis that could easily have been avoided. This attitude also often prevents effective crisis response since there is no planning for a worst-case-scenario. This is why engineering fields whose designs can impact public safety have long had a culture of *encouraging* thinking about failure. Understanding how a product or system will function in non-ideal conditions, at the boundaries of intended use, or even outside those boundaries, is essential to building in appropriate margins of safety and developing a plan for unwelcome scenarios. Thinking about failure makes engineers' work *better*, not worse. Cybersecurity practitioners must promote the same cultural habit in their work. Known vulnerabilities and past incidents/breaches should be carefully analyzed and discussed ('post-mortems') and results projected into the future. 'Pre-mortems' (imagining together how a currently secure system could be breached, so that we can envision to prevent that outcome) can be a great cybersecurity practice. It's also essential to develop crisis plans that go beyond deflecting blame or denying harm (often the first mistake of a PR team after a breach or security flaw is exposed). Crisis plans should be intelligent, responsive to public input, and most of all, able to effectively mitigate or remedy harm being done. This is much easier to plan *before* a crisis has actually happened.

VII. Promote Values of Transparency, Autonomy, and Trustworthiness: The most important thing to preserve a healthy relationship between cybersecurity practitioners and the public is to understand the importance of transparency, autonomy, and trustworthiness in that relationship. Hiding a severe security risk to others behind legal, technical or PR jargon, disempowering users' efforts to promote their own security, and betraying public trust are almost never good strategies in the long run. Clear and understandable security attestations, policies, and recommendations, when accurate and reliable, help to promote the values of transparency, autonomy, and trustworthiness. Notifications of security flaws, patches, and breaches should be shaped by these same values, to the maximum extent compatible with the value of security itself. Thus delaying or burying a vulnerability or breach notification in order to spare oneself, or one's team, from professional or public scorn is not typically an ethical choice. It undermines transparency, and by doing so prevents affected stakeholders from making their own informed, self-guided choices to manage their risk. It also violates the public trust that their security *is* deeply valued. However, if a premature notification would expose others to unreasonable risk, a delay may often be justified by careful reasoning from the facts, assuming that reasoning is itself reliable, and not an example of 'motivated reasoning' (believing something only because it benefits me to do so, or because I strongly wish it were true).

VIII. Consider Disparate Interests, Resources, and Impacts: It is important to understand the profound risk in cybersecurity practices of producing or magnifying disparate impacts; that is, of *making some people better off and others worse off*, whether this is in terms of their social share of economic well-being, political power, health, justice, or other important goods. *Not all disparate impacts are unjustifiable or wrong*. For example, while a device that uses strong end-to-end encryption may make it easier for criminals to avoid government scrutiny of their communications, it may also have a disparate impact on authoritarian governments' ability to track and neutralize their political opposition. Here, the ethical balance of the disparate impacts is quite complex (as seen in 2016's case of Apple v. the FBI.) But imagine *another* device that offers cutting-edge security tools and features only to those buying the most expensive model, and outdated/weak security features in all other models. Can the disparate impact of this choice be justified, insofar as it may expose millions who are not at the top of the socioeconomic ladder to real deprivations of property, privacy, and reputation, while only protecting the *already* secure and privileged? Or consider a visual recognition security challenge that is inaccessible to the blind. What about a facial recognition security lock that doesn't properly function with darker skin tones? This is why there must be a *presumption in cybersecurity practice of ethical risk from disparate impacts; they should be anticipated, actively audited for, and carefully examined for their ethical acceptability*. Likewise, we must investigate the extent to which different populations affected by our practice have different interests, training, and resources that give them a differential ability to benefit from our product or project.

IX. Invite Diverse Stakeholder Input: One way to avoid 'groupthink' in ethical risk assessment and design is to invite input from diverse stakeholders outside of the team and organization. It is important that stakeholder input not simply reflect the same perspectives one already has within the organization or group. Many cybersecurity practitioners have unusually high levels of educational achievement and economic status, and in many technical fields, there may be skewed representation of the population in terms of gender, ethnicity, age, and other characteristics. Also, the nature of the work may attract people who have common interests and values--for example, a shared optimism about the potential of science and technology, and comparatively less faith in other social mechanisms. All of these factors can lead to organizational *monocultures*, which magnify the dangers of groupthink, blind spots, insularity of interests, and poor design. For example, many of the best practices above can't be carried out successfully if members of a team struggle to imagine how a cybersecurity practice would be perceived by, or how it might affect, people unlike themselves. Actively recognizing the limitations of a team perspective is essential. Fostering more diverse cybersecurity organizations and teams is one obvious way to mitigate those limitations, but soliciting external input from a more truly representative body of those likely to be impacted by our practice is another.

