Ethics in Technology

Ed Weber

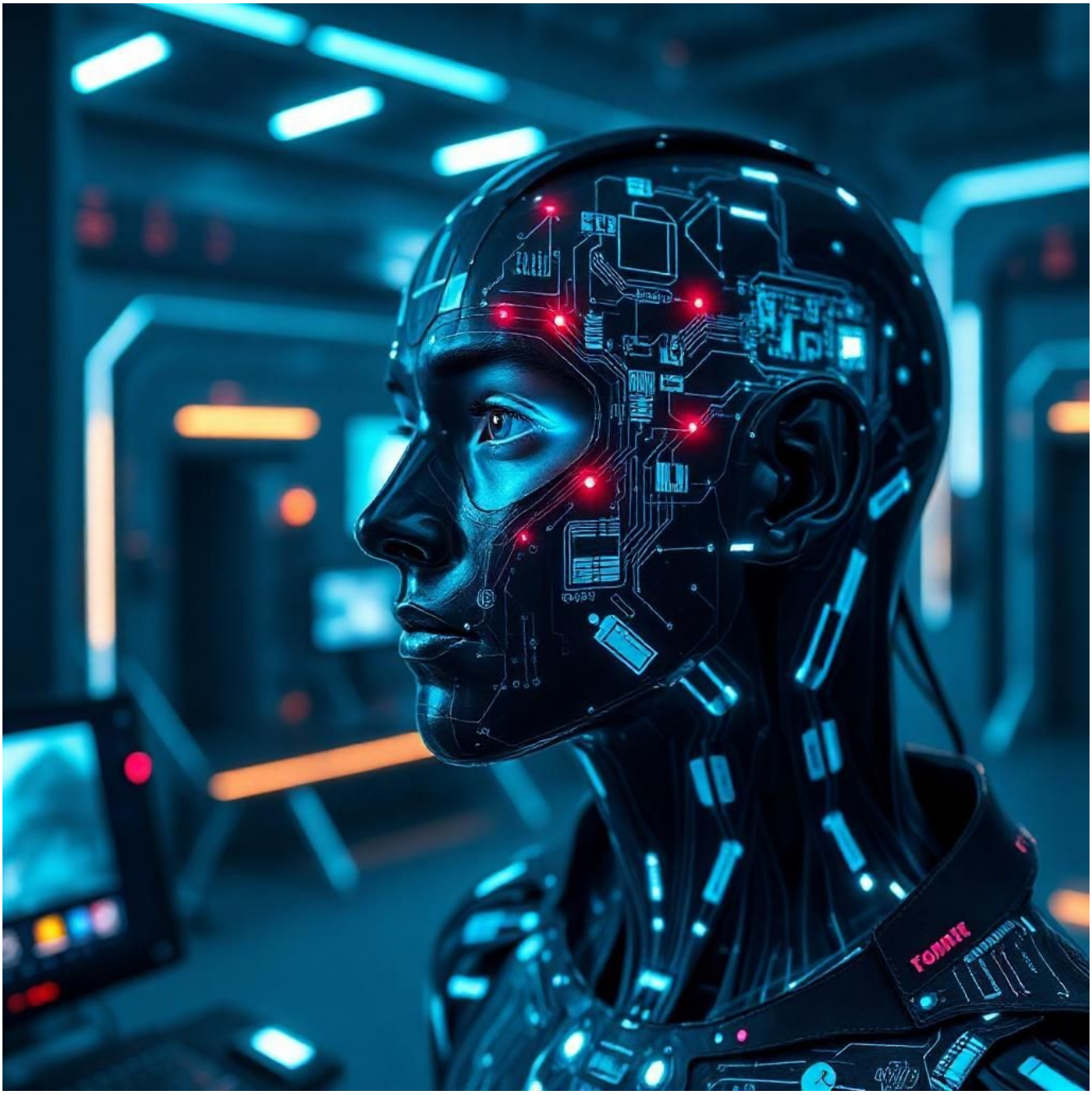


Figure 1: Cover Art generated by Pixlr

Original Publication: July 7, 2025

Table of Contents

1. Preface

About this text, the author, and Open Education Resource (OER) Copyright

About this text

The purpose of this text is to serve as an Open Education Resource (OER) designed initially to be used in a secondary or post-secondary education setting. It is intended to be a guide to facilitate focused discussions about contemporary issues of the ethical considerations related to technology evolution, development, deployment, and consumption, as well as issues (both known and unknown) of potential misuse and abuse of technology. This is *not* a traditional Ethics textbook in that it is not intended to provide a survey of all of the history of Ethics through the ages nor is it intended to dive deeply into any particular ethical movements or frameworks as may be the focus of other ethics studies. Rather, it is intended to focus predominantly on the concepts of *applying critical and ethical thinking* to issues and subsequent decisions related to our interactions with technology in the 21st century.

If you came here looking for definitive answers – I'm so sorry to disappoint you. This text does not purport to include any categorical absolutes or any sort of an ethical road map for the reader to adopt. Rather, the intent is to be a *starting point* for the thinking person to consider one's own perspectives and understandings of:

- what the concept of 'ethics' means to you as you begin your exploration...
- what influences (family, school, religion, region, ethnicity, gender identity, socioeconomic status, etc.) have come together to make you the 'who' you are at this moment…
- what are the skills necessary to be able to *objectively* review a concept or situation so as to understand what its ethical issues may be…
- what it actually means to have a choice between more than one option and how to be able to make an informed decision *for yourself* that includes ethical considerations…
- how to recognize that while technology continues to advance, other systems like legal systems, economic systems, political systems, social systems, and individual and group moral and ethical systems often lag *significantly* behind the rate of change of technology.

This text is best used in conjunction with case studies and examples (both historic and contemporary) to serve as springboards for in-depth discussion surrounding the various topics. As an OER, it is expected that some of the case studies and examples that are initially presented throughout the text will become 'stale' over time. Therefore, it is encouraged that adopters of this text consider enhancing this base text with additional, contemporary case studies or other source materials which exemplify the topics. Likewise, it is encouraged that students and other consumers of this text *also* bring suggested new case studies and examples for possible inclusion. New examples of both ethical

and unethical behaviors, decisions, and applications of technology continue to happen every single day. It is a hope of the author that those who work with this text will begin to adopt a habit of intentionally and closely examining the ethical considerations of their respective interactions with technology.

Throughout this text, we will discover that having a shared understanding of the *intended definition* of critical terms (if not a shared agreement of those meanings) is critical in order to have meaningful discourse about these ethereal concepts. As a result, many terms will be presented throughout this text which will require this shared understanding of the author's intended meaning.

As a result, terms that may be subject to multiple definitions or interpretations are highlighted in **bold** in this text. The definition of these terms may appear when they are first used, or may be defined at the end of the chapter in which they are used. Throughout the use of this text, it is important that the reader and others involved in discussions about these topics have a minimum of a shared definition of what each critical term means and the context in which the terms are being used.

About the Author

Figure 2: Ed Weber, Assoc. Prof. of Computer Science SCC

Hello good reader! I am Ed Weber, an Associate Professor of Computer Science at St. Charles Community College (SCC) in Cottleville, MO. I also am the President and owner of Weber Enterprises, LLC of Wildwood, MO, which was founded in 1995. I have spent my entire career in Information Systems working with both very large companies, and with mid-size and small clients. I have been teaching Information Systems and Computer Science since 1996 originally as an adjunct instructor and then as a full-time Assistant Professor with Millikin University for 9 ½ years before joining SCC. I have seen countless technologies come and go throughout my career and I have witnessed both the ethical *and* unethical implementations of technology as well.

When I wrote my first textbook, Spreadsheet Fundamentals, in 2018, it was for the primary purpose of reducing the cost of a required textbook for my class. This was a direct and intentional action when I realized that some of my students were struggling because they didn't have the financial support to buy the textbook we were previously using. This was my first real exposure to the realities of the ethical issues surrounding the *digital divide* (see Chapter 6). At that time, I was unaware of the Open Education Resources (OER) concepts and that there was a way for me to publish the textbook to be 100% free of charge. Rather, I was approached by a traditional textbook publisher who helped me in my first publishing endeavor.

So, while my first publication allowed me to reduce the cost of the text from nearly $200 to under $40, I have subsequently learned how the OER model affords me an opportunity to make new

classroom materials for students that will be forever 100% free of charge. That is my primary purpose in developing *this* text.

Throughout my career, I have often found myself in situations where I had to make decisions and take actions which would have *significant* ethical implications for myself, my family, my colleagues, my staff, my employees, my clients, my organization, and even my entire community. The more often that these types of situations occurred, the more I realized that you don't want to *begin* thinking about the ethical issues of your situation when you are already knee-deep in the middle of it! Rather, it seems to be healthier for me to be more *proactive* when it comes to thinking about ethics and how I incorporate my understandings into my day-to-day life and decisions.

Therefore, this text will attempt to lay out just a sampling of some of the major technology-related topics that are happening at this time which have *exceptional* ethical considerations. It is my hope that by thinking about (and discussing) these topics *before* you find yourself in the middle of making any significant decisions, you will be able to find yourself much more prepared for the decisions that life will be throwing at you.

Open Education Resource (OER) Copyright

Open Educational Resources (OER) are teaching, learning, and research materials that are freely available for anyone to use, adapt, and share. These resources can include textbooks, course materials, videos, tests, and software, and are either in the public domain or released under an open license that permits no-cost access, reuse, modification, and redistribution by others. The purpose of OER is to reduce barriers to education by providing high-quality materials that can be tailored to meet local needs and contexts.

The images found in this text have the following attributions:

- The internet memes and Maslow's hierarchy image do not receive any attribution as they are considered in the public domain.
- The screenshot of the website is attributed with the citation for the entire content taken from that site
- All of the rest of the images were created by me and referenced when using the Pixlr AI tool.

2. Introduction, Ethical Frameworks and Personal Lenses

Foundations; Frameworks and Personal Lenses; Key Concepts

Foundations

From an early age, most people experience the concept of *Ethics* long before they ever learn that there is a term to describe the concept that they are experiencing. Many individuals might say that the term includes some concept of **right vs. wrong**, or **good vs. evil**, and how *these* concepts affect a person's behaviors. And maybe, they consider *Ethics* to be the full collection of a person's attitude and behaviors and their **rightness vs. wrongness**. But as we can see, often trying to define one term leads us down a rabbit-hole where we discover that we need to define even more terms! In fact, a large part of the first few chapters of this text will focus on the necessity of **defining terms** and why it is necessary to have a **shared understanding** of the critical terms which we use to have discussions about ethics.

For example, what do *you think* is the meaning of the term: **Ethics**? I'm sure that most folx would be able to come up with their own definition of what they think Ethics means. Take a few moments to see if you can come up with your own definition of what you think the term *Ethics* means for you… go ahead… we'll wait.

Now that you have your own definition of *Ethics* in your mind, let's now consider a follow-up question: How did you come to have this understanding of what you think Ethics means? Did you previously learn a formal definition of the term from a textbook or a dictionary? Did you learn it from some previous class or somewhere else in school? Were you told what the term means from your parents or grand-parents or other family members? Did you learn the term from your religious leaders? Did you read it in a sacred book? Did you learn it from television or the movies? Did you learn it on the Internet? Did you Google it? From social media? From an influencer? Did you as a generative AI tool? Really think about it. Where *did* you get your understanding of this term?

And next, while you contemplate all of the possible places where you might have *learned* the term, the next follow-up question is this: Whomever provided you with this definition… were they *right*? Where did *they* learn it from? Is it possible (… *just possible* …) that they got it *wrong*? Who, ultimately, gets to decide – for you – what the acceptable definition of this term *Ethics* may be? Or, for that matter, who gets to decide – for you – what the acceptable definition of *any* term is going to be?

As you can quickly see, this text will be full of a *lot* more questions than answers! But it is precisely these questions that will help guide you through thoughtful and insightful discussions about how the ethical aspects of technology are becoming more and more significant every day.

Before continuing, it may be helpful to list some of the significant philosophical movements and just a few of the many ethicists whose work may be considered most relevant to the concept of *applying ethical thinking* to issues surrounding technology.

Applicable Ethical Movements

- **Deontological Ethics (18th Century)**
  Deontological ethics emphasizes duty, rules, and the inherent rightness or wrongness of actions regardless of consequences. This framework provides essential grounding for technology ethics by establishing inviolable principles such as respect for human dignity, autonomy, and rights that must be preserved regardless of technological benefits. In applied technology ethics, deontological thinking helps establish non-negotiable boundaries around issues like privacy, consent, and human agency that cannot be overridden by utilitarian calculations of greater good.
- **Rationalism (Enlightenment Era, 17th-18th Century)**
  Rationalism emphasizes reason, logic, and systematic thinking as the primary sources of knowledge and ethical guidance. This movement is foundational to applied technology ethics because it provides methodological approaches for analyzing complex technological systems and their ethical implications through structured reasoning. Rationalist approaches help technologists and ethicists develop systematic frameworks for evaluating emerging technologies rather than relying solely on intuition or tradition.
- **Utilitarianism (18th-19th Century)**
  Utilitarianism judges actions based on their consequences and seeks to maximize overall well-being or happiness for the greatest number of people. This consequentialist approach is highly relevant to technology ethics because it provides frameworks for weighing the benefits and harms of technological innovations across large populations. Applied technology ethics frequently employs utilitarian analysis when evaluating trade-offs between technological progress and potential societal risks, such as balancing AI efficiency gains against job displacement or privacy concerns.
- **Humanism (Renaissance/Modern Era, 15th-20th Century)**
  Humanism places human dignity, agency, and flourishing at the center of ethical consideration. This perspective is crucial for technology ethics as it ensures that technological development serves human needs and preserves human agency rather than subordinating humans to technological systems. Applied technology ethics draws on humanist principles to advocate for human-centered design, meaningful human oversight of automated systems, and the preservation of human choice and autonomy in technological environments.

- **Feminism (19th-20th Century)**
  Feminist ethics emphasizes care, relationships, context, and the examination of power structures, particularly how they affect marginalized groups. This movement brings essential perspectives to technology ethics by highlighting how technological systems can perpetuate or challenge existing inequalities and by advocating for inclusive design processes. Applied technology ethics incorporates feminist insights to address issues like algorithmic bias, the digital divide, and ensuring diverse voices are included in technological development and governance.
- **Phenomenology (20th Century)**
  Phenomenology focuses on lived experience, consciousness, and how individuals encounter and make meaning of their world. This movement contributes to applied technology ethics by emphasizing the importance of understanding how people actually experience and interact with technology in their daily lives. Phenomenological approaches help bridge the gap between abstract ethical principles and the concrete realities of how technology affects human experience, informing more nuanced and contextually sensitive ethical frameworks.

There are entire courses that could be taken on each one of these broad philosophical movements. But just knowing their names and descriptions can give you a starting point should you should choose to explore them in greater detail.

Now, let’s take a quick look at just a few of the historical and contemporary ethicists who have studied, expanded upon, and have otherwise contributed greatly to the pursuit of understanding of applied ethics and summarize some of their major propositions and how they *might* approach ethical issues related to technology today.

Ethicists and Their Approach to Technology Ethics

- **Immanuel Kant (Deontological Ethics)**
  - **Ethical Center:** Kant's ethical philosophy is grounded in the "Categorical Imperative," asserting that moral duties are universal and rational, requiring actions that could be applied without contradiction to all individuals and treating humanity as an end in itself, never merely as a means. Morality stems from reason and duty, independent of consequences.
  - **Approach to Technology Today:** Kant would scrutinize technological advancements through the lens of human dignity and autonomy, insisting that AI, data collection, and automation must never instrumentalize individuals. He would advocate for strict, universal ethical rules in technology design and usage, such as mandatory privacy by design and

algorithmic transparency, ensuring that technological systems uphold inherent human rights and rational agency.

- **René Descartes (Rationalism)**
  - **Ethical Center:** Descartes' ethical center is built on methodical doubt, systematic reasoning, and the pursuit of clear and distinct knowledge through logical analysis rather than relying on tradition or emotion. His approach emphasizes breaking down complex problems into manageable parts and building knowledge from foundational principles through careful reasoning.
  - **Approach to Technology Today:** Addressing contemporary technology ethics, Descartes would advocate for systematic, step-by-step analysis of technological systems, demanding clear logical justification for each design choice and rejecting technological implementations based merely on convenience, profit, or popular opinion without rigorous ethical reasoning.
- **John Stuart Mill (Utilitarianism)**
  - **Ethical Center:** Mill's ethical center focuses on maximizing overall happiness and well-being while protecting individual liberty, emphasizing that the greatest good for the greatest number must be balanced against the fundamental importance of personal freedom and self-determination. His harm principle argues that society can only restrict individual liberty to prevent harm to others, creating a framework that values both collective welfare and individual autonomy.
  - **Approach to Technology Today:** When applied to technology, Mill’s ideas guide ethical evaluations of innovations like autonomous vehicles or predictive algorithms, helping to weigh benefits (e.g., safety, efficiency) against societal costs (e.g., job loss, privacy erosion).
- **Martha Nussbaum (Humanism)**
  - **Ethical Center:** Nussbaum's ethical center emphasizes human capabilities, dignity, and flourishing, arguing that societies should be structured to enable all individuals to develop their full human potential across multiple dimensions of well-being. Her capabilities approach focuses on what people are able to do and be, rather than just material resources, emphasizing the importance of agency, practical reason, and meaningful relationships.
  - **Approach to Technology Today:** Approaching contemporary technology ethics, Nussbaum would evaluate digital systems based on whether they enhance or diminish human capabilities – supporting technologies that expand access to education, meaningful work, and social connection while opposing those that create dependency, reduce critical thinking, or undermine human agency and authentic relationships.

- **Carol Gilligan (Feminist Ethics)**
    - **Ethical Center:** Gilligan's ethical center emphasizes an ethics of care that values relationships, context, and responsibility, challenging traditional moral frameworks that prioritize abstract rights and justice over concrete care and connection. Her work highlights how ethical reasoning often involves understanding particular situations and maintaining relationships rather than applying universal principles, and she emphasizes the importance of listening to marginalized voices, especially women's moral perspectives.
    - **Approach to Technology Today:** In addressing technology ethics today, Gilligan would focus on how digital systems affect relationships and care networks, advocating for inclusive design processes that center the experiences of marginalized users and questioning whether technologies strengthen or weaken our capacity for empathy, care, and authentic human connection.
- **Don Ihde (Phenomenology)**
    - **Ethical Center:** Ihde's ethical center focuses on human-technology relations and how humans and technologies mutually shape each other's existence, arguing that we cannot understand human experience without examining our relationships with technological artifacts. His postphenomenological approach emphasizes that technologies are neither neutral tools nor autonomous forces, but rather extend and transform human capabilities while simultaneously shaping how we perceive and act in the world.
    - **Approach to Technology Today:** Approaching contemporary technology ethics, Ihde would analyze how specific technologies – from smartphones to AI systems – alter our ways of being-in-the-world, advocating for careful attention to how digital interfaces change our perceptual habits, social relationships, and bodily engagement with our environment, while emphasizing that ethical evaluation must consider the concrete, lived experience of human-technology interactions rather than abstract technological assessments.

As you review the descriptions above and the works of these (or other) historical and contemporary ethicists, you will quickly discover that there are not singular, universally accepted definitions for the *terms* that are used to discuss ethics. As a matter of course, as scholars work to build their own understandings within their own disciplines, they often find themselves *redefining* previously accepted terms with new or altered meanings and nuances. In fact, you will discover completely new terms being coined to describe specific concepts or novel interpretations of life observations.

Frameworks and Personal Lenses

In this section we need to explore a bit more detailed information about myself as the author, and how this information is necessary to establish the framework in which the rest of the material for this text will be presented. It is highly suggested that everyone who utilizes this text (instructors and students alike) prepare their own supplemental *Full Disclosure* section (found below) to help you to identify and understand your own personal frameworks and personal lenses. This will greatly facilitate future topic discussions.

Full Disclosure: Your textbook author is a 61-year-old, white, cisgender, heterosexual married man. He was born and raised Catholic and went to Catholic elementary and high schools. He grew up in the Midwest of the USA in a lower-middle-class household within a homogeneous neighborhood (re: ethnicity, religion, socioeconomic status). He has been married to his wife, Kim for 40 years and they have no children by choice (… except for dogs… there will always be dogs!) Your author currently consider himself to be in the middle class on a socioeconomic scale. While your author does have some minor health issues and wears glasses to correct his vision, he would consider himself non-disabled. He is no longer a Catholic and identifies instead as an agnostic.

Your textbook author initially earned a Certificate of Proficiency in Data Processing in the late 1980s. This credential allowed him to begin a decades-long career in Information Technology. Much later on, he earned a Bachelor's Degree in Psychology with a Minor in Computer Science after having already been actively working in the field for over 20 years. In 1995, he started his own computer consulting firm which is still active today. In the mid-2000s, he earned a Master's Degree in Computer Science so as to facilitate his transition into full-time teaching at colleges and universities. He considers himself to be a life-long learner and enjoys working with others on challenging activities.

Now, considering these details about your textbook author, I am going to shift modes into a conversational mode just to talk to you about *why* I shared all of those details: I have shared these detail – not because the I consider myself to be significant or special in any way – but rather it is because these facts (and more) are the things that make up the '*who*' that I am today as I compose this text. And, as a matter of practice, whenever I attempt to think about the ethics of a given situation or technology, I try to actively take a step backwards and try to view the situation through all of the lenses that make me who I am. It can be very enlightening when I discover, "… Oh! *That* is where my attitude about this particular thing is coming from!" Sometimes, this type of introspection leads me to be able to say, "Wait a minute! It isn't **ME** that thinks this particular way about this particular thing… Rather, I was *taught/told/indoctrinated/instructed* to think this particular way about this particular thing! And now that **I** *really think about it – for myself* – **I** realize that **I** am actually free to *choose* how **I** *actually* think about this thing – all on my own!"

So, I offer up my own details here just so that you will have a good understanding of the framework that I am using to present and discuss the various concepts we cover throughout the rest of this text. It

is by intentionally inspecting and acknowledging our own lenses, that we might be able to uncover and appropriately restrain our own preconceived biases.

As you engage with the concepts and case studies in this textbook, it is important to recognize the unique set of experiences, values, and perspectives that shape your own ethical viewpoints. In this text, we will call these perspectives your **personal lenses**. Honest self-reflection can help you become more aware of your own assumptions and biases as you look through your personal lenses, allowing for more thoughtful and inclusive ethical reasoning. To help us consider these personal lenses, consider this internet meme:

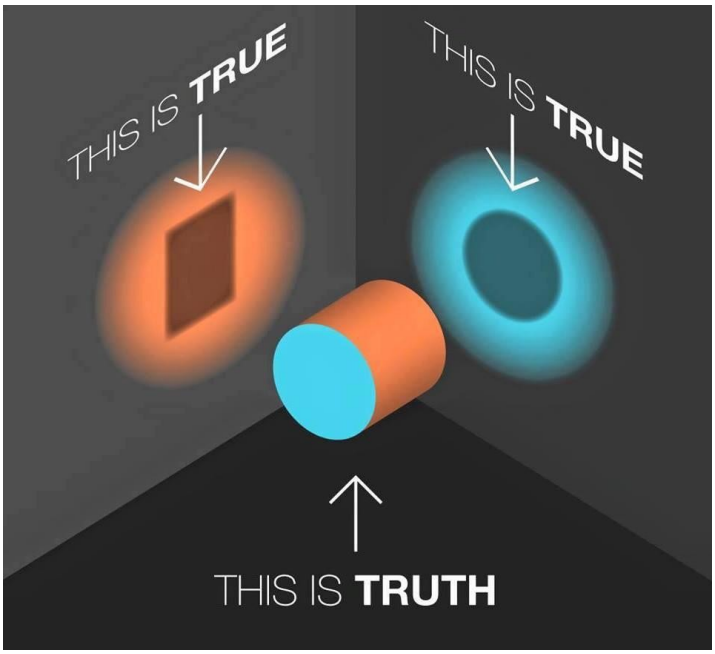


Figure 3: Truth perceived from different perspectives

The person standing near the orange light source and looking at the shadow only might say that the shape making this shadow is a square or a cube. And from *their perspective at that moment in time*, this may seem to be true.

But the person standing near the blue light source and looking at the shadow only might say that the shape making this shadow is a circle or a sphere. And, once again, from *their perspective at that moment in time*, this *too* may seem to be true.

However, by taking a step back to view even more pertinent information, a third observer can see that the shape appears to be – *as seen from this third perspective* – a cylinder suspended in such a way that the two light sources cast these two unique shadows.

Understanding that there *may, in fact,* be a difference between 'Truth' as defined with a capital 'T' when viewed from an *objective perspective,* as compared to what appears to be 'true' from our own unique perspective at any moment in time, may help us think more critically about the importance of understanding our own personal lenses.

Consider asking yourself the following questions:

- What aspects of my background (such as age, race, ethnicity, gender identity, sexual orientation, religion, socioeconomic status, education, or geographic location) have most influenced the way I see the world?
- How did my family, community, or culture shape my attitudes toward technology, authority, and ethics?
- What are my core values, and where did they come from? Have any of my values changed over time? If so, why?
- Are there beliefs or viewpoints I hold mainly because they were taught to me, rather than ones I have critically examined for myself?
- How do my personal experiences with privilege or marginalization affect the way I interpret ethical dilemmas?
- Have I ever changed my mind about a major ethical issue? What prompted that change?
- In what ways do my current roles (student, employee, family member, etc.) influence my perspective on ethical questions?
- Are there perspectives or experiences I am less familiar with? How might I seek out and learn from voices different from my own?
- When I encounter a viewpoint that challenges my own, how do I typically respond? Am I open to reconsidering my position?
- What steps can I take to recognize and address my own biases as I study Ethics in Technology?

By thoughtfully considering these questions, you can better understand the framework through which you interpret ethical issues and strive for greater objectivity and empathy in your analysis.

Let's also look at this concept of reviewing a situation both *passively* (ignoring our own personal lenses and perspectives) and then subsequently reviewing the same situation *intentionally*

(acknowledging and evaluating our own personal lenses and perspectives.) Consider this initial internet meme:

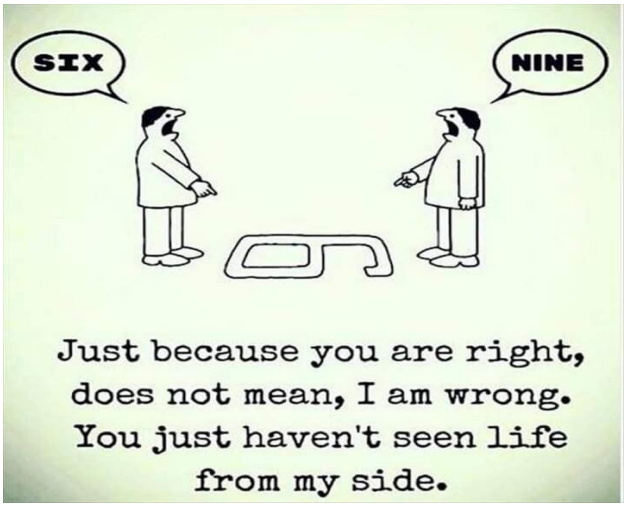


Figure 4: 6 vs. 9 as evaluated from one's own perspective

This meme, similar to the one shown in the Figure 2 earlier in this chapter, illustrates how the same 'Truth' (with a capital 'T') can actually represent two significantly different 'truths' when one only focuses on their own personal lenses and their own current perspective.

In fact, the caption within this meme attempts to establish the importance of trying to help the viewer consider what the other perspectives may look like. But is this easy to do? Consider, for example, all of the personal lenses that this textbook author shared in the previous section. Will I ever be able to realistically look at (or more rightly so – even *imagine*) any situation through the lenses of a non-white, economically struggling, lesbian, Baptist, still wanting to finish their GED someday…? My personal lenses are so significantly different than their lenses – and yet we may be looking at the exact same situation.

But is this realistic? Is it realistically even possible for us to *completely* recognize, understand, acknowledge and then fully contain all of our own personal lenses and our own current, unique perspective? Are we certain that there may not be any residual ***biases*** still influencing our interpretation of what we perceive to be both 'true' as well as the 'Truth'?

Do I have what it takes to be able to step *away* from my own personal lenses (without forgetting them or failing to acknowledge them) so that I can *try* to see through what I *imagine* another person's personal lenses might look like? Do I also recognize that my own imaginations of someone else's

personal lenses may be *pure fantasy*? How can I go about really trying to understand what another's personal lenses really look like for *them*?

For me, this kind of effort begins and ends with *communications*. Finding ways to actually ask another about their own personal lenses and perspectives seems to be a profound beginning. Then, *actively listening* as they share their own experiences – without judgment – and trying to repeat back your own understanding of what they actually say seems like an effective follow-up. Only after we have a shared understanding of each other's personal lenses can we really begin to have effective ethical discussions about various technical topics.

Now, for contrast, consider this follow-up internet meme that was based on the original theme:

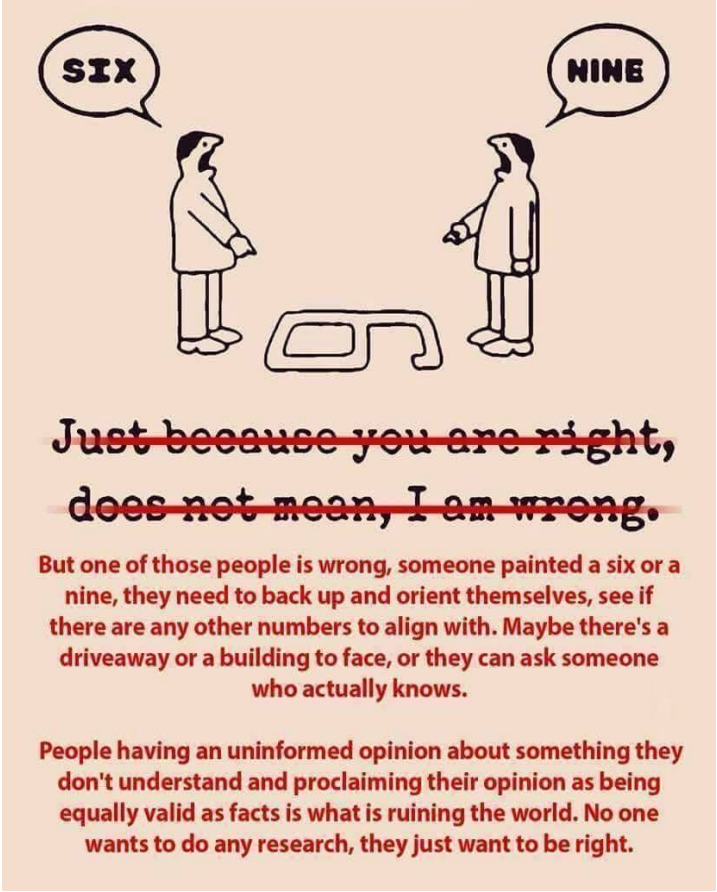


Figure 5: 6 vs. 9 reconsidered from an objective view

This meme attempts to suggest that 'Truth', with a capital 'T' exists (a concept that has been heavily debated by many ethicists throughout history!) and can be justly recognized if one simply chooses to step away from their own perspective and view the situation objectively. So, while we

might agree with the concept of trying to step outside of our own personal lenses to see a situation from a different perspective, this meme author seems more intent to show that the value from the act itself *isn't* about fostering empathy for each person's perspective (and personal lenses). Rather, this meme author seems to imply that the value is more-so that one of these people can use this technique to *prove the other one wrong!* For this unknown meme author, it's not about *empathy* but rather it is about *winning*.

Key Foundational Concepts

As you continue deeper into this text, you will discover there are a number of key concepts that are used repeatedly to help facilitate greater discussions and understandings of the various topics. This list will also serve as a preview of some of the upcoming chapter concepts.

- **Definition of terms** – Whenever not previously defined, new critical terms will be defined at each introduction so as to present what I, as the author, am using as the definition of each given term. This does **not** mean I am claiming supreme authority regarding the term! Rather, it is the *starting point* from which you can determine if you agree with the definition or not and what, if any, compromises might need to be made so as to have a meaningful discussion. It is imperative that individuals who intend to have meaningful interactions at least have a shared *understanding* of the terms being used – if not full agreement regarding the terms!
- **Technology can be found almost everywhere** – If you are reading this text, it is most likely that you are already familiar with very many forms of technology. For the vast majority of individuals, the year 2025 is synonymous with technology being integrated into almost every aspect of our existence. And as such, technology is often taken for granted without full consideration of any potential ethical considerations of that tech. For example, how often do we think about how a particular piece of tech was developed or created or distributed? Do we ever wonder just who has access to that tech and who does *not* have access? Are there any unintended uses of the tech that we should be thinking about?
- **The rate of change of technology is NOT linear** – Throughout most of human history, technological change was slow and incremental, with major breakthroughs – like the control of fire, the invention of the wheel, and the development of agriculture – occurring over thousands of years. This gradual pace continued through the Bronze and Iron Ages and even into early modern times. However, beginning with the Industrial Revolution, the **rate of technological advancement** accelerated dramatically, as mechanization, mass production, and new forms of energy rapidly transformed societies in mere centuries. Now within less than the last 100 years, the emergence of computers, the internet, and digital technologies, have brought an unprecedented surge in innovation and human adoption rates. The current era is unique for its exponentially rapid, transformative impact on nearly every aspect of life.