X. Design for Privacy and Security: This might seem like an obvious one, but nevertheless its importance can't be overemphasized. 'Design' here means not only technical design (of networks, databases, devices, platforms, websites, tools, or apps), but also social and organizational design (of groups, policies, procedures, incentives, resource allocations, and techniques) that promote privacy and security objectives. How this is best done in each context will vary, but the essential thing is that along with other project goals, the values of privacy and security remain at the forefront of project design, planning, execution, and oversight, and are never treated as marginal, external, or 'after-the-fact' concerns.

XI. Make Ethical Reflection & Practice Standard, Pervasive, Iterative, and Rewarding: Ethical reflection and practice, as we have already said, is an essential and central part of professional excellence in cybersecurity. Yet it is still in the process of being fully integrated into the profession. The work of making ethical reflection and practice *standard* and *pervasive*, that is, accepted as a necessary, constant, and central component of every cybersecurity context, must continue to be carried out through active measures taken by individual practitioners and organizations alike. Ethical reflection and practice in cybersecurity must also, to be effective, be instituted in *iterative* ways. That is, because the nature and extent of threats to cybersecurity are continually evolving, we must treat cybersecurity ethics as an active and unending learning cycle in which we continually observe the ethical outcomes of our security practice, learn from our mistakes, gather more information, acquire further ethical and technical expertise, and then update and improve our security practice accordingly. Most of all, ethical practice in cybersecurity environments must be made *rewarding*: team, project, and institutional/company incentives must be well aligned with the ethical best practices described above, so that those practices are reinforced and so that cybersecurity practitioners are empowered and given the necessary resources to carry them out.

XII. Model and Advocate for Ethical Cybersecurity Practice: As we saw in Section 4's discussion of virtue ethics, one way to be guided well in practical ethical contexts is to find and pay attention to excellent models of that practice. Eventually, becoming excellent *oneself* not only allows you to guide others, it also allows you to collaborate with *other* excellent persons and professionals, to improve the standards by which we all live. Aspiring cybersecurity professionals can benefit from seeking, identifying, and developing strong mentoring relationships with excellent models of cybersecurity practice—models who not only possess *technical* excellence, but who are also exemplars of *ethically superior* cybersecurity leadership. A diverse range of models to learn from is best, as even experts have their weaknesses and blind spots. But those who develop practical wisdom in cybersecurity practice by learning from the best mentors can in turn become excellent mentors to others, raising the overall excellence and nobility of the field. Jointly, they can also work to advocate for more technically and ethically superior cybersecurity norms, standards, and practices in the field, raising the bar for everyone, and ensuring that cybersecurity professionals secure the promise of the information society for us all.

Question 5:1: Of these twelve best practices for cybersecurity ethics, which two do you think are the most challenging to carry out? What do you think could be done (by an individual, a team, or an organization) to make those practices easier?

Question 5:2: What benefits do you think might come from successfully instituting these practices in cybersecurity environments—for society overall, *and* for cybersecurity professionals?

2. General Best Practices for Living Well

There are a number of unfortunate habits and practices that create *obstacles* to living well in the moral sense; fortunately, there are also a number of common habits and practices that are highly *conducive* to living well. Here are five ethically beneficial habits of mind and action:

I. Practice Self- Reflection/Examination: This involves spending time on a regular basis (even daily) thinking about the person you want to become, in relation to the person you are today. It involves identifying character traits and habits that you would like to change or improve in your private and professional life; reflecting on whether you would be happy if those whom you admire and respect most knew all that you know about your actions, choices and character; and asking yourself how fully you are living up to the values you profess to yourself and others.