- **There is no universally accepted Ethical system** – The absence of a universally accepted ethical system means that actions are often interpreted through a variety of moral frameworks, leading to nuanced discrepancies or even diametrically opposed viewpoints. For example, the act of taking another person's life can be labeled as "murder," "justifiable homicide," or "self-defense," depending on the ethical system, cultural context, or legal tradition applied. What one society or theory may condemn as inherently immoral, another may view as permissible or even obligatory under certain circumstances, illustrating how ethical judgments can range from subtle distinctions to fundamentally conflicting positions. This diversity reflects the influence of different normative theories – such as utilitarianism, deontology, virtue ethics, and cultural relativism – each offering its own criteria for evaluating right and wrong. This illuminates the complexity and subjectivity inherent in ethical reasoning.
- **Legal and Societal systems attempt to implement a well defined and accepted Ethical system –** Legal and societal systems tend to follow a well-defined and accepted ethical system because such alignment provides a consistent moral foundation for laws and policies, ensuring that actions and decisions are guided by shared principles of fairness, justice, and respect for all individuals. This ethical grounding fosters public trust, transparency, and accountability, helping to protect the rights and interests of all members of society while reducing arbitrary or biased decision-making. Ultimately, integrating ethics into legal and societal frameworks promotes social cohesion, supports long-term sustainability, and enhances the legitimacy and effectiveness of institutions by aligning them with the values and expectations of the community.
- **When considering the Ethics of Technology, the issue is almost *never* the Technology, but rather the issue is almost always the Ethics** – The ethical evaluation of technology often reveals that the core issue lies not with the technology itself, but with how humans choose to use it, as the same contemporary tool can enable outcomes at nearly opposite ends of the moral spectrum. For example, artificial intelligence can be harnessed to improve healthcare diagnostics, enhance disaster response, and promote environmental sustainability, yet the very same AI systems can also be deployed for mass surveillance, autonomous weaponry, or discriminatory decision-making. This dual-use dilemma illustrates that technologies are inherently neutral, but their ethical character is defined by human intentions, societal values, and regulatory choices, resulting in applications that can be seen as highly beneficial or deeply problematic depending on context and use. Thus, it is the ethical framework guiding deployment and oversight – not the technology itself – that determines whether its impact is viewed as just, responsible, or harmful.
- **With technology, very often science fiction can be viewed as science fact that just hasn't happened yet** – Since the age of radio and television, science fiction authors, movies, and

shows have repeatedly imagined technologies that later became reality, often serving as inspiration or conceptual blueprints for real-world innovation. Classic examples include video calling, featured in "The Jetsons" and "Metropolis," now realized through platforms like Zoom; wireless earbuds, reminiscent of Ray Bradbury's "Fahrenheit 451," now ubiquitous as devices like AirPods; and handheld communicators from "Star Trek," which anticipated today's smartphones. Science fiction has also envisioned self-driving cars, as described by Isaac Asimov, and immersive virtual reality, as seen in "The Matrix," both of which are now active areas of technological development. Even broader concepts, such as global information networks and intelligent digital assistants, were explored in early fiction long before the internet or AI became commonplace. This demonstrates how speculative storytelling has consistently anticipated – and sometimes directly influenced – the trajectory of technological advancement.

Textbook Definitions – Introduction, Ethical Frameworks and Personal Lenses

- **right vs. wrong** – The distinction between actions or choices considered morally acceptable and those considered morally unacceptable.
- **good vs. evil** – The contrast between that which is morally virtuous, beneficial, or constructive and that which is morally wrong, harmful, or destructive.
- **rightness vs. wrongness** – The quality of being in accordance with moral or ethical principles versus being in violation of them.
- **defining terms** – The process of clearly explaining the meaning of words or concepts to ensure clarity and understanding.
- **shared understanding** – A mutual agreement or common interpretation of ideas, terms, or values among individuals or groups.
- **Ethics** – The branch of philosophy concerned with moral principles that govern behavior and decision-making.
- **Deontological Ethics** – An ethical theory that judges the morality of actions based on adherence to rules or duties, regardless of their consequences.
- **Rationalism** – A philosophical view that emphasizes reason and logical analysis as the primary sources of knowledge and ethical judgment.
- **Utilitarianism** – An ethical framework that evaluates actions based on their outcomes, aiming to maximize overall happiness or well-being.

- **Humanism** – A worldview that centers human dignity, agency, and the promotion of individual and collective flourishing as ethical priorities.
- **Feminism** – An ethical and social movement that advocates for gender equality and emphasizes the importance of care, context, and power dynamics in moral decision-making.
- **Phenomenology** – A philosophical approach that focuses on individuals' lived experiences and the ways in which they perceive and interpret the world around them.
- **personal lenses** – The unique perspectives shaped by an individual's experiences, values, and cultural background through which they interpret the world.
- **rate of technological advancement** – The speed at which new technologies are developed and adopted within society.

3. Defining Ethics and Related Terminology

Why are we here?; Textbook Definitions – the basics; Ethical vs. Legal; Critical Thinking and Limiting Biases

Why are we here?

Wow! If THAT isn't a loaded question!

But that is exactly what we would like to tackle at this point. *Why* should we think about this concept of Ethics and how it can be defined and applied to technology?

To get our own thoughts germinating, I asked several generative AI platforms (Perplexity, ChatGPT, Claude, and Gemini) to provide a hypothetical response to this question as written from the perspective of several selected ethicists. Here is what was generated:

- **Immanuel Kant (Deontological Ethics)**
  "We must think about ethics in technology because human beings possess inherent dignity as rational agents, and technology must never treat us merely as means to an end. Every technological system embeds moral choices about how humans should be treated, and without ethical reflection, we risk creating tools that violate our fundamental duty to respect human autonomy and dignity. The categorical imperative demands that we only develop technologies whose principles we could will to be universal laws—would we want to live in a world where all technology operates according to the ethical assumptions built into our current systems?"
- **René Descartes (Rationalism)**
  "We must apply systematic ethical reasoning to technology because, without methodical analysis, we build upon uncertain foundations that may lead us astray. Just as I doubted everything to reach clear and distinct knowledge, we must doubt the moral assumptions embedded in our technologies and rebuild them on solid rational principles. Technology amplifies human action, so any errors in our ethical reasoning will be magnified across society—we cannot afford to proceed on mere tradition, convenience, or popular opinion when the stakes are so high."
- **John Stuart Mill (Utilitarianism)**
  "Ethics in technology matters because technology's power to generate both tremendous benefits and serious harms across vast populations demands careful calculation of consequences. We must evaluate whether our technological choices truly maximize overall human happiness and well-being, while vigilantly protecting individual liberty from technological systems that might restrict human self-determination. The harm principle requires us to examine whether our technologies prevent individuals from pursuing their own good in their own way, even when such technologies might benefit the majority."

- **Martha Nussbaum (Humanism)**
  "We need ethics in technology because technology should serve human flourishing by expanding rather than constraining human capabilities. Every technological design choice affects whether people can live fully human lives—whether they can engage in practical reason, form meaningful relationships, experience joy, exercise bodily autonomy, and participate in political life. Without ethical reflection, we risk creating technologies that diminish rather than enhance what makes us human, particularly for those who are already marginalized or vulnerable in society."
- **Carol Gilligan (Feminist Ethics)**
  "Ethics in technology is essential because technological decisions affect relationships, care networks, and the voices that get heard in our society. We must ask not just whether technologies work efficiently, but whether they strengthen or weaken our capacity for care, empathy, and connection with others. Ethical reflection helps us recognize whose perspectives have been excluded from technological design and ensures that we consider how our tools affect the most vulnerable members of our communities, particularly when those voices are often silenced in traditional ethical frameworks."
- **Don Ihde (Phenomenology)**
  "We must think ethically about technology because humans and technologies co-constitute each other's existence—there is no neutral technology, and every technological relation shapes how we perceive, act, and experience the world. Ethics helps us examine how specific technologies alter our ways of being-in-the-world, sometimes in ways we don't immediately recognize. Without phenomenological reflection on our actual lived experience with technologies, we may inadvertently adopt tools that fundamentally change what it means to be human without conscious deliberation about whether those changes align with our values."

Did these hypothetical responses from historic and contemporary ethicists *actually* help you discover or clarify your own reason for being here?

For some individuals, simply reviewing what others have previously thought or discovered about a topic can be truly enlightening and inspiring! Academics and Ethicists through the ages have invested much of their lives and studies to review, categorize, differentiate, and subsequently expand and expound on what *others* have to say about Ethics. And sometimes, they find that one or more of these other people had previously found ways to express, *precisely or nearly so*, just what it was that they, themselves, think about the topic.

And yet for other individuals, the flood of disparate and often contradictory positions on the *supposed* same topic seems to simply add levels of confusion and introduce unintentional biases.

These individuals feel that the research actually *gets in the way* of their own ability to figure anything out for themselves.

So, whichever kind of person you may be, I'd like to re-ask the questions: Why are we here? Why should we think about this concept of Ethics and how it can be defined and applied to technology?

Very early in my career, I learned an important lesson that has informed my entire professional and teaching philosophy: When working with adults, **if** all individuals involved can *first* understand and agree on 'the **WHY'** of whatever it is that they are doing, then adults tend to be more receptive to fully engage in the related tasks. So, for me, I try to consistently first ask and answer the question, "Why are we doing this again?" before we even get started.

For me, the WHY is that, as a technology professional for my entire career, I have seen too often – first hand – what the ***un***ethical implementation of technology looks like and what I have perceived to be the harmful ramifications of these unethical situations. And as such, I choose to intentionally explore the ethics surrounding technology so that I can be more prepared to work with students, colleagues and clients as we collectively discover just what the ethical issues might be. This has helped me identify and recognize some of my own biases and has helped me learn how to be more objective in my ethical analysis of new technological advancements.

Also, as previously mentioned, the *proactive intentional examination* of the Ethics of Technology may reward individuals by helping them to feel more prepared when they find themselves required to make decisions or take actions with significant ethical implications.

Textbook Definitions – Defining Ethics and Related Terminology

In order to create a baseline of terminology that will be used throughout the rest of the text, this section now provides a collection of terms along with definitions to be used as some of the basic 'textbook definitions' for continuing conversations. These definitions are ***not*** to be considered absolute! In fact, it will be important for you to ask yourself *if* you agree with the definition as presented or, *if not*, what aspects do you think may need clarification. Also, in future chapters, the additional terms will be listed at the *end* of the chapter vs. here, in the middle of the chapter.

- **Ethics** – The systematized principles and standards of right and wrong behavior, typically established and endorsed by a community or society.
- **Morals** – Personal beliefs and internalized values about what is right and wrong, guiding individual behavior.
- **Virtues** – Positive character traits or qualities, such as honesty or courage, that are considered morally good and enable individuals to act in alignment with ethical principles.

- **Vices** – Negative character traits or habits, such as dishonesty or greed, that are considered morally bad and detract from ethical behavior.
- **Beliefs** – Convictions or accepted ideas that shape an individual's morals, virtues, and worldview.
- **Right** – Actions or behaviors that are considered morally or ethically acceptable or good.
- **Wrong** – Actions or behaviors that are considered morally or ethically unacceptable or bad.
- **Education** – The process of acquiring knowledge, skills, values, and attitudes, often shaping ethical understanding and personal development.
- **Traditions** – Long-standing customs or practices passed down within a culture or community, influencing values and behavior.
- **Life Experiences** – Personal events and interactions that shape one's perspectives, beliefs, and ethical outlook.
- **Culture** – The shared values, norms, practices, and artifacts of a group that influence behavior and ethical perspectives.
- **Religion** – Organized systems of beliefs and practices related to the sacred or divine, often providing ethical guidance.
- **Gender** – Socially constructed roles, behaviors, and identities associated with being male, female, or non-binary, influencing experiences and perspectives.
- **Age** – The length of time a person has lived, often affecting their perspectives and ethical viewpoints.
- **Personal Lenses** – The unique set of experiences, values, and perspectives that shape your own current ethical viewpoints.
- **Critical Thinking –** The disciplined process of actively analyzing, evaluating, and synthesizing information to form reasoned judgments and make well-informed decisions.
- **Semantics** – The branch of linguistics that studies the meaning of words, phrases, and sentences, examining how meaning arises from language structure, word choice, and context to convey and interpret information.
- **Individual** – A single person, distinct from a group, with unique experiences and perspectives.
- **Group** – A collection of individuals who interact and share common characteristics, goals, or interests.
- **Group Member** – An individual who belongs to and participates in a group.

- **Integrity** – The quality of being honest and having strong moral principles, consistently acting in accordance with ethical standards.
- **Law** – A system of rules established by a governing authority to regulate behavior within a society.
- **Legal** – Actions or behaviors that are permitted or recognized by law.
- **Illegal** – Actions or behaviors that are forbidden by law.
- **Moral** – Conforming to principles or standards of right conduct; virtuous.
- **Amoral** – Lacking a sense of morality or indifference to right and wrong.
- **Ethical** – In accordance with accepted principles of right and wrong, especially within a professional or societal context.
- **Unethical** – Contrary to accepted standards of right and wrong.
- **Misconduct** – Improper, unethical, or illegal behavior.
- **Lying** – Knowingly making a false statement with the intent to deceive.
- **Cheating** – Acting dishonestly or unfairly to gain an advantage.
- **Stealing** – Taking something that does not belong to you without permission or legal right.
- **Abusive Behavior** – Actions that cause harm, mistreatment, or suffering to others.
- **Discrimination** – Unjust or prejudicial treatment of individuals or groups based on characteristics such as race, gender, age, or religion.
- **Hazardous** – Posing a risk of harm or danger.
- **Conflict of Interest** – A situation in which a person's personal interests could improperly influence their professional decisions or actions.
- **Falsifying Information** – Deliberately altering, inventing, or misrepresenting information with the intent to deceive.
- **Honesty** – The quality of being truthful, transparent, and free from deceit.
- **Fairness** – Treating people equally and justly, without favoritism or discrimination.
- **Responsibility** – The obligation to act correctly and be accountable for one's actions.
- **Duty** – A moral or legal obligation to perform or refrain from certain actions.

- **Obligation** – A requirement to act in a particular way, often arising from law, contract, or moral principle.
- **Stakeholder** – Any individual or group affected by or having an interest in the actions and decisions of an organization.
- **Shareholder** – An individual or entity that owns shares in a corporation and has a financial interest in its performance.
- **Consumers** – Individuals or groups who purchase and use goods or services.
- **Customers** – People or organizations that buy goods or services from a business.
- **Employers** – Individuals or organizations that hire and pay people to work for them.
- **Suppliers** – Entities that provide goods or services to other organizations.
- **Community** – A group of people living in the same area or sharing common interests, values, or goals.
- **Environment** – The natural world, including air, water, land, and ecosystems, affected by human activity.
- **Corporation** – A legal entity that is separate from its owners, with its own rights and responsibilities.
- **Corporate Social Responsibility** – A business model in which companies integrate social and environmental concerns into their operations and interactions with stakeholders.
- **Sustainability** – Meeting present and continuing needs without compromising the ability of future generations to meet their own needs, especially regarding environmental stewardship.
- **Consistency** – Acting in the same way over time, maintaining coherence in values, principles, and behavior.
- **Goodwill** – A positive reputation or relationship built through ethical actions and trustworthiness.
- **Protection** – The act of keeping people, property, or the environment safe from harm.
- **Favorable** – Producing or indicating a positive outcome or approval.
- **Unfavorable** – Producing or indicating a negative outcome or disapproval.
- **Diversity** – The presence of a wide range of different characteristics, backgrounds, and perspectives within a group or organization.
- **Respect** – Recognition and regard for the rights, feelings, and dignity of others.

- **Principles** – Fundamental truths or rules that guide behavior and decision-making.
- **Standards** – Established benchmarks or criteria used to measure and guide conduct or performance.
- **Reward** – Something given in recognition of service, effort, or achievement.
- **Punishment** – A penalty imposed for wrongdoing or violation of rules.
- **Profit** – The financial gain obtained when revenue exceeds expenses.
- **Loss** – The negative financial result when expenses exceed revenue.
- **Empowered** – Having the authority, confidence, or power to make decisions and take action.
- **Disenfranchised** – Deprived of rights, power, or access, especially to participate in decision-making.
- **Code of Ethics** – A formal set of guidelines and principles designed to help professionals conduct business honestly and with integrity.
- **Leading by Example** – Demonstrating desired behaviors and standards through one's own actions, serving as a model for others.

As new content is introduced, additional terms will be collected and presented at the end of each chapter to facilitate future discussions using those same terms. If you feel strongly that your own personal definition of any particular term varies significantly from these 'textbook definitions', you should always discuss these differences with the rest of the individuals in your discussion group to determine how these differences may or may not affect the ongoing conversations. It is important to not simply dismiss these differences as minor differences in semantics when, in fact, these differences *may* represent the root cause of major differences in perspectives.

As you can see, in order to fully examine a concept like *Ethics in Technology*, a large part of the preparatory work involved is making sure that we each have a shared, common baseline from which to begin our work together. This includes coming to a shared agreement on a large number of terms that may effect the conversations. Here are just a *few* examples of terms that will need to be defined in upcoming chapters as part of their exploration:

intention, manipulation, transparency, true vs. false, excess, greed, bias, preferential treatment, conflict of interest, bribery vs. gift, fraud, whistle-blowing, negligence, reasonable person, adult, child, assault, threat, harm, freedom of speech, hate speech, censorship, obscenities, rights, privileges, national security, responsibility, liability, expectation of privacy, safety, liberty, risk, customer lock-in,

profit, loss, capitalism, socialism, communism, feudalism, representation, health and welfare, marketing, stalking, exploitation, employee rights vs. employer rights, … so many more…

Not to mention all of the technology-related terms we will explore in future chapters such as:

automation, robotics, artificial intelligence (AI), big data, natural language processing (NLP), machine learning, telecommunications, vulnerabilities, spam, phishing, virtual private networks (VPNs), biometrics, passwords, personally-identifiable information (PII), firewalls, prevention, surveillance, remote monitoring, doxing, sexting, copyright, trademark, intellectual property, trade secret, cybersquatting, industrial espionage, quality assurance, telemedicine, 3D printing, 3D bio-printing, planned obsolescence, chatbots, digital assistants, product liability, breaches, electronic medical records (EMR), cyberstalking, cyberbullying, sexual predators, revenge porn, … and so many more of these as well!

Ethical vs. Legal

Using the definitions of *Ethical*, *Unethical*, *Legal,* and *Illegal,* as defined above, consider this matrix:

Ethical vs. Legal Matrix

Ethical ↓ vs. Legal →	Something that is LEGAL	Something that is ILLEGAL
Something that is ETHICAL	Legal & Ethical	Illegal But Ethical
Something that is UNETHICAL	Legal But Unethical	Illegal & Unethical

Figure 6: Ethical vs. Legal Matrix

Several concepts that tend to be regularly (but incorrectly) confounded during discussions, are the concepts of something being either Ethical or Unethical, as well as that same thing being either Legal or Illegal. Ethics and Legalities are *two different concepts.* As you can see by the matrix above, a single item or situation can exist in any single one of the white cells.

In other words, something can be both Ethical as well as Legal – which many individuals think is the ideal situation. But our shared reality has shown us that the ideal situation isn't always what we experience. Rather, you may discover that another thing may be completely Legal, while simultaneously being completely Unethical. It many societies, one can simply examine the current or historic laws or codes of conduct and they will inevitably be able to discover numerous instances of

laws that, at the time, were considered *Legal,* however they can simultaneously be considered completely *Unethical* if not abhorrent.

Likewise, there can be many situations where something is completely Ethical, but may be simultaneously Illegal! And finally, something could be completely Unethical and also completely Illegal. We all have probably seen these kinds of situations as these often end up as the *Breaking New* stories because of their often significant *shock factor*!

Take a few minutes now and see if you can come up with several instances of situations for each of those four possible matrix cells. Then, ask yourself how you would be able to present, to someone else, your reasoning for placing each individual situation into its own respective cell. Understanding the 'WHY' that you have used to come to your conclusions is a major aspect of applied critical thinking skills.

Critical Thinking and Limiting Biases

Thinking now about the terms that have been presented in this chapter, what happens when one or more of our **personal lenses** illuminates a conflict when accepting the definition of a particular term? What happens when an education lens defines a concept one way and that definition is in conflict with a definition previously constructed through a religious lens? What about when a definition changes when viewed through a gender lens vs. using a cultural lens? How about when your family lens defines something one way, but your work community defines that same thing a different way? Do you know how to first identify whenever there is a conflict in definitions? Do you then know how to isolate the differences so that points of agreement and points of disagreement can be fully fleshed out?

The ability to review your own perspectives from an *objective point of view* is a very large part of applying the concept called **Critical Thinking**. This activity can help you to become well-prepared to have in-depth, meaningful discussions about the underlying ethics of any given topic. This helps you be able to see things more clearly through your own personal lenses as well as helps you be able to more closely understand how others see the same concept through their own personal lenses.

In the previous section, you were asked to think of several situations that might be appropriately placed into each of the four white cells in the *Ethical vs. Legal Matrix* above. Re-consider those issues or situations once again, but this time, review each instance or situation while *intentionally* looking through your multiple personal lenses. Can you identify which lens or lenses most significantly influence your decisions as you categorized where each situation should end up? Do the lenses that you use weigh more heavily with one lens vs. the others? What if someone else's lenses would put the same situation into a different cell? Are you prepared to have an *objective* conversation with that person to delve down to discover the root differences?

The more you can *practice* these skills of self-reflection, the greater your capacity will become to truly understand yourself as well as your ability to empathize with those who may be viewing situations through other personal lenses or through lenses with different weights than your own. This effort pays for itself through greater shared understandings and, hopefully, with greater positive ethical decisions.

4. Ethics for Tech Developers and Tech Consumers

Tech Consumer Responsibilities; Professional Codes; and Everyday Decision-Making

Tech Consumer Responsibilities

Considering the typical audience for this textbook, nearly 100% of you would most likely consider yourselves to be *consumers of tech*. Take a few moments to think about all of the tech that you regularly use as a part of your day-to-day experiences. From checking your smartphone for messages and social media updates, to using laptops or tablets for school or work assignments, streaming music and videos, playing video games, and even relying on smartwatches or fitness trackers to monitor your health – technology is woven into nearly every aspect of your daily routine. Whether you're ordering food through an app, catching up on news, attending virtual classes, or collaborating on group projects using cloud-based tools, it's clear that tech plays a central role in how you learn, work, connect, and entertain yourselves.

What would be some of the ethical considerations for *consumers of tech*? As a starting point for this discussion, I posed this exact question to a generative-AI tool (Perplexity) to see the response. Here is what Perplexity had to say:

> "Some key ethical considerations for consumers of tech include protecting personal privacy and data, being aware of how their information is collected and used, ensuring informed consent when using digital services, recognizing and avoiding technologies or companies that engage in discriminatory or unfair practices, respecting intellectual property, and considering the broader social and environmental impacts of their tech use. Consumers should also be mindful of the potential for technology to amplify bias or harm vulnerable groups, and strive to make choices that support transparency, fairness, and accountability in the tech industry."

Interesting indeed!

Let's look at each of these concepts and turn them each into questions for you to review through your own personal lenses:

- protecting personal privacy and data – Is your personal privacy and data actually protected? Do you know where (all) this data exists and who (all) has access to it? Does it really need to be kept private and protected?
- being aware of how their information is collected and used – Do you have any control (or say) over what is collected or how it might be used (or shared, or sold)? Does it matter?

- informed consent when using digital services – Have you willingly and knowingly given away your information? How about your rights? Can you change your mind? If you do change your mind, is it already too late? Do you have any recourse?
- recognizing and avoiding technologies or companies that engage in discriminatory or unfair practices – Do you ever investigate the provider(s) of the tech you consume and does that information affect your decision to work with (and consequently support and enable) those companies? Do you have any responsibility to *not* support and enable unethical companies?
- respecting intellectual property – Do things like pirating games, software, or music have ethical implications? Does it matter if we're talking about an artist's intellectual property or a company's intellectual property? What about your colleagues' work? If they didn't 'legally' protect it, is it fair-game?
- considering the broader social and environmental impacts – Does it matter that buying the newest version of a phone will mean that the 'old' phone may become e-waste with long-term global environmental harm? Does it matter when trash-talking someone in a gaming app if we are completely unaware of their own propensity toward self-harm? Do you have any responsibility and/or culpability in the outcomes that derive from your own actions with tech?
- technology amplifying bias or harming vulnerable groups – Am I using platforms or tools that have been shown to perpetuate or amplify biases, such as facial recognition systems with higher error rates for people with darker skin tones or recommendation algorithms that reinforce stereotypes or exclude certain groups? How might my engagement with algorithm-driven content – such as clicking, sharing, or purchasing – contribute to feedback loops that reinforce existing biases or marginalize underrepresented communities?

As technology becomes ever more integrated into daily life, intentionally reflecting on how we interact with it is essential for fostering a more ethical and responsible digital world. By asking ourselves thoughtful questions about privacy, consent, fairness, and the broader impacts of our choices, we can move beyond passive consumption and become conscious participants in shaping the tech landscape. This means not only protecting our own interests but also considering the well-being of others and the environment, holding companies accountable, and striving for transparency and inclusivity in all our digital interactions. Through ongoing awareness and deliberate action, each of us can contribute to a culture where technology empowers rather than exploits, and where ethical considerations guide both innovation and everyday use.

Professional Codes

Now, for some of you, technology isn't going to be something you simply consume. Rather, some of you may be heading down a path toward becoming a technology practitioner. As a technology practitioner, all of the previously discussed ethical responsibilities of a tech consumer exist – first and foremost – but there are also additional ethical factors that will be found in addition to those basic considerations.

Some common tech-related job titles include the following:

• Software Engineer	• AR/VR Developer	• Data Scientist
• Systems Administrator	• Network Architect	• Cloud Architect
• Cybersecurity Analyst	• Business Systems Analyst	• IT Support Specialist
• UI/UX Designer	• DevOps Manager	• AI Computer Scientist

Think of all of the people that you will have an ethical relationship with as a part of your technology-based profession. This diagram represents some of the main relationships you will experience in your IT careers.

Figure 7: IT Professionals' Ethical Relationships

In your tech-related path, you will find yourself working with very many different individuals who may have many different expectations as to how you will apply ethics in your day-to-day interactions. Think about all of the different people shown here and remember that each person has their own set of personal lenses which they are using (whether intentionally or subconsciously) during each interaction with you.

Often, the details of these relationships may be spelled out (at least partially) via various relationship agreements. These agreements can take many forms (i.e. contracts, non-disclosure agreements, license agreements, professional codes of conduct, etc.) with many of these forms having both ethical and legal ramifications.

But at other times, the details of the relationships are not spelled out *at all*! And, as a result, conflicts can certainly arise when it becomes evident that there are competing interests being considered and viewed through conflicting personal lenses.

A great starting point for considering the additional ethical responsibilities of a tech practitioner is to review the Association for Computing Machinery (ACM) Code of Ethics and Professional Conduct. This document attempts to codify the ethical responsibilities of tech professionals. But with even a cursory review of this professional code, one can easily discover how conflicts can arise when different constituents prioritize their own agendas related to tech development.

Let's consider the following case study:

Case Study: Apple Settles 'Batterygate' Class Action Suit with an additional $113 Million[1]

> In November of 2020, Apple agreed to pay $113 million to settle consumer fraud lawsuits. These lawsuits were brought by more than 30 states over alleging that Apple was *intentionally and without notice* slowing down and shutting off iPhones resulting in the devices having sluggish performance or completely shutting down.
>
> At first, Apple *denied* that it purposefully impeded the devices' performance in any way. Later, Apple admitted that it *did, in fact,* alter the devices' performance but it was for the purpose to "…preserve battery life amid widespread reports of iPhones unexpectedly turning off."
>
> "Many consumers decided that the only way to get improved performance was to purchase a newer-model iPhone from Apple," Arizona Attorney General Mark Brnovich wrote in the complaint. "Apple, of course, fully understood such effects on sales."
>
> The slowdown effected phones that were released between 2014 and 2016, but it wasn't until December of 2017 that Apple eventually admitted to the slowdowns. Then, they issued an *apology of sorts* by saying, "We have never – and would never – do anything to intentionally shorten the life of any Apple product, or degrade the user experience to drive customer upgrades." But they settled anyway! Initially, they agreed to a settlement of $500 Million to pay affected consumers $25 per phone. The $113 Million was in addition to the initial $500 Million.

To think about this case in more detail, let's put ourselves in different shoes and examine this situation from different perspectives with differing lenses.

1 "Apple Agrees To Pay $113 Million To Settle 'Batterygate' Case Over iPhone Slowdowns", NPR, updated Nov. 18, 2020, https://www.npr.org/2020/11/18/936268845/apple-agrees-to-pay-113-million-to-settle-batterygate-case-over-iphone-slowdowns

Person 1: Apple Executive – We've sold and shipped millions of units of phones from 2014 through 2016 – and they are *excellent products*! Maybe *too good*. But that was then. How will we continue to get new sales if our older products are still working just fine? Why should our customers throw away perfectly good and working devices if they are still working for them? If we don't continue to have the same (or better) sales growth, my position (and my bonuses) will be at risk. And if the new features of our new devices aren't *so appealing* that the consumers won't willingly abandon their working tech, then we need to make the older devices less-than-desirable if we will have any chance of getting those new replacement sales. But we also can't disclose what we're doing because we can't risk our competitors seeing our strategies. Let's just find a way to make the old phones 'go away'. (planned obsolescence, trade secrets, intellectual property)

Person 2: Apple Customer – I just spent hundreds of dollars on a device less than 5 years ago and it did *everything I needed it to do.* And for several years now, it has been a *great device!* But now, for no apparent reason, my regular apps have become unmanageably sluggish and, sometimes, without warning, my phone will just shut itself off. Apple said that it didn't do anything, but *I* certainly didn't change anything! The device *was* working perfectly, and then all of a sudden, it is no longer functioning the way it should. Isn't it reasonable to have an expectation that something that is working will continue to work as designed without interruption or performance degradation? Also, when I ask Apple about what's going on, shouldn't they have a responsibility to tell me the truth right up front? And if this device no longer works for me, then it won't work for anyone. Where will this device end up? In a landfill I suppose… oh, the waste! (corporate responsibility, transparency, environmental responsibility)

Person 3: YOU – as any one of a number of different technology professionals working at Apple.

Developer – The boss just asked me to start working on a program that would run constantly – undetectable and behind-the-scenes – that would basically do nothing but would consume a lot of clock cycles of the processor. The purpose of this program is simply to intentionally drain the battery as quickly as possible. I'm no dummy. I know *exactly* why I am being asked to do this. If I didn't work here at Apple, and I wrote something like this, I would be considered a cyberterrorist. Am I really OK with being a part of 'planned obsolescence'? Is this why I went to school to learn how to be an app developer? Is this the kind of app I thought I'd be developing? Is this really what I signed up for?

Marketing – The boss just asked me to develop a campaign targeting existing phone users telling them how much they are missing out because their older devices just can't keep up with the new apps. I'm supposed to focus on new apps that only run on the newest devices. We've already seen that the 'new apps' aren't that big of a hit because we aren't getting a lot of 'new' customers at this time anyway. It doesn't seem to be true that the new

apps are all that they're supposed to be. When does 'exaggeration' become 'lying'? Is this really what I signed up for?

Customer Service – The boss just told us that we are experiencing a huge increase in disgruntled customers because their batteries keep draining very quickly and some phones are just shutting off. The boss told me, "Your response is that the customer is just using technology that is too old and they should upgrade to a newer phone right away" and then I should try to transfer them to Sales. I asked the boss, "What changed? Why have the devices suddenly started failing?" The boss said, 'That's above our pay-grade.' and left me on my own. Something doesn't seem right here. If *I* were the customer, I would expect more of a concrete answer. And I certainly wouldn't appreciate a 'hard sales pitch' if the reason I called in was to get my current device restored to the way it was working fine just a bit ago. And why can't my own company be transparent about what is going on? Is this really what I signed up for?

Sales Person – The boss just told me that we will begin using two different sales pitches for our potential customers. First, we have to find out if they are a 'new' customer (without one of our previous models.) If so, then we are supposed to first pitch our great Apple brand (be one of the cool kids), and then next we should pitch the differences between our brand and the other brands, and then, finally, we should close with the pitch that the new phones are positioned to handle *any new technology advancements* that may come in the future. But if the prospect is an 'old' customer, then the pitch needs to be just 'sad commiseration'. They will be grousing about how they thought their old phone should have lasted a lot longer and how they always took great care with it… I am supposed to just sadly nod my head and say, "yeah – the tech just keeps changing… it's getting hard to keep up… but what are you gonna' do? You need the latest tech to be able to do all of the things you've gotten used to doing." But then the boss says I should also use the pitch that the new phones are positioned to handle *any new technology advancements* that may come in the future. Are you kidding me? How am I supposed to do that with a straight face? Isn't the reality that this investment is *designed* to fail in less than 3 – 5 years? Is this really what I signed up for?

When looking at this exact same situation through the different perspectives of different involved people, we can see that there are quite a number of ethical considerations that should not be too easily dismissed. One of the most common conflicts when it comes to the ethics associated with business and technology involves the distinctions and differentiations between two different groups of people: **stockholders** vs. **stakeholders**.

Stockholders (or shareholders) are individuals, companies, or institutions that own shares in a corporation, giving them partial ownership and certain rights such as voting on major company decisions and receiving dividends when profits are distributed. Their *primary* interest lies in the *financial performance* of the company, as their returns depend on stock value and dividend payouts, and they can typically buy or sell their shares at will.

In contrast, stakeholders encompass a much broader group, including not only shareholders but also employees, customers, suppliers, and members of the local community, all of whom have an interest in the company's performance and impact, even if they do not own any shares. While stockholders are mainly concerned with financial returns, stakeholders may prioritize long-term stability, ethical practices, job security, product quality, and the company's social and environmental responsibilities.

This means that stakeholders' interests may not always align with those of stockholders. It has been this author's experience that the vast majority of corporate boards and executive leadership prioritize stockholder interests over stakeholder interests.

So, where does this leave us when we consider how a Professional Code of Conduct can help us in making our ethical decisions? First, this can be something that one can intentionally look for when interviewing for a position with a potential employer. individuals can find out if the organization has adopted the ACM Code of Ethics and Professional Conduct. Or perhaps they have their own code of conduct that they have developed.

individuals can also discover the policies and procedures that the organization uses for dealing with conflicts that arise from competing priorities. Some organizations utilize internal and/or external mediation boards to help provide unbiased, objective reviews and conflict resolutions.

Additionally, individuals can adopt their own code of ethics and professional conduct to be a guide for their own, personal decisions. But in order to do this, one should also proactively consider what they may do when they are asked to do something that violates their adopted code of ethics.