II. Look for Moral Exemplars: Many of us spend a great deal of our time, often more than we realize, judging the shortcomings of others. We wallow in irritation or anger at what we perceive as unfair, unkind or incompetent behavior of others, we comfort ourselves by noting the even greater professional or private failings of others, and we justify ignoring the need for our own ethical improvement by noting that many others seem to be in no hurry to become better people either. What we miss when we focus on the shared faults of humanity are those exemplary actions we witness, and the exemplary persons in our communities, that offer us a path forward in our own self-development. Exemplary acts of forgiveness, compassion, grace, courage, creativity and justice have the power to draw our aspirations upward; especially when we consider that there is no reason why we would be incapable of these actions ourselves. But this cannot happen unless we are in the habit of looking for, and taking notice of, moral exemplars in the world around us. We can also look specifically to moral exemplars in our chosen profession.

III. Exercise Moral Imagination: It can be hard to notice our ethical obligations, or their importance, because we have difficulty imagining how what we do might affect others. In some sense we all know that our personal and professional choices almost always have consequences for the lives of others, whether good or bad. But rarely do we try to really imagine what it will be like to suffer the pain that our action is likely going to cause someone – or what it will be like to experience the joy, or relief of pain or worry that another choice of ours might bring. This becomes even harder as we consider stakeholders who live outside of our personal circles and beyond our daily view. The pain of your best friend who you have betrayed is easy to see, and not difficult to imagine before you act - but it is easy not to see, and not to imagine, the pain of a person on another continent, unknown to you, whose life has been ruined by identity theft or political persecution because you recklessly allowed their sensitive data to be exposed. The suffering of that person, and your responsibility for it, would be no less great simply because you had difficulty imagining it. Fortunately, our powers of imagination can be increased. Seeking out news, books, films and other sources of stories about the human condition can help us to better envision the lives of others, even those in very different circumstances from our own. This capacity for imaginative empathy, when habitually exercised, enlarges our ability to envision the likely impact of our actions on other stakeholders. Over time, this can help us to fulfill our ethical obligations and to live as better people.

IV. Acknowledge Our Own Moral Strength: For the most part, living well in the ethical sense makes life easier, not harder. Acting like a person of courage, compassion and integrity is, in most circumstances, also the sort of action that garners respect, trust and friendship in both private and professional circles, and these are actions that we ourselves can enjoy and look back upon with satisfaction rather than guilt, disappointment or shame. But it is inevitable that sometimes the thing that is right will not be the easy thing, at least not in the short term. And all too often our moral will to live well gives out at exactly this point – under pressure, we take the easy (and wrong) way out, and try as best we can to put our moral failure and the harm we may have done or allowed out of our minds.

One of the most common reasons why we fail to act as we know we should is that we think we are too weak to do so, that we lack the strength to make difficult choices and face the consequences of doing what is right. But this is often more of a self-justifying and self-fulfilling fantasy than a reality; just as a healthy person may tell herself that she simply can't run five miles, thus sparing her the effort of trying what millions of others just like her have accomplished, a person may tell herself that she simply can't tell the truth when it will greatly inconvenience or embarrass her, or that she simply can't help someone in need when it will cost her something she wants for herself. But of course people do these things every day; they tell the morally important truth and take the heat, they sell their boat so that their disabled friend's family does not become homeless, they report frauds from which they might otherwise have benefited financially. These people are not a different species from the rest of us; they just have not forgotten or discounted their own moral strength. And in turn, they live very nearly as they should, and as we at any time can, if we simply have the will.

V. Seek the Company of Other Moral Persons: Many have noted the importance of friendship in moral development; in the 4th century B.C. the Greek philosopher Aristotle argued that a virtuous friend can be a 'second self,' one who represents the very qualities of character that we value and aspire to preserve in ourselves. He notes also that living well in the ethical sense requires ethical actions, and that activity is generally easier and more pleasurable in the company of others. Thus seeking the company of other moral persons can keep us from feeling isolated and alone in our moral commitments; friends of moral character can increase our pleasure and self-esteem when we do well alongside them, they can call us out when we act inconsistently with our own professed ideals and values, they can help us reason through difficult moral choices, and they can take on the inevitable challenges of ethical life with us, allowing us to weather them together.