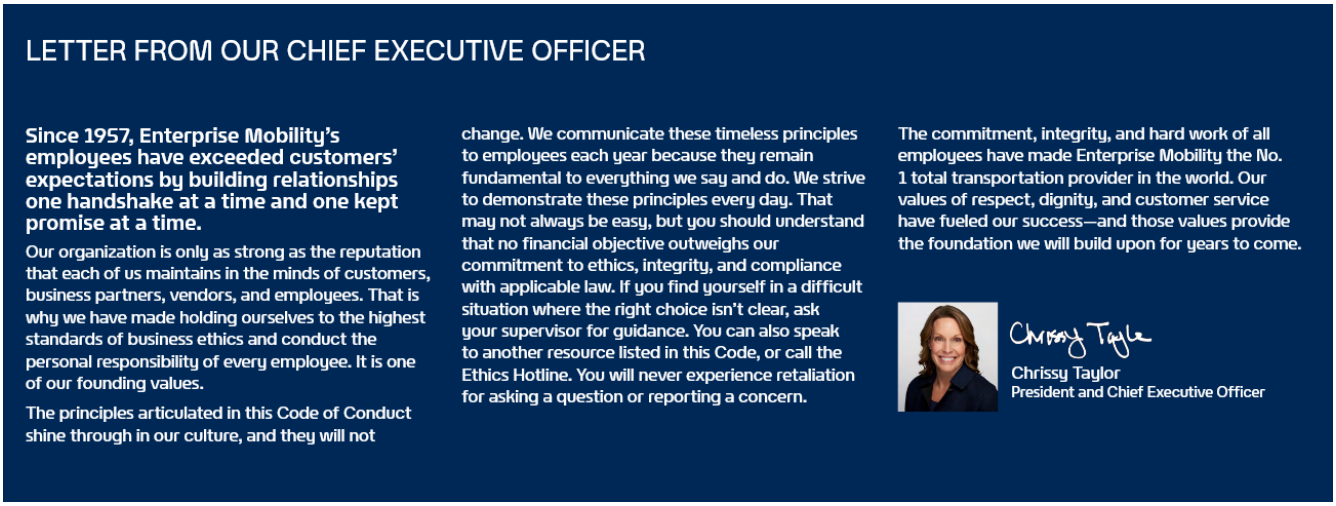
A look at one company's Code of Conduct

The company Enterprise Mobility (formerly Enterprise Holdings) is a 68-year-old company that includes several brands – such as Enterprise Rent-A-Car, National Car Rental and Alamo – and provides services such as fleet management, car-sharing, van-pooling, truck rental, luxury rental, retail car sales and vehicle subscription. Enterprise currently has a global fleet of more than 2.3 million vehicles with rental locations in more than 90 countries and territories, including more than 40 countries across Europe.

In a strong example of corporate responsibility, transparency, and commitment to a professional code of conduct, Enterprise publishes their Code of Conduct here:

https://www.enterprisemobility.com/content/dam/enterpriseholdings/marketing/about-us/compliance-and-ethics/enterprise-holdings-employee-code-of-conduct.pdf

This comprehensive document defines and discloses precisely what is expected of its employees as well as how its customers and vendors can expect their relationships to exist. The introductory letter from the President and Chief Executive Office (CEO) of Enterprise, Chrissy Taylor, clearly illustrates the 'WHY' that Enterprise has adopted and publicly declared their commitment to this Code of Conduct.



LETTER FROM OUR CHIEF EXECUTIVE OFFICER

Since 1957, Enterprise Mobility's employees have exceeded customers' expectations by building relationships one handshake at a time and one kept promise at a time.

Our organization is only as strong as the reputation that each of us maintains in the minds of customers, business partners, vendors, and employees. That is why we have made holding ourselves to the highest standards of business ethics and conduct the personal responsibility of every employee. It is one of our founding values.

The principles articulated in this Code of Conduct shine through in our culture, and they will not change. We communicate these timeless principles to employees each year because they remain fundamental to everything we say and do. We strive to demonstrate these principles every day. That may not always be easy, but you should understand that no financial objective outweighs our commitment to ethics, integrity, and compliance with applicable law. If you find yourself in a difficult situation where the right choice isn't clear, ask your supervisor for guidance. You can also speak to another resource listed in this Code, or call the Ethics Hotline. You will never experience retaliation for asking a question or reporting a concern.

The commitment, integrity, and hard work of all employees have made Enterprise Mobility the No. 1 total transportation provider in the world. Our values of respect, dignity, and customer service have fueled our success—and those values provide the foundation we will build upon for years to come.

Chrissy Taylor
President and Chief Executive Officer

Figure 8: Enterprise's Code of Conduct Introduction Letter by Chrissy Taylor, President and CEO

Contained within their code of conduct, Enterprise shows that there is a clearly defined path that individuals *can use* (but, more importantly, also have a *responsibility to use*) to report and resolve issues of ethical concern. This path includes one's immediate supervisor, a next-level supervisor, the Human Resources department, or the Compliance and Ethics Committee. They even have an ethics hotline which includes a link for online reporting as well as a toll-free number which are both available and monitored 24 hours a day, 7 days a week, and 365 days a year!

Take a few minutes to review this one company's published Code of Conduct. Just a few of the topics that you will find covered here include concepts that allow us to also introduce additional terms to be further explored:

- **Obligations of Leadership –** leaders are required to 'lead by example' as a requirement of their position.
- **Copyright, trade secret, patent, intellectual property –** creations of the mind that the law defines and protects.

- **Conflicts of Interest –** occurs when one's personal interests interfere with their ability to make unbiased decisions on behalf of the organization.
- **Gift** – Something of value given willingly to another person without any expectation of return or influence.
- **Bribe** – Something of value offered or given with the intent to influence the recipient's actions or decisions for the giver's benefit.
- **Insider Trading** – buying or selling of a company's securities by individuals who possess material, nonpublic information about that company, often in violation of a duty to keep that information confidential.
- **Anti-Corruption Laws –** these vary by region/country and can be complex, but these remain part of the *legal* requirement as well as an *ethical* requirement.
- **Harassment –** any unwelcome behavior toward another person relating to a person's legally protected characteristics that have the purpose or effect of creating an intimidating, hostile, or offensive work environment. Such conduct may be physical, sexual, or psychological.

Review the Enterprise Code of Conduct and compare and contrast what you find there with the ACM Code of Ethics and Professional Conduct. Where do you discover similarities? Are there differences? Do you feel that any differences are significant? Which, if any (and in which document), would you suggest should be changed and why? How do these codes of conduct currently match up to your own way of thinking about your own personal ethics?

Everyday Decision-Making

So far in this chapter you have:

- considered your own ethical responsibilities as a *consumer of tech*
- reviewed the generic but widely adopted *ACM Code of Ethics and Professional Conduct*
- reviewed one company's comprehensive and transparent Code of Ethics

It is now time to consider what these might mean for you in your everyday decision-making process. For example, there appear to be some rather valid reason for individuals to consider their own ethical *consumption* of all things tech – for both their own health, safety and well-being – but also for how their actions might impact others. There appear to be some strong starting points and examples of

Ethical Codes of Conduct for both individuals and organizations to use to help define, clarify, and formalize their own approaches to adopting ethics in their own day-to-day actions.

So now, here come the real questions for this chapter:

What does your own, personal Ethical Code of Conduct look like? What are some of the areas that you feel are pretty well defined? What are some areas that you feel may be in conflict – depending on which personal lenses you choose to use? What are some areas of your own personal code of ethics that may be in conflict with your school, or your work, or your family, or your church, or your community, or your culture? Can you imagine writing up your own, personal code of ethics? What all would be included? What do you feel is still too undefined or situational, so much so that it means that you may not have a *consistent* ethical response in certain situations? What are the risks of inconsistently or sporadically adhering to a personal code of ethics? Is it OK to change your ethical position on a particular subject? If so, what circumstances would allow for this?

As promised in the early chapters of this text… we aren't providing any concrete, absolute answers to these questions. But rather, we are hoping that by listing a collection of questions, these may help individuals to discover and implement some *intentionality* into what it means to be an ethical person making informed, ethical decisions in their day-to-day activities.

5. Cybersecurity, Hacking, and Digital Identity

Cybersecurity; Vulnerabilities; Hacking; Digital Identity; Online Reputation

In the previous chapter, we explored some of your own personal ethical responsibilities as they relate to you as a consumer of all things 'tech'. We also, explored some of your ethical responsibilities as they relate to your role in an organization that utilizes 'tech'. Now, for this chapter and each of our subsequent chapters, we will look at various individual aspects of technology and try to focus on the ethical considerations within some narrower contexts. As we will quickly see, however, all of these chapters cannot be completely isolated from each other. Rather, it will be common to discover that there are aspects of each of these subsequent chapters that *significantly overlap* along with other chapters.

Cybersecurity

To begin this discussion, once again, let's use a generative-AI tool (Perplexity) to help us provide the 'textbook definition' of *cybersecurity.* Here is the prompt that was used:

> "In a single sentence, please define the term 'Cybersecurity'."

Here are the results we received:

Cybersecurity – The art and practice of protecting networks, devices, programs, and data from unauthorized access, cyberattacks, or criminal use, ensuring the confidentiality, integrity, and availability of information.

Figure 9: Graphic representing cybersecurity

It seems that there may be some significant omissions from this definition: We already have a feel for 'Why' cybersecurity is important… But what about the other questions? 'Who' is responsible for effective cybersecurity? 'When' do we need to think about cybersecurity? 'Where' do we need to be cognizant of cybersecurity issues? And 'How' do we actually address cybersecurity concerns?

So, here is a follow-up prompt for our friend Perplexity:

> "This definition answers the question of 'what' is Cybersecurity. Assuming that we already know the 'why' associated with a need for cybersecurity, in a single sentence each, what would be the answers to the questions 'when', 'where', 'how', and most importantly, 'who' that should be associated with the concept of effective cybersecurity?"

Here are the additional results:

> **When**: Effective cybersecurity must be practiced continuously, adapting to evolving threats and technological changes, and is especially critical whenever digital systems, networks, or sensitive data are in use.
>
> **Where**: Cybersecurity is required wherever digital assets exist, including on-premises networks, cloud environments, remote work setups, mobile devices, and any location where information is stored, processed, or transmitted.
>
> **How**: Effective cybersecurity is achieved through a combination of risk assessments, robust security policies, technical controls like encryption and multi-factor authentication, continuous monitoring, regular training, and incident response planning.
>
> **Who**: Everyone with access to digital systems – including individuals, employees, IT professionals, organizational leaders, and specialized cybersecurity teams – shares responsibility for maintaining effective cybersecurity, with organizations often relying on dedicated experts, external consultants, and collaborative initiatives like cybersecurity clinics to strengthen their defenses.

The generative AI seems to get this one nearly 100% right! (When we look into the AI systems themselves in greater detail in Chapter 11, we will see this is ***not*** always the case!) *Everyone* is responsible – in part at least – for effective cybersecurity. The following sub-topics of this chapter will explore just a few of the concepts related to cybersecurity where a deeper dive into the corresponding ethics can illustrate some interesting and maybe even unexpected challenges!

Vulnerabilities

Vulnerabilities in digital systems represent weaknesses or flaws that can be exploited by malicious actors to gain unauthorized access, disrupt operations, or compromise sensitive information. These vulnerabilities may be targeted through various forms of **cybercrime**, such as **phishing**, **ransomware**, or **distributed denial-of-service (DDoS)** attacks, often leveraging exploits that take advantage of unpatched software or misconfigured systems.

Ethically speaking, addressing vulnerabilities requires timely identification and remediation – typically through "fixes" or patches – to prevent harm to individuals and organizations. Without proper prevention and remediation, threats like **viruses, Trojan horses, botnets**, **logic bombs**, or **blended threats** that can propagate across interconnected networks. The presence of sophisticated threats, such as **rootkits** or phishing campaigns (including **spear phishing**, **smishing**, and **vishing**, etc.), underscores the ongoing responsibility of cybersecurity professionals *and* tech users alike to remain vigilant, promote best practices, and uphold principles of fairness, accountability, and non-maleficence in protecting digital assets and identities.

Hacking

Hacking, in its broadest sense, refers to the act of gaining unauthorized access to computer systems or networks, but the motivations and ethical implications of hacking can vary widely depending on the individuals involved. **Black-hat hackers**, for example, engage in hacking for malicious purposes such as stealing data, causing disruption, or committing cybercrime, often motivated by personal gain or the intent to inflict harm. In contrast, **white-hat hackers** use their technical skills to identify and report vulnerabilities, helping organizations strengthen their security by acting as ethical defenders – sometimes as part of formal roles like **penetration testers** or through coordinated vulnerability disclosure programs like **hack-a-thons**.

The landscape of hacking also includes figures such as **crackers**, who break into systems to bypass protections or copy software illegally, and **hacktivists**, who use hacking as a form of protest or to promote social or political causes. The actions of hacktivists can raise complex ethical questions, as their activities may be intended to expose injustice or raise awareness, yet still involve unauthorized access and potential harm to innocent parties. As technology evolves, so too do the methods and motivations of hackers, making it essential for society to continually reassess the ethical boundaries of hacking, the responsibilities of those with advanced technical knowledge, and the appropriate legal and organizational responses to both harmful and beneficial forms of hacking.

Digital Identity

Digital identity, as it relates to an individual, is the collection of digitally or electronically captured attributes, behaviors, **credentials**, and data points that uniquely verify and represent a person online. This identity is not static; it is dynamically shaped by both the information individuals *actively* provide – such as usernames, email addresses, social media profiles, and **biometric** data – as well as the data *passively* collected through their online activities, including browsing habits, search histories, and transaction records. Key aspects that make up a person's digital identity include **personally identifiable information (PII)** like social security numbers, dates of birth, and biometric traits; login

credentials; device identifiers; behavioral patterns; and contextual signals such as location and device usage.

Bad actors often seek to access and exploit digital identities through methods like phishing, **credential theft**, or **malware**, using the compromised information for identity theft, financial fraud, or unauthorized access to sensitive accounts. Once a digital identity is breached, attackers can leverage it to impersonate individuals, commit cybercrime, or even build more convincing attacks against others by harvesting further data from compromised accounts. Ethically, individuals have a responsibility to be intentional and mindful about the information they share and the **digital footprint** they create, as their digital identity not only reflects on their personal reputation but also affects their privacy and security. Practicing thoughtful self-representation and safeguarding personal data are essential not just for personal protection but also for fostering a trustworthy and respectful digital environment.

Online Reputation

This leads us to our final concept for this chapter – one's online reputation. Online reputation refers to the collective perception and judgment that others form about an individual based on their digital presence, including the content they create, share, and are associated with across various online platforms. Unlike digital identity, which is the sum of all information that identifies a person online, online reputation is shaped not only by one's own actions but also by what *others* post, comment, or tag about them, and is visible to third parties through search engines, forums, blogs, and especially social media. Social media usage plays a significant role in building or damaging online reputation, as posts, comments, likes, and shares contribute to the overall digital footprint, and even a single viral incident can have lasting effects – positive or negative – on how a person is viewed by peers, employers, and the broader public.

Also, in today's society, there is often an ongoing blending of work and personal life which appears to be mostly unavoidable. At work, you may use the corporate computer to prepare for some personal meetings such as with your doctor, etc. Additionally, some organizations have **bring-your-own-device (BYOD)** requirements and/or policies which stipulate if and how you will use your own devices in the work setting. These kinds of intersections between what is 'personal' vs. what is 'public' introduces unique risks to one's online reputation. When individuals commingle work and home information on shared devices, they increase the chances of accidental data leaks, inappropriate content exposure, or breaches that could affect both professional and personal reputations. For example, a security lapse on a personal device used for work could expose sensitive corporate information or inadvertently link personal social media activity with professional contacts, complicating the separation between private and public personas.

Virtual Private Networks (VPNs) are often used to enhance privacy by encrypting internet traffic and masking a user's IP address. However, using a VPN – especially one provided by a third party –

does not guarantee true anonymity or untraceability. While a VPN can obscure activity from local networks or **Internet Service Providers (ISPs)**, the VPN provider itself can potentially (and usually does!) *log* user activity. They do this because if the tech fails for any reason, it is only through reviewing the logs that the provider can discover and remedy the failure! As a result of this known logging, both law enforcement as well as sophisticated attackers may still trace actions back to the individual if the VPN is compromised or if endpoints are not secure. Direct-to-endpoint VPNs (such as those connecting directly to a corporate network) offer more control but still do not provide absolute anonymity, highlighting the need for individuals to remain vigilant and intentional about their online actions and the security tools they use.

Ultimately, maintaining a positive online reputation requires individuals to be mindful of their digital footprint and the potential consequences of their online behavior. Ethical self-management involves regularly reviewing privacy settings, thinking critically before posting or sharing information, and understanding that online actions can have far-reaching effects on credibility, trustworthiness, and future opportunities.

Textbook Definitions – Cybersecurity

- **cybercrime** – Illegal activities conducted using computers or networks, including theft, fraud, or disruption of services.
- **phishing** – A deceptive technique where attackers impersonate legitimate entities to trick individuals into revealing sensitive information, such as passwords or financial details.
- **ransomware** – Malicious software that encrypts a victim's data and demands payment for its release.
- **distributed denial-of-service (DDoS)** – An attack in which multiple compromised systems flood a target with traffic, overwhelming it and rendering services unavailable to legitimate users.
- **viruses** – Malicious programs that attach themselves to legitimate files or programs and replicate, spreading to other systems and causing harm.
- **Trojan horse** – Malicious software disguised as legitimate applications, which, when executed, enable unauthorized access or cause damage.
- **botnets** – Networks of compromised computers, controlled remotely by attackers, used to perform coordinated malicious activities such as DDoS attacks or spam distribution.
- **logic bombs** – Malicious code embedded in software that triggers a harmful action when specific conditions are met.

- **blended threats** – Attacks that combine multiple types of malware or attack methods to exploit different vulnerabilities simultaneously.
- **rootkits** – Malicious tools designed to hide the existence of certain processes or programs, allowing continued privileged access to a system.
- **spear phishing** – Targeted phishing attacks aimed at specific individuals or organizations, often using personalized information to increase credibility.
- **smishing** – Phishing attacks delivered via SMS text messages, aiming to trick recipients into divulging sensitive information.
- **vishing** – Voice-based phishing attacks conducted over the phone to deceive individuals into providing confidential information.
- **black-hat hackers** – Individuals who exploit vulnerabilities in systems for malicious purposes, personal gain, or to cause harm.
- **white-hat hackers** – Ethical hackers who identify and help fix security vulnerabilities to improve system security, often with permission.
- **penetration testers** – Security professionals who simulate cyberattacks on systems or networks to identify and address vulnerabilities before malicious actors can exploit them.
- **hack-a-thons** – Collaborative events where programmers and security experts work intensively to solve problems, develop software, or test security in a short period.
- **crackers** – Individuals who break into computer systems or software, often to bypass protections or copy software illegally.
- **hacktivists** – Hackers who use their skills to promote social or political causes, often through unauthorized digital actions.
- **credentials** – Usernames, passwords, or other authentication information used to verify identity and gain access to systems.
- **biometrics** – Unique physical or behavioral characteristics, such as fingerprints or facial recognition, used for automated identity verification.
- **personally identifiable information (PII)** – Data that can be used to uniquely identify an individual, such as name, address, social security number, or date of birth.
- **credential theft** – The act of stealing authentication information, such as usernames and passwords, to gain unauthorized access to systems or data.

- **malware** – Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems or networks.
- **digital footprint** – The trail of data and activity a person leaves behind when using digital services, including social media posts, browsing history, and online transactions.
- **bring-your-own-device (BYOD)** – A policy or practice where employees use their personal devices for work purposes, often increasing security and privacy risks.
- **Virtual Private Networks (VPNs)** – Services that encrypt internet traffic and route it through a secure server, providing privacy and security for online activities.
- **Internet Service Providers (ISPs)** – Companies that provide individuals and organizations with access to the internet.

6. Technology, Justice, and Social Equity

Tech in Education; Healthcare Access and Tech; Tech for Accessibility and Inclusion; Maslow's Hierarchy of Needs and Tech; Digital Divide;

Tech in Education

The integration of technology in education has transformed how students learn, educators teach, and institutions deliver knowledge. From digital textbooks and online learning platforms to adaptive learning software and virtual classrooms, technology can help bridge gaps in access to quality education, particularly for students in remote or underserved areas. However, the ethical considerations are complex: unequal access to devices and reliable internet can reinforce existing educational disparities, and the use of student data for **algorithmic personalization** raises questions about **privacy**, **informed consent**, and potential **bias**.

Educators and policymakers must grapple with the responsibility to ensure that technology enhances learning equitably, rather than exacerbating divides. This involves not only providing hardware and connectivity but also supporting **digital literacy**, offering accessible content for students with disabilities, and critically evaluating the impact of educational technologies on student well-being and **autonomy**. Ultimately, the ethical deployment of technology in education requires ongoing reflection on who benefits, who may be left behind, and how to foster a more just and inclusive learning environment.

Healthcare Access and Tech

Technology has revolutionized healthcare delivery through **telemedicine**, **electronic medical records (EMR)**, **wearable health monitors**, and **AI-driven diagnostics**. These advances can increase access to care for rural populations, streamline patient management, and enable earlier detection of disease. Yet, ethical challenges persist: not all patients have equal access to the internet or smart devices, and the digital skills needed to navigate modern healthcare tools are unevenly distributed.

There is also the risk that algorithmic decision-making in healthcare may reflect or amplify existing biases, leading to disparities in diagnosis or treatment. Protecting **patient privacy** and ensuring **informed consent** are paramount as more sensitive health data is collected and shared across digital platforms. Ethically, healthcare providers and technologists must work to ensure that technological innovation does not widen the gap between those who can and cannot access high-quality care, but instead promotes justice by making healthcare more inclusive, affordable, and responsive to the needs of all communities.

Tech for Accessibility and Inclusion

One of the most promising aspects of technology is its potential to empower individuals with disabilities and promote broader social inclusion. Assistive technologies – such as **screen readers**, **voice recognition** software, and **adaptive hardware** – can enable people with visual, auditory, motor, or cognitive impairments to participate more fully in education, employment, and civic life. The ethical imperative is to design technology that is accessible by default, not as an afterthought, and to involve people with disabilities in the design and evaluation process.

At the same time, barriers remain: not all digital content is accessible, and some emerging technologies (like AI-powered interfaces) may introduce new obstacles if not thoughtfully implemented. Promoting digital inclusion means addressing affordability, usability, and cultural relevance, while also challenging stereotypes and assumptions about disability. Ethically, the goal is to create a digital world where everyone can participate with dignity and autonomy, regardless of ability.

Maslow's Hierarchy of Needs and Tech

Maslow's Hierarchy of Needs provides a useful framework for considering the ethical implications of technology's role in fulfilling human needs.

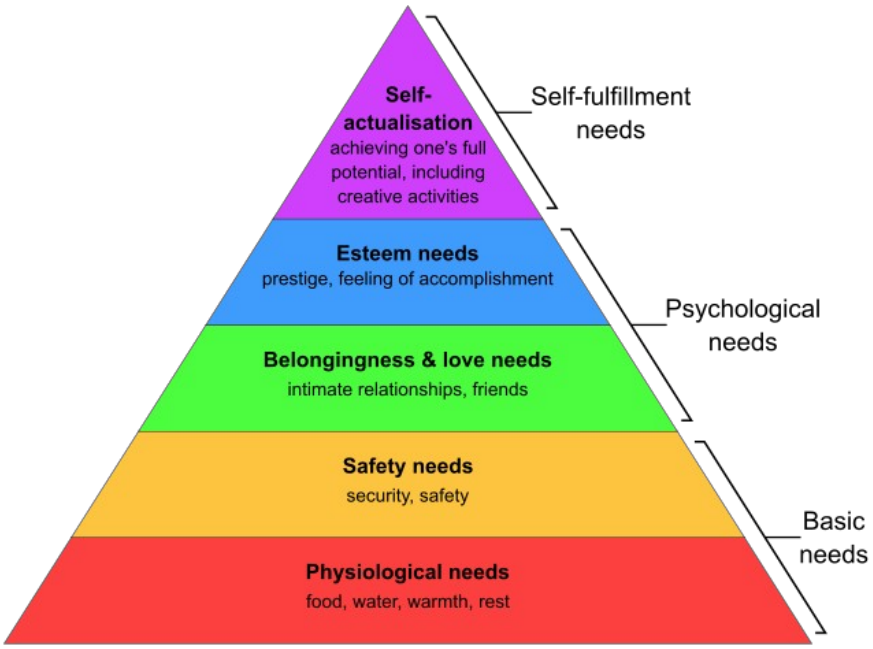


Figure 10: Maslow's Hierarchy of Needs

At the base level, technology can support physiological needs – such as food, water, and shelter – through innovations in agriculture, clean water delivery and clean air maintenance, and smart housing. Safety needs are addressed through security systems, health monitoring and health care, and emergency communication tools. As we move up the hierarchy, technology supports belonging and esteem through social media, online communities, and platforms for self-expression.

It has often been said that we currently live in a time where **literally all** of the basic needs at the lowest levels of Maslow's hierarchy could be assured for all people of the world! We already have the *technology* for production, distribution and re-distribution, monitoring for need, and all associated communication needs, to completely eradicate food insecurity (hunger, thirst and starvation), clothing needs and housing needs (shelter and safety), assure clean air, land and water (pollution removal), health care (diagnostics and treatment) and provide the peace-of-mind and mental wellness that comes from having all of these other needs addressed. The *technology* isn't what is getting in the way of achieving all of this!

Rather, it is the insistence of holding on to the status-quo of man-made economic systems which favor one economic group to the detriment of all others. This is the ***only*** thing that is preventing all of these achievements. It isn't the *tech* that is lagging. Rather, it is the socioeconomic constructs that are the root cause preventing the ethical implementation of the tech.

Even worse, additional ethical tensions arise when technology is used in ways that actually exacerbate rather than work to address Maslow's hierarchy needs: for example, when farmers are paid to *not produce* food to keep prices at an artificial level – all while people go hungry. Or when drug companies are allowed to charge obscene prices for life-saving treatments resulting in millionaire-class executives, while simultaneously standing idly by while poor people die without the treatments. Or when surveillance systems undermines privacy (a component of safety), or when social media algorithms foster isolation or harm self-esteem. The challenge for technologists and society is to ensure that digital tools are designed *and deployed* in ways that genuinely enhance human flourishing at every level of Maslow's hierarchy, being mindful of unintended consequences and the needs of the most vulnerable.

Digital Divide

The digital divide refers to the gap between those who have ready access to computers, the internet, and possess **digital literacy**, and those who do not. This digital divide is most readily recognized along lines of income, geography, age, and/or ability. This divide often limits opportunities for education, employment, healthcare, and civic participation, reinforcing cycles of disadvantage. Ethically, bridging the digital divide is not just a matter of providing hardware or connectivity, but also of addressing affordability, digital skills, and culturally relevant content.

Consider this hypothetical case:

A 24-hour convenience store in New York has been robbed multiple times in the last several years. Fortunately, no employees were ever *physically* harmed although most have experienced some amount of psychological trauma and many of them have subsequently quit. In fact, it is very hard to find any employees to work because of the continuing threat of being robbed at knife or gun-point.

So, the business owner decides that an ideal solution is to simply *stop accepting cash*! Instead, the owner places signs that says, "No CASH accepted and No CASH on premises." and "Credit or Debit Cards only accepted." The owner tells the local news team that they decided to go this route because, '… nobody ever robbed a store and asked them to hand over all of their credit card receipts! The cash is the problem.' The owner said, the technology will allow them to have a safe store once again, and this will allow the store to stay in business.

But there is only one problem with this plan… in 2020, New York passed a law that said it was *illegal* for a business to "**not** accept cash".

The law stated that its aim was to protect the rights of the 'unbanked' and 'underbanked' population. The state used, as part of its assertion, the picture of a $1 bill noting the inscription found on each bill of US currency:

Figure 11: US $1 bill highlighting 'legal tender' phrase

The state argues that it is *illegal* for anyone to *not* accept cash. They say that the currency says "**all debts, public and private"**… not just the debts that anyone wants to choose.

Note, that there actually have been multiple legal cases about this very topic – and not just in New York! But, for the moment, let's not focus on the *legal* aspects of the case, but rather, let's think about the *ethical* aspects of the case.

If we look at the situation through the bodega owner's perspective and lenses, we can potentially see the following:

- The owner is trying to make a living and provide for their family while providing goods for their community at reasonable prices. (Maslow's hierarchy level 1)
- The owner needs workers to supplement their own work and keep the store open 24 hours as there are many customers who work all 3 shifts in the neighborhood. (Maslow's hierarchy level 1)
- The workers need to feel safe and the risk of being robbed for cash prevents this. (Maslow's hierarchy level 2)
- A tech solutions (cashless-payments) exists that address the need previously mentioned.
- The owner wants *everyone* to have a cashless payment option and says it is the banks responsibility to give a card to anyone who has cash and let the bank take on the exclusive risk of being robbed for their cash.

But now, let's look at it from the bank's perspective and lenses:

- The bank will only allow for a new account to be opened if there is a minimum original deposit, and a minimum maintained balance, and/or a repeating direct deposit.
- The bank *claims* that this is necessary because the cost of maintaining an account requires these balances.
- Meanwhile, the bank has reported that once again this year, the bank has earned *record profits* and its executives are making multi-million-dollar bonuses.
- The bank points to the statement emblazoned on the currency itself and declares – the cash is already here so it's not our problem.

Finally, let's look at the situation from one particular customer's perspective and lenses:

- I was laid off from my previous job and I am currently freelancing odd jobs just to get by.
- The jobs I can get all pay me in cash.
- I had to close my bank account because I couldn't maintain a minimum balance and I no longer have direct deposit. Since I had to file for bankruptcy, I can't get a credit card anymore.

- I am *just barely getting by – literally –* and pretty much all that I have to my name is right here in my pocket.
- I just need to get some food before I drive over to the park to crash for a few hours in my car.

As we look at this kind of situation through the various lenses of the different individuals involved, it can become pretty obvious pretty quickly that the issues that are causing concern are **not the tech**! But rather, the issues surround the facts that the socioeconomic systems, and the legal systems, have not kept pace with the changes that have been brought about by tech advancements. And, rather than focusing on the ***ethical*** considerations of the situation, our current society tends to put greater focus on the *legal* considerations that have too often tended to foster adherence to the status-quo.

And it is this perpetuation of the status-quo that continues to exacerbate the divides (socioeconomic and technological) which become an ever-widening and unsustainable downward spiral.

Efforts to close the digital divide must be intentional and sustained, involving collaboration among governments, private sector, educators, and community organizations. There is also an ethical obligation to consider the environmental and social impacts of technology deployment, ensuring that solutions are sustainable and respect the needs and voices of marginalized communities. In a world increasingly shaped by digital technology, promoting justice and social equity means ensuring that everyone has the opportunity to participate fully and fairly in the digital society.

Textbook Definitions – Tech, Justice and Social Equity

- **Algorithmic personalization** – The use of computer algorithms to tailor digital content, services, or experiences to individual users based on their data and behaviors, raising ethical questions about fairness, autonomy, and the reinforcement of social inequalities.
- **Privacy** – The right of individuals to control access to their personal information and data, particularly regarding how it is collected, used, and shared by technology platforms.
- **Informed consent** – The process by which individuals are provided with clear, understandable information about how their data will be used by technology systems, enabling them to make voluntary and knowledgeable decisions about their participation.
- **Digital Divide** – Refers to the gap between those who have ready access to computers, the internet, and possess digital literacy, and those who do not. The digital divide is often obviously recognized along socioeconomic lines.

- **Bias** – Systematic and unfair discrimination that can be embedded in technological systems, such as algorithms, which may perpetuate or amplify existing social inequalities and injustices.
- **Digital literacy** – The ability to critically understand, evaluate, and effectively use digital technologies, which is essential for individuals to navigate, question, and challenge the impacts of technology on justice and social equity.
- **Autonomy** – The capacity for individuals to make self-directed, informed choices in digital environments, which can be threatened by technologies that manipulate or constrain decision-making without transparency or consent.
- **Telemedicine** – The remote delivery of healthcare services and clinical information using telecommunications technology, which expands access to care but raises ethical concerns about patient privacy, confidentiality, and the quality of the patient-provider relationship.
- **Electronic medical records (EMR)** – Digital versions of patients' medical histories maintained by healthcare providers, designed to improve care coordination and efficiency while presenting challenges related to data security, privacy, and equitable access.
- **Wearable health monitors** – Technology-enabled devices worn on or in the body that continuously collect and transmit health data, offering opportunities for proactive health management but also raising issues of data privacy, consent, and potential disparities in access.
- **AI-driven diagnostics** – The use of AI systems to analyze medical data and assist in diagnosing health conditions, which can enhance diagnostic accuracy and efficiency but may simultaneously introduce algorithmic bias, and lack of transparency, and accountability.
- **Patient privacy** – The ethical and legal obligation to protect individuals' health information from unauthorized access or disclosure, a critical concern heightened by the use of digital health technologies such as telemedicine, wearable health monitors and EMRs.
- **Screen readers** – Software applications that convert digital text into synthesized speech or braille, enabling people with visual impairments to access and interact with digital content and promoting greater accessibility and inclusion.
- **Voice recognition** – Technology that interprets and processes spoken language, allowing users – especially those with mobility or dexterity challenges – to control devices and input information hands-free, thereby enhancing digital accessibility.
- **Adaptive hardware** – Specialized physical devices designed to accommodate the needs of individuals with disabilities, such as modified keyboards or alternative input devices, which help remove barriers and foster inclusive participation in technology use.

7. Technology in Personal and Social Life

Digital Relationships; Online Dating; Personal Data Tracking; Digital Minimalism; Technology Addiction

Technology has become deeply woven into the fabric of daily life, shaping how individuals interact, form relationships, and manage personal well-being. As digital tools and platforms increasingly mediate everything from communication to leisure, they bring both opportunities for connection and challenges around **autonomy**, **privacy**, and **mental health**. The pervasive nature of technology means that personal choices – such as how much time to spend online or which platforms to use – can have far-reaching effects on social dynamics, emotional resilience, and even one's sense of self.