Aside from this, and as compared with persons who are ethically compromised, persons of moral character are direct sources of pleasure and comfort – we benefit daily from their kindness, honesty, mercy, wisdom and courage, just as they find comfort and happiness in ours. On top of all of this, Aristotle said, it is only in partnership with other good and noble people that we can produce good and noble things, since very little of consequence can be accomplished in life without the support and help of at least *some* others.

Question 5:3: Of these five moral habits and practices, which do you think you are best at presently? Which of these habits, if any, would you like to do more to cultivate?

Question 5.4: In what specific ways, small or large, do you think adopting some or all of these habits could make a person a better cybersecurity professional?

CASE STUDY 5

Anthony and Sarah are a cybersecurity team hired by a young but growing mobile device manufacturer to beef up their infosec operations. The company had two embarrassing security breaches in recent months and is determined to take a more aggressive security approach moving forward; a friend of the company's founders recommended Anthony and Sarah as fitting the bill. Anthony and Sarah favor an especially aggressive and offense-driven style of cybersecurity practice. Their techniques include:[13]

> *Forced Inoculation in the Wild*: If Anthony and Sarah discover a worm that is beginning to spread quickly on the manufacturer's devices, they will design and release 'into the wild' (on the Internet) a worm of their own design that remotely and autonomously patches host systems against the malware. Users are not made aware that they are downloading or installing the patch worm, it is spread and activated through the same surreptitious techniques as malware.
>
> *Automated Disabling*: They create a security tool that, if it detects an infected host computer on the network, immediately launches a disabling attack on that computer, breaking its link to the network so that it cannot infect more systems. The infected host computer will, without warning, lose its network connection and all networked programs running will be interrupted until the security administrator can come to disinfect, patch, and reboot the host computer.
>
> *Hacking Back and Honeypots*: Anthony and Sarah use a variety of techniques to attack computers that appear to be carrying out hostile actions against their network: from installing spyware on attacking systems in an effort to identify the perpetrator, installing disabling malware on the attacking system, deleting stolen data, and creating 'honeypots' on their own network that appear to be vulnerable troves of sensitive data but really allow them to lure and infect attackers' systems. They are aware that these techniques in many contexts are illegal and pose the risk of 'collateral damage' to innocent third parties whose systems have been commandeered or spoofed without their knowledge, but they see their vigilante approach as justified, at least in some cases, by the lack of effective law enforcement remedies for ransomware and other cyberattacks on the company.

Anthony and Sarah know that their methods are regarded as ethically questionable by a significant portion of the security community, and so they do not disclose details of their methods, either to their employer (who takes a "the less I know the better" approach,) or to users of the company network or the public whose systems may be impacted by their methods. Their motto is, 'the ends justify the means,' and if they can discourage future attacks on the company, they regard their job as well done.

[13] See https://www.secureworks.com/blog/ethics for a description of some of these techniques and the ethical dilemmas they pose.

Question 5.5: Identify the 5 most significant ethical issues/questions raised by this Anthony and Sarah's cybersecurity practice.

Question 5.6: Off the first set of 12 ethical best practices in cybersecurity listed in Section 5, which ones do Anthony and Sarah seem *not* to reliably practice? Explain your answer.

Question 5.7: How might Anthony and Sarah's conduct be judged according to each of the three ethical theories described in Section 4: Utilitarian, Deontological, and Virtue Ethics? Briefly explain your answers for each.

Question 5.8: How should the conduct of Anthony and Sarah's employer be evaluated here? Was it ethical, and if not, what ethical standards/duties/best practices were violated by the employer?

Question 5.9: What might be the fallout if Anthony and Sarah's methods cause harm to the property, data, or other significant interests of innocent parties, and this becomes public knowledge? How are the impacted stakeholders: the company's employees, investors, members of the public, the tech media, and the cybersecurity community of professionals— likely to react? Will they accept Anthony and Sarah's claims of justification? Why or why not?

CASE STUDY 6

In this concluding exercise, you (or, if your instructor chooses, a team) will design your own case study involving a hypothetical cybersecurity scenario.

(Alternatively, your instructor may provide you or your team with an existing case study for you to analyze, for example, the 2016 Apple vs. FBI dispute over encryption.)