Figure 12: Graphic representation of a digital footprint

Navigating this landscape requires a thoughtful approach to the ethical questions that arise when technology intersects with personal and social spheres. Issues such as the management of **digital footprints**, the boundaries between public and private life, and the impact of constant connectivity on relationships demand careful consideration. As society continues to adapt to evolving digital norms, individuals must balance the benefits of technological convenience with the responsibility to protect their own well-being and that of their communities.

Digital Relationships

Digital relationships are connections that are primarily formed, maintained, or deepened through digital communication channels such as social media, messaging apps, online forums, or video calls. Unlike traditional relationships that rely on physical proximity and face-to-face interaction (i.e. **in-real-life (IRL)**, digital relationships transcend geographical boundaries and can develop between individuals who *may never meet in person*. These connections can be romantic, platonic, or professional, and are often characterized by the use of text, images, video, and other digital media to convey emotion, share experiences, and build trust.

While some view digital relationships as fleeting or **"throw-away" connections** – easily formed and just as easily discarded – others experience profound intimacy and authenticity in their online interactions. The digital environment can lower barriers to self-disclosure, allowing individuals to share personal thoughts and feelings more openly than they might in person. This can lead some to value

digital connections as deeply, or even more so, than their in-person relationships. However, the lack of physical cues and the potential for **curated online personas** can blur the lines between genuine connection and illusion, sometimes causing individuals to lose perspective on the nature and depth of their digital ties.

Online Dating

Online dating refers to the practice of seeking romantic or sexual partners via internet platforms, typically through dedicated websites or mobile apps that facilitate the creation of personal profiles and digital communication. These platforms allow users to present curated aspects of their identity – such as interests, values, and appearance – and to browse or be matched with others based on compatibility algorithms or personal preferences. The convenience, broad reach, and **relative anonymity** of online dating have made it a mainstream method for meeting new people, offering opportunities to connect beyond traditional social circles and geographic boundaries. For online dating sites to be considered valuable, they must foster a safe, respectful environment, provide accurate and meaningful matches, and protect user privacy. Features such as robust identity verification, **transparent algorithms**, and clear communication tools contribute to a platform's credibility and user trust.

However, online dating also presents significant risks and ethical challenges. **Algorithmic bias** can skew matches, reinforcing stereotypes or excluding certain groups, while aggressive data collection and the sale of personal information raise concerns about user privacy and consent. Some platforms may personalize content or matches to such an extent that they inadvertently **censor** or limit users' choices, reducing the diversity of potential connections. The prevalence of deceptive practices – including **catfishing** (posing as someone else), fraudulent schemes, and the creation of **fake profiles** – can lead to emotional harm or financial loss. These issues highlight the need for **ethical oversight**, **transparency in data use**, and robust safeguards to ensure that online dating remains a positive and equitable experience for all users.

Personal Data Tracking

In an era of '**big-data**', there is no such thing as **'TMI' (too-much-information)**. Every digital interaction, no matter how trivial it may seem, contributes to a vast and ever-expanding profile of personal data. Companies routinely track direct data points such as names, email addresses, phone numbers, and purchase histories, but the scope goes far beyond this. Indirectly, organizations can derive sensitive information from **patterns in browsing behavior**, **location data** from GPS, **device fingerprints**, app usage, social media activity, and even **metadata** embedded in videos, photos and messages. By aggregating and analyzing these diverse data streams, companies can infer a person's habits, preferences, health status, social circles, and even political leanings.

Consider a hypothetical user who only provides their name, email address, date of birth, and country when signing up for a service on their smartphone. Even with just these four data points, the device and associated apps can collect a wealth of additional information. The smartphone's operating system and apps may automatically log the user's IP address, device type, language settings, and geolocation. By linking the email address to other online accounts, **data brokers** can cross-reference social media profiles, public records, and past purchase histories. The date of birth enables age-based **profiling**, while the country helps narrow down cultural, legal, and economic backgrounds.

Meanwhile, passive data collection – such as app usage patterns, movement tracked via GPS, and browsing history – can reveal daily routines, frequented locations, and social interactions. Machine learning algorithms can then synthesize these disparate data points to construct an eerily accurate and invasive profile: predicting the user's income bracket, relationship status, health risks, interests, and even likely future behaviors. This comprehensive profiling, often invisible to the user, highlights the profound privacy risks and ethical dilemmas posed by ubiquitous personal data tracking in the digital age.

Digital Minimalism

Digital minimalism is often seen as a response to the overwhelming realities of big-data collection, where every online action contributes to a growing digital footprint that is neither fully transparent nor easily controlled. For some, embracing digital minimalism can resemble "sticking one's head in the sand" – a knee-jerk reaction to the anxiety and fatigue caused by constant notifications, **information overload**, and the persistent sense of **surveillance**. In this light, digital minimalism may appear as an attempt to escape rather than confront the pervasive reach of technology. This is especially apparent when "**opting out**" entirely is rarely practical (… or even possible…) in a world where digital connectivity underpins nearly every aspect of work, social life, and civic engagement.

Despite these limitations, the appeal of digital minimalism lies in its promise to restore balance, focus, and well-being by encouraging a more intentional and mindful relationship with technology. Rather than rejecting digital tools outright, digital minimalism advocates for curating one's digital environment to prioritize high-value activities that align with personal values and goals. Practitioners report benefits such as improved mental clarity, stronger relationships, and enhanced productivity, as they reduce digital clutter and reclaim their attention from low-value distractions.

However, the practical challenge remains: even the most disciplined digital minimalist cannot fully escape the data-driven infrastructure that shapes modern existence. Thus, digital minimalism is less about total withdrawal and more about making *conscious choices* to engage with technology in ways that support, rather than undermine, a meaningful and healthy life.

Technology Addiction

Technology addiction is a behavioral disorder characterized by compulsive and excessive engagement with digital devices and online activities, often to the detriment of personal, social, and professional well-being. Like other addictions, those affected may not recognize – or may actively deny – that their technology use has become problematic. Denial is a common defense mechanism, with individuals believing they are in control or rationalizing their behavior as normal, even as they neglect responsibilities, relationships, or self-care. This lack of self-awareness is compounded by the ubiquity of technology in daily life, making it difficult to distinguish between healthy use and dependency.

Many app developers and tech companies intentionally design their products to maximize user engagement, leveraging psychological principles such as **variable rewards** and **social validation** to create habit-forming experiences. Features like **endless scrolling**, **push notifications**, and **algorithmic content feeds** are engineered to keep users returning, increasing **screen time** and, ultimately, **advertising revenue**.

There have been high-profile legal actions against major tech firms alleging that their platforms are intentionally addictive, particularly to young users. For example, lawsuits have been filed against social media companies for allegedly exploiting vulnerabilities in children and teens to encourage **compulsive use**, with claims that these practices contribute to mental health crises.

In response, some governments and advocacy groups have called for increased regulation, **transparency in algorithm design**, and the implementation of features like **screen time limits** and digital well-being tools. It is their hope and intent that these additional approaches will help users regain control over their technology use. Despite these efforts, addressing technology addiction remains a significant challenge in an increasingly digital world.

Textbook Definitions – Technology in Personal and Social Life

- **digital footprint** – The unique trail of data created by an individual's online activities, both intentionally and unintentionally, including websites visited, emails sent, and information submitted online.
- **Digital relationships** – Connections formed and maintained primarily through digital communication channels such as social media, messaging apps, or online forums.
- **in-real-life (IRL)** – Interactions or relationships that occur in the physical, offline world rather than through digital platforms.
- **"throw-away" connections** – Brief, low-commitment digital interactions that are easily formed and just as easily discarded, often lacking depth or long-term significance.

- **curated online personas** – Carefully crafted digital identities where individuals selectively present aspects of themselves to shape how they are perceived online.
- **Online dating** – The practice of seeking romantic or sexual partners through internet platforms that facilitate profile creation, matching, and digital communication.
- **relative anonymity** – The condition in which users can interact or share information online without fully revealing their true identities, often lowering barriers to self-disclosure.
- **transparent algorithms** – Algorithms whose functioning, criteria, and decision-making processes are openly disclosed and understandable to users.
- **Algorithmic bias** – Systematic and unfair discrimination embedded in automated decision-making processes, often reflecting or amplifying existing social prejudices.
- **censor** – To suppress, limit, or remove content or information from digital platforms, often based on specific rules, policies, or external pressures.
- **catfishing** – The act of creating a fake digital identity to deceive others, typically for personal, financial, or emotional gain.
- **fake profiles** – Online accounts that use false or misleading information to impersonate someone else or create a fictitious persona.
- **ethical oversight** – The process of monitoring and guiding technology development and deployment to ensure alignment with ethical standards and societal values.
- **transparency in data use** – The practice of clearly informing users about how their personal data is collected, processed, shared, and stored.
- **big-data** – Extremely large and complex datasets that are analyzed computationally to reveal patterns, trends, and associations, especially relating to human behavior.
- **TMI (too-much-information)** – The idea that excessive sharing or collection of personal data can occur, though in the context of big-data, there is often no perceived limit to what is gathered or analyzed.
- **information overload** – A state in which the volume of information received exceeds an individual's capacity to process or make decisions effectively.
- **patterns in browsing behavior** – Trends and habits revealed by analyzing the websites and content an individual visits or interacts with online.
- **location data** – Information about the geographical position of a device or user, often collected via GPS, Wi-Fi, or IP address.

- **device fingerprints** – Unique combinations of device attributes (such as browser type, operating system, screen size) used to identify and track users across digital platforms.
- **metadata** – Data that provides information about other data, such as time stamps, location, author, or device details associated with digital files or communications.
- **data brokers** – Companies or entities that collect, aggregate, and sell personal data from various sources, often without direct user consent.
- **profiling** – The process of analyzing and combining personal data to create detailed user profiles that predict behaviors, preferences, or characteristics.
- **Digital minimalism** – A lifestyle approach that emphasizes intentional and selective use of digital technologies to reduce distractions and focus on meaningful activities.
- **surveillance** – The continuous monitoring or observation of individuals' activities, often through digital means, for purposes such as security, marketing, or data collection.
- **opting out** – The act of choosing not to participate in certain digital services or data collection practices, often to protect privacy or reduce digital exposure.
- **Technology addiction** – A behavioral disorder involving compulsive and excessive use of digital devices or online platforms, leading to negative impacts on daily life.
- **variable rewards** – Unpredictable and intermittent incentives that reinforce repeated engagement with digital platforms, making them more habit-forming.
- **social validation** – The psychological reinforcement gained from receiving approval, likes, or positive feedback from others in digital environments.
- **endless scrolling** – A design feature that allows users to continuously view new content without explicit breaks, encouraging prolonged engagement.
- **push notifications** – Alerts sent by apps or websites to users' devices to prompt immediate attention or action.
- **algorithmic content feeds** – Streams of information or media curated and delivered to users based on automated analysis of their preferences and behaviors.
- **screen time** – The amount of time an individual spends using digital devices or engaging with screens.
- **advertising revenue** – Income generated by digital platforms through displaying ads to users, often driven by high engagement and data collection.

- **compulsive use** – Repetitive and uncontrollable engagement with digital technology, often despite negative consequences.
- **transparency in algorithm design** – The practice of making the logic, criteria, and functioning of algorithms open and understandable to users and stakeholders.
- **screen time limits** – Tools or policies that restrict the duration an individual can spend on digital devices or specific applications to promote healthier usage patterns.

8. Privacy, Surveillance, and Data Ethics

Big Data and Privacy; Public vs. Private; Urban Surveillance and Smart Cities; Data Collection and Consent; Cloud Computing; Data Ownership and Open-Source Solutions

As our lives become increasingly intertwined with digital technologies, the boundaries between public and private spheres have grown more complex. The preceding chapters have explored how technology shapes our identities, relationships, and access to opportunities, while also highlighting the responsibilities of both developers and consumers in navigating ethical challenges. From the responsibilities of tech users and professionals, to the impact of technology on justice, equity, and personal well-being, we have seen that ethical decision-making is rarely straightforward – often requiring us to balance competing values and anticipate unintended consequences.

Building on these foundations, this chapter delves into the critical issues of **privacy**, **surveillance**, and **data ethics**. In a world driven by **big data**, **cloud computing**, and **ubiquitous connectivity**, questions about who owns our information, how it is collected, and for what purposes it is used have become central to the ethical landscape. We will examine the evolving definitions of privacy in the digital age, the rise of **urban surveillance** and smart cities, and the ethical dilemmas posed by large-scale **data collection** and **consent**. By considering the implications of **data ownership** and the responsibilities of both individuals and organizations, this chapter aims to equip readers with the tools to critically assess the ethical dimensions of privacy and surveillance in contemporary society.

Big Data and Privacy

The rise of big data has fundamentally transformed the landscape of personal privacy. Every day, individuals generate vast amounts of digital information through online interactions, purchases, social media activity, and even **passive data collection** via mobile devices and **smart home technology**. This information is not only collected by the platforms and services individuals use directly, but is also routinely shared with third-party **data aggregators**, sold to marketers, and analyzed by a wide array of organizations seeking to infer deeper insights about users' behaviors and preferences. The sheer scale and interconnectedness of data collection means that a single piece of personal information – such as an email address or geolocation – can be replicated, cross-referenced, and stored in dozens, if not hundreds, of separate databases worldwide.

A crude (but conservative) estimate suggests that for any active digital user, there may be hundreds to thousands of copies of their personal data distributed across various entities. Each online service, retailer, social media platform, and app may create its own record; **data brokers** and aggregators further multiply these records as they buy, sell, and combine data sets; and backup systems, **cloud**

storage, and analytics platforms add further redundancy. Moreover, big data analytics can *infer* additional attributes and connections, effectively creating new "copies" of information by extrapolating from existing data points. This exponential proliferation makes it nearly impossible for individuals to fully track or control the spread of their digital footprints.

Consider this scenario: A big cell phone provider sells *anonymized* (de-identified) data points to a data aggregator and analysis group which cover a period of one-week for a particular region. The data was requested because a store in this region wants to learn more about the individuals who showed up for their *big sale event.* The aggregator starts by focusing on all of the cell phones that went to that particular store during the store's event.

But, they don't stop there. They then review where the data points go *after they left the store* to see the other destinations for these devices. They discover that quite a number of phones left the store and went to food establishments. This might suggest that the store should have some 'snacks' available during their next sale event. They also discover that a number of the devices went to a competitor's store… this may be interesting to both the original store as well as to the competitor store.

But then, they follow the phones to their 'final destinations' for that day to see where they ended up that night. Then, they repeat this process for each day (not just the sale day) to see what else they can learn about the 'anonymous' data points. Just by analyzing where the phones end up for the 'end-of-the-day' these data points may likely represent the 'homes' of the 'anonymous data points'. And tracking where the phones go each day, they are likely to discover other patterns as well. So much for anonymized data!

Privacy, in its most common definition, refers to the ability of individuals to control the collection, usage, and distribution of their personal information. It encompasses the right to decide what information is shared, with whom, and for what purposes. In the digital age, however, this expectation is increasingly challenged. The default practices of data collection, the complexity of data flows, and the **lack of transparency** in how information is shared or sold mean that true control over personal data is often illusory. While privacy remains a foundational value and a legal right in many jurisdictions, the reality is that maintaining a reasonable **expectation of privacy** online requires significant effort, technical literacy, and often, a willingness to opt out of many modern conveniences. Thus, while the principle of privacy is still widely recognized, its practical realization in the age of big data is fraught with challenges and, for many, may no longer be a fully reasonable expectation without substantial systemic change.

Public vs. Private

In the previous section, we considered the *expectation of privacy* in the age of big-data. So it seems now we should differentiate between the legal definitions vs. the ethical definitions of the terms '**Public**' vs. '**Private**'.

The distinction between 'public' and 'private' is foundational both in legal and ethical discussions, yet the definitions and boundaries can shift depending on context. Legally, 'public' typically refers to spaces, actions, or information that are accessible or visible to the general population and where individuals have a reduced expectation of privacy. 'Private,' on the other hand, denotes areas, behaviors, or data that are restricted to individuals or select groups, where a higher expectation of privacy is recognized and protected by law.

Ethically, the distinction often hinges on the **reasonable expectations** of those involved. Consider the scenario of looking through an open window into someone's home: while the window may be open and the view technically accessible from a public sidewalk, most people would agree that peering inside or, more invasively, taking a photo or video crosses an ethical line. The act transitions from a passive observation in a public space to an active intrusion into someone's private life, highlighting how **context** and **intent** matter.

Similarly, recording audio or video of people inside a grocery store – where there is a general expectation of being in a semi-public space – differs ethically (and sometimes legally) from recording those same people outside on a public sidewalk. The boundaries blur further in places like restaurants, public transportation, or even online forums, where the mix of public accessibility and private interaction complicates the ethical calculus.

Additional examples illustrate these nuances. In a workplace, conversations in a private office are generally considered private, while those in a break room may not be. In digital contexts, posting on a public social media page is typically considered public, but sending a direct message is private – though the technical ability to copy, share, or leak messages challenges this expectation. Even in public spaces, certain activities, such as using a restroom or changing clothes in a locker room, retain strong legal *and* ethical protections of privacy despite their location.