After coming up with your case outline, **you or your group must *identify*:**

1. The various types of stakeholders potentially affected by the case, and the different stakes/interests they have in the outcome.

2. The different types of cybersecurity professionals or practitioners that might be involved in a case like this, and their specific responsibilities.

3. The potential benefits and risks of harm that could be created by effective or ineffective cybersecurity practices in the case, including 'downstream' impacts.

4. The ethical challenges most relevant to this case (be sure to draw your answers from the list of challenges outlined in Part Two of this module, although feel free to note any other ethical challenges not included in that section).

5. The ethical obligations to the public that such a case might entail for the cybersecurity professionals involved.

6. Any potential in the case for disparate impacts on others, and how those impacts might affect the lives of different stakeholders.

7. The ethical best-case scenario (the best outcome for others that the cybersecurity practitioners involved could hope to secure from their practice) *and* a worst-case scenario (how their failures, poor decisions, or missed opportunities could lead to an ethical disaster or at least substantial harm to the significant interests of others).

8. *One* way that the risk of the worst-case-scenario could be reduced in advance, and one way that the harm could be mitigated *after*-the-fact by an effective crisis response.

9. At least *two* brief proposals or ideas for approaching the case in the most ethical way possible. Use the module content, especially Parts Two and Five, to help you come up with your ideas.

APPENDIX A. RELEVANT PROFESSIONAL ETHICS CODES & GUIDELINES

As noted in the Introduction to this module, the sheer variety of professional and personal contexts in which cybersecurity is practiced is such that no single code of professional ethics or list of professional cybersecurity guidelines will be relevant for all practitioners. However, below are some available resources that will be relevant to many readers:

Information Security Systems Association (ISSA) Code of Ethics
http://www.issa.org/?page=CodeofEthics

SANS Institute Code of Ethics
https://www.sans.org/security-resources/ethics

Cybersecurity Institute Code of Ethics and Conduct
http://www.cybersecurityinstitute.biz/training/ethicsconduct.htm

ASIS Code of Ethics
https://www.asisonline.org/About-ASIS/Pages/Code-of-Ethics.aspx

Code of Ethics and Professional Conduct of ACM (Association for Computing Machinery)
https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct

Software Engineering Code of Ethics and Professional Practice of ACM (Association for Computing Machinery) and IEEE-Computer Society
http://www.acm.org/about/se-code

APPENDIX B. BIBLIOGRAPHY/ADDITIONAL READING

Online Resources (see also Appendix A)

ABET (Accreditation Board for Engineering and Technology). http://www.abet.org/

ACM/IEEE-Computer Society. Software Engineering Code of Ethics and Professional Practice. Version 5.2. http://www.acm.org/about/se-code

National Academy of Engineering's Center for Engineering, Ethics and Society (CEES). http://www.nae.edu/26187.aspx

NSPE (National Society of Professional Engineers). Engineering Ethics. http://www.nspe.org/Ethics/index.html

Online Ethics Center for Engineering and Research. http://www.onlineethics.org/

Selected Books and Edited Collections (in reverse chronological order)

Manjikian, Mary (2017) *Cybersecurity Ethics: An Introduction*, Routledge; 240 pp.

Taddeo, Mariarosaria and Glorioso, Ludovica (2017) *Ethics and Policies for Cyber Operations*, Springer.

EC Council (2016) *Ethical Hacking and Countermeasures* (Book Series, 4 volumes), Cengage Learning.

Lucas, George (2017) *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare*, Oxford University Press; 187 pp.

Spinello, Richard (2014) *Cyberethics: Morality and Law in Cyberspace*, 5th ed., Jones & Bartlett; 246 pages.

Taddeo, Mariarosaria, ed. (2013) *Online Security and Civil Rights* A Special Issue of *Philosophy & Technology*, 26:4.

Tavani, Herman T. (2013) *Ethics and Technology: Controversies, Questions, and Strategies in Ethical Computing*, 4th Ed., John Wiley & Sons; 454 pages.

Solove, Daniel (2011) *Nothing to Hide: The False Tradeoff Between Privacy and Security*. Yale University Press; 256 pages.

Floridi, Luciano, ed. (2010) *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press; 342 pages.

Johnson, Deborah G., ed. (2009) *Computer Ethics*, 4th ed., Pearson; 216 pages.

Nissenbaum, Helen (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press; 304 pages.

Himma, Kenneth E. and Tavani, Herman T., eds., (2008) *The Handbook of Information and Computer Ethics*, John Wiley & Sons; 702 pages.

Weckert, John, ed. (2007) *Computer Ethics*, Ashgate; 516 pages.

Spinello, Richard and Tavani, Herman T. eds. (2004) *Readings in Cyberethics*, Jones and Bartlett; 697 pages.

Bynum, Terrell Ward and Rogerson, Simon, eds. (2004) *Computer Ethics and Professional Responsibility*, Blackwell; 378 pages.

Johnson, Deborah G. and Nissenbaum, Helen, eds. (1995) *Computers, Ethics & Social Values*, Prentice Hall; 656 pages.

Selected Articles and Encyclopedia Entries (in reverse chronological order)

Bustard, John D. (2017), "Improving Student Engagement in the Study of Professional Ethics: Concepts and an Example in Cyber Security" *Science and Engineering Ethics*, 1-16.

Trull, Jonathan "A Snapshot in Cybersecurity Ethics," Regis University College of Computer and Information Sciences, http://informationassurance.regis.edu/ia-programs/resources/blog/cyber-security-ethics. Accessed September 22, 2017.

Baldini, Gianmarco, Botterman, Maarten, Neisse, Ricardo, and Tallacchini, Mariachiara (2016) "Ethical Design in the Internet of Things," *Science and Engineering Ethics*, 1-21.

Rogaway, Philip (2015) "The Moral Character of Cryptographic Work," http://web.cs.ucdavis.edu/~rogaway/papers/moral.pdf

Cavelty, Myriam D. (2014) "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities," *Science and Engineering Ethics* 20:3, 701-715.

Grodzinsky, Frances S., Miller, Keith W. and Wolf, Marty J. (2012) "Moral responsibility for computing artifacts: "the rules" and issues of trust." *ACM SIGCAS Computers and Society*, 42:2, 15-25.

Bynum, Terrell (2011) "Computer and Information Ethics", *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta (ed.), http://plato.stanford.edu/archives/spr2011/entries/ethics-computer/

Dipert, Randall R. (2010) "The Ethics of Cyberwarfare," *Journal of Military Ethics* 9:4, 384-410.

Berenbach, Brian and Broy, Manfred (2009). "Professional and Ethical Dilemmas in Software Engineering." *IEEE Computer* 42:1, 74-80.

Erdogmus, Hakan (2009). "The Seven Traits of Superprofessionals." *IEEE Software* 26:4, 4-6.

Hall, Duncan (2009). "The Ethical Software Engineer." *IEEE Software* 26:4, 9-10.

Rashid, Awais, Weckert, John and Lucas, Richard (2009). "Software Engineering Ethics in a Digital World." *IEEE Computer* 42:6, p. 34-41.

Gotterbarn, Donald and Miller, Keith W. (2009) "The public is the priority: making decisions using the Software Engineering Code of Ethics." *IEEE Computer*, 42:6, 66-73.

Gotterbarn, Donald. (2008) "Once more unto the breach: Professional responsibility and computer ethics." *Science and Engineering Ethics* 14:1, 235-239.

Johnson, Deborah G. and Miller, Keith W. (2004) "Ethical issues for computer scientists." *The Computer Science and Engineering Handbook* 2nd Ed,, A. Tucker, ed. Springer-Verlag, 2.1-2.12.

Gotterbarn, Donald (2002) "Software Engineering Ethics," *Encyclopedia of Software Engineering*, 2nd ed., John Marciniak ed., John Wiley & Sons.

On General Philosophical Ethics

Aristotle (2011). *Nicomachean Ethics.* Translated by R.C. Bartlett and S.D. Collins. Chicago: University of Chicago Press.

Cahn, Steven M. (2010). *Exploring Ethics: An Introductory Anthology*, 2nd Edition. Oxford: Oxford University Press.

Shafer-Landau, Russ (2007). *Ethical Theory: An Anthology.* Oxford: Blackwell Publishing.