Ultimately, the legal definitions of public versus private are shaped by statutes and case law, often focusing on the impact of actions on society versus individuals. Ethically, the distinction is more fluid, relying on context, **societal norms**, and the reasonable expectations of those involved. As technology continues to blur these boundaries – through ubiquitous cameras, data collection, and online sharing – it becomes increasingly important to critically examine not just what is legally permissible, but what is ethically respectful of individuals' privacy and autonomy.

Urban Surveillance and Smart Cities

Urban surveillance and the development of smart cities have introduced a range of technologies that promise to enhance public safety, improve efficiency, and optimize city services. **Traffic cameras**, for instance, are widely deployed to monitor intersections, enforce traffic laws, and provide real-time data to manage congestion. These systems can reduce accidents and improve emergency response times by allowing authorities to quickly identify and address incidents. Similarly, vehicle tracking – enabled through **license plate readers** and various **connected sensors** – can help locate stolen vehicles, optimize public transportation routes, and even support environmental goals by monitoring emissions and traffic patterns.

However, these same technologies raise significant concerns about privacy and the potential for misuse. Traffic cameras and vehicle tracking systems can be repurposed for **mass surveillance**, enabling authorities or third parties to monitor individuals' movements without their knowledge or consent. This persistent observation can erode the sense of urban anonymity and create a chilling effect on personal freedom, as people may change their behaviors if they feel constantly watched. The aggregation of vehicle movement data, when combined with other data sources, can reveal sensitive patterns about individuals' routines and associations.

Facial recognition technology represents another powerful but controversial tool in the smart city arsenal. On the positive side, it can assist in locating missing persons, identifying suspects in criminal investigations, and enhancing security at large public events. Yet, the deployment of facial recognition in public spaces has sparked intense debate over **accuracy, bias,** and the risk of **wrongful identification**. Moreover, the widespread use of facial recognition can enable pervasive government or corporate monitoring, undermining **civil liberties** and disproportionately impacting **marginalized communities**.

Other notable examples include smart utility meters and environmental sensors. Smart meters can help residents and city officials monitor and reduce energy and water consumption, contributing to sustainability goals and lowering costs. Environmental sensors, such as those monitoring air quality or flood risks, can provide early warnings and improve public health outcomes. Yet, both technologies collect detailed data about residents' habits and activities, raising questions about who has access to this information and how it might be used beyond its intended purpose.

Ultimately, while urban surveillance and smart city technologies offer clear benefits – improved safety, efficiency, and sustainability – they also introduce complex ethical challenges. The risk of **cyberattacks**, unauthorized data sharing, and the erosion of privacy demands robust governance, transparent policies, and meaningful public engagement to ensure that technological progress does not come at the expense of individual rights and community trust.

Data Collection and Consent

The distinction between explicit and implied consent is central to understanding how data is collected and used in the digital environment. **Explicit consent** requires a clear, affirmative action from the user – such as checking a box, signing a form, or clicking an "I Agree" button – indicating unambiguous agreement to the collection and processing of their data. This type of consent is often accompanied by detailed language in **End-User License Agreements (EULAs)** or **Terms of Service (ToS)**, specifying what data will be collected, how it will be used, and who it may be shared with. For example, a ToS might state, "We collect your name, email, and usage data to provide and improve our services," and the company *requires* the user to actively accept these terms before proceeding.

Implied consent, by contrast, is inferred from a user's actions or the context in which those actions occur. If a user continues to browse a website after being notified of a **cookie policy**, or submits a contact form expecting a response, their behavior is interpreted as agreement to certain data practices – even if they have not explicitly acknowledged them. Implied consent is often used for routine or less sensitive data collection, but it is inherently less transparent and can lead to ambiguity or disputes over what the user actually agreed to.

A critical nuance in these agreements is the use of open-ended language regarding data use. For instance, a clause might state, "We may use your data for purposes such as backups or translation to another language." The phrase "such as" does not restrict the company to only those listed uses; rather, it leaves the door open for additional, unspecified uses of the data. The stated intent behind this language (if it is ever actually stated) is said by the company to provide flexibility for operational needs. However, it can also be used to *mask* broader data exploitation. For example, data collected for "service improvement" could be repurposed for targeted advertising, profiling, or even sold to third parties – uses not explicitly disclosed in the original agreement – but made legal through the agreement as written.

The concept of **intent** becomes central here. While a company may claim its intent is benign – such as improving user experience or ensuring data security – the same permissions can be leveraged for more intrusive or profit-driven activities, like behavioral advertising, location tracking, or sharing data with law enforcement or other organizations without further user notification. Other examples include using voice recordings from smart speakers to train AI beyond the stated purpose, or aggregating fitness tracker data for insurance risk assessment, even when the original consent was for personal health monitoring.

Legally, the sufficiency of consent – whether explicit or implied – depends on the jurisdiction and the sensitivity of the data involved. Regulations like the **General Data Protection Regulation (GDPR)** developed and implemented in the European Union, require explicit, informed consent for most personal data processing, especially for sensitive categories, and *place the burden on organizations* to demonstrate that valid consent was obtained.

Ethically, the bar is even higher: true consent should be **informed**, **freely given**, and **revocable**, with users fully understanding both the scope and intent of data collection. In practice, however, the complexity of agreements and the opacity of data flows make it difficult to prove that users have genuinely understood or agreed to all possible uses of their data.

Likewise, demonstrating the true intent of a company's data practices is challenging, as broad or ambiguous language can be exploited for purposes far beyond those originally disclosed. As a result, both proving consent and intent remains a fraught process, highlighting the ongoing need for clearer communication, stronger regulation, and more transparent data practices.

Cloud Computing

Cloud computing has become deeply integrated into the daily routines of non-corporate users, offering convenience and flexibility across a range of applications. Common examples include file storage and sharing services like Google Drive, Apple iCloud, and Dropbox, which allow users to save documents, photos, and videos remotely and access them from any device. Email services such as Gmail and Yahoo Mail rely on the cloud to store messages and attachments, making communication seamless and accessible from anywhere. Social media platforms like Facebook and Instagram use cloud infrastructure to let users upload and share photos, videos, and other content. Streaming services, including Netflix and Spotify, leverage the cloud to deliver on-demand entertainment to millions, while cloud-based productivity suites like Google Docs and Microsoft 365 enable real-time collaboration and document editing without the need for local software installations.

The primary appeal of these cloud-based applications lies in their promise of **accessibility across devices**, ease of use, and the ability to **synchronize data across multiple devices**. Users are drawn to the convenience of **automatic backups**, the ability to share files instantly, and the reduction in the need for physical storage or device-specific software. Cloud computing also supports mobile banking, online education, and even health and fitness tracking, making it a central pillar of modern digital life.

However, as discussed in the previous section on data collection and consent, the agreements users accept when adopting cloud services often grant providers broad rights over their personal information. While the stated intent may be to facilitate backups or enhance user experience, the legal language typically allows providers to use, analyze, and even share user data for purposes far beyond those original use cases. This creates a significant imbalance: the value extracted from user data – through targeted advertising, analytics, or third-

Figure 13: There is no cloud...

party partnerships – can exceed the utility provided to the user in the form of basic storage or convenience.

Consider this figure describing 'the cloud'. If we understand that **there is no cloud**, but rather, it is just someone else's computer, we begin to understand that we are just *using* their computers for storage, and that *they* are perpetually *peeking* at literally everything you put up there!

Transparency remains a major issue. Once data is uploaded to the cloud, users have little visibility into where it is stored, how it is processed, or with whom it is shared. The lack of clear, accessible information about data practices means that users cannot easily verify how their information is being used or if it is being sold or repurposed for profit. This opacity is compounded by the trend of phasing out traditional, locally-installed productivity software in favor of cloud-based, subscription-only models. Companies are increasingly steering users toward exclusive cloud solutions to ensure recurring revenue, gain greater control over software updates, and – crucially – maintain ongoing access to user data. As a result, users are often left with little choice but to accept these terms if they wish to continue using familiar tools, further eroding their control over personal information and privacy in the digital age.

Data Ownership and Open-Source Solutions

Data ownership refers to the legal rights, control, and authority an individual or entity has over specific sets of data, including how that data is accessed, used, modified, shared, or deleted. It is about both possession and responsibility, granting the owner the power to determine the fate of the data and to enforce those rights legally and ethically. Data ownership is foundational for accountability, privacy, and security in a world where personal and organizational data are invaluable assets.

Questions to Consider About Data Ownership:

- Does a person own their own name, or is it merely a public identifier?
- Who owns an individual's email address: the person, the email provider, or both?
- If you purchase a phone, do you own all the data stored on it, or does the manufacturer or service provider retain some rights?
- Is your fingerprint your property, or does an entity that collects and stores its digital representation (e.g., for authentication) share ownership?
- Who owns your DNA sequence: you, your healthcare provider, or the company that analyzes it?
- If a company collects your location data via a mobile app, do you retain ownership, or does the company claim rights through its terms of service?

- Who owns the photos and messages you upload to social media platforms – you, the platform, or both?
- If you generate creative works (art, writing, code) using a cloud-based app, do you own the content, or does the app provider have rights to it?
- When you use voice assistants, do you own the recordings, or does the service provider?
- Who owns aggregated or anonymized data derived from your personal information?
- If your data is sold to third parties, do you still have any ownership or control over it?
- Who owns the metadata (such as timestamps, device info, or usage statistics) generated by your interactions with digital services?
- If a government agency collects your data for public health or security, do you retain any ownership or rights over that data?

These questions illustrate the complexity and spectrum of data formats – ranging from **personally identifiable information (PII)** like names and fingerprints, to digital content, behavioral metadata, and even **biological data**. Legally, ownership can depend on jurisdiction, contractual agreements, and the nature of the data, while ethically, many argue individuals should retain primary rights and control over their personal information.

Some types of data, such as **biometric identifiers** (**fingerprints, facial scans, DNA**) and commonly accessed data (emails, social media posts), are inherently difficult to isolate and protect due to the way they are collected, stored, and shared across platforms and organizations. Once digitized and uploaded, these data types often become subject to broad terms of service that can dilute individual ownership and control.

By contrast, data that a user creates – such as documents, code, or media files – can, actually be more readily controlled and protected! **Open-source software** and **personal computing resources** provide the mechanisms by which users can take a modicum of control over digital information that they create. Open-source solutions empower users to retain ownership by allowing them to store, manage, and modify their data locally or on self-hosted platforms, free from restrictive proprietary agreements. This approach not only enhances privacy and security but also aligns with the ethical principle that individuals should have meaningful control over their own digital creations and personal information.

There are many open-source solutions for the vast majority of the computing activities that typical users experience. Here is a brief list (as of this publication) of just some of the open-source titles and their typical uses:

Here are several of the most popular open-source software titles across a wide range of productivity and creative tasks, suitable for non-corporate users:

Operating Systems

• Ubuntu	• Linux Mint	• Debian
• Fedora	• Manjaro	• OpenBSD
• FreeBSD	• Puppy Linux	

Personal Information Managers & Email

• Thunderbird	• Evolution	• KOrganizer/KMail

Office Applications

• LibreOffice	• OnlyOffice	• Calligra Suite

Artistic and Image Editing

• GIMP (Photo Editing)	• Inkscape (vector graphics)	• Krita (digital painting)

Video Editing and Production

• Shotcut	• Blender (also for 3D modeling and animation)	• OBS Studio (Open Broadcaster Software)

Audio Editing and Production

• Audacity	• LMMS (Linux Multi Media Studio)	• Ardour

Other Productivity and Creative Tools

• VLC Media Player (media playback)	• Nextcloud (personal cloud storage and collaboration)	• Joplin (note-taking and to-do lists)
• Scribus (desktop publishing)	• Darktable (photo workflow and raw development)	• Calibre (e-book management)
• Rocket.Chat (team communication)	• Jupyter Notebook (interactive computing and data science)	

These tools provide robust alternatives to proprietary solutions and empower users to retain greater control over their data and creative output.

Textbook Definitions – Privacy, Surveillance, and Data Ethics

- **privacy** – The right and ability of individuals to control the collection, use, and sharing of their personal information, ensuring freedom from unwarranted intrusion into their lives.
- **surveillance** – The monitoring or observation of individuals or groups, often by authorities or organizations, to collect information or ensure security, which can threaten privacy if unwarranted.
- **data ethics** – The moral principles and guidelines that govern the collection, analysis, and use of data, emphasizing privacy, transparency, accountability, and fairness.
- **big data** – Extremely large and complex datasets generated from various sources, analyzed to reveal patterns, trends, and associations, especially relating to human behavior.
- **cloud computing** – The delivery of computing services – including storage, processing, and software – over the internet, allowing users to access and manage data and applications remotely.
- **ubiquitous connectivity** – The state of being continuously connected to digital networks and services from virtually anywhere, enabling constant data exchange.
- **urban surveillance** – The use of technology such as cameras, sensors, and tracking systems in cities to monitor public spaces and activities for safety, efficiency, or control.
- **data collection** – The process of gathering information from various sources, either actively or passively, for analysis, storage, or decision-making.

- **consent** – Permission granted by individuals for the collection and use of their data, which should be informed, freely given, and revocable.
- **data ownership** – The legal rights and control an individual or entity has over specific data, including how it is accessed, used, shared, or deleted.
- **passive data collection** – Gathering information from users without their direct input or awareness, often through background processes or device sensors.
- **smart home technology** – Devices and systems within a home that use internet connectivity to automate and control functions such as lighting, security, and climate.
- **data aggregators and brokers** – Entities that collect, combine, and sell data from multiple sources, often creating detailed profiles of individuals.
- **cloud storage** – A service that allows users to save data on remote servers accessed via the internet, rather than on local devices.
- **lack of transparency** – The absence of clear, accessible information about how data is collected, used, or shared, making it difficult for individuals to understand or control their data.
- **expectation of privacy** – The belief or assumption that one's personal information or activities will not be observed or disclosed without consent.
- **Public** – Legally and ethically, spaces, actions, or information accessible to the general population, where individuals have a reduced expectation of privacy.
- **Private** – Spaces, actions, or information restricted to individuals or select groups, where a higher expectation of privacy is recognized and protected.
- **reasonable expectations** – What an average person would consider appropriate regarding privacy or data use in a given context.
- **context** – The circumstances or setting in which data is collected, used, or observed, which influence privacy expectations and ethical considerations.
- **intent** – The purpose or motivation behind collecting, using, or sharing data, which affects the ethical evaluation of those actions.
- **societal norms** – The shared expectations and rules within a community that shape perceptions of privacy, consent, and acceptable data practices.
- **Traffic cameras** – Cameras installed in public areas to monitor vehicle flow, enforce traffic laws, and enhance public safety.

- **license plate readers** – Automated systems that capture and process images of vehicle license plates for law enforcement or traffic management.
- **connected sensors** – Devices embedded in infrastructure or vehicles to collect and transmit data on movement, environment, or system status.
- **mass surveillance** – The large-scale monitoring of populations, often by governments, using technology to collect and analyze vast amounts of data.
- **Facial recognition** – Technology that identifies or verifies individuals by analyzing facial features from images or video.
- **accuracy** – The degree to which a system or process correctly identifies, measures, or represents information, crucial for fair outcomes in surveillance and data use.
- **bias** – Systematic errors or prejudices in data collection, analysis, or technology that can lead to unfair or discriminatory outcomes.
- **wrongful identification** – Incorrectly matching or labeling an individual by surveillance or recognition systems, leading to potential harm.
- **civil liberties** – Fundamental rights and freedoms, such as privacy and free expression, that are protected from excessive government or organizational intrusion.
- **marginalized communities** – Groups that experience discrimination or disadvantage, often disproportionately affected by surveillance and data misuse.
- **cyberattacks** – Malicious attempts to access, disrupt, or damage digital systems or data.
- **Explicit consent** – Clear, affirmative agreement to data collection or processing, usually given through direct actions like checking a box or clicking “I Agree”.
- **End-User License Agreements (EULAs)** – Legal contracts between software providers and users outlining the terms for using the software, including data rights.
- **Terms of Service (ToS)** – Agreements specifying the rules, responsibilities, and data practices associated with using a digital service.
- **Implied consent** – Permission inferred from a person’s actions or the context, rather than a direct statement or agreement.
- **cookie policy** – A statement on a website detailing how cookies are used to collect and process user data.
- **General Data Protection Regulation (GDPR)** – A comprehensive European Union law that governs data protection and privacy, emphasizing informed, explicit consent and user rights.

- **informed** – Having adequate information to understand the implications and risks before agreeing to data collection or use.
- **freely given** – Consent provided voluntarily, without coercion or undue pressure.
- **revocable** – The ability to withdraw consent at any time, stopping further data collection or use.
- **Cloud Computing** – The practice of using remote servers on the internet to store, manage, and process data, rather than relying on local hardware.
- **accessibility across devices** – The capability to use data and applications seamlessly from multiple devices via cloud services.
- **synchronize data across multiple devices** – Keeping files, settings, and information consistent and updated on all user devices through cloud-based solutions.
- **automatic backups** – The process of regularly copying data to a remote server to prevent loss and ensure recovery.
- **Data ownership** – The legal and ethical right to control, access, and manage one's own data, including decisions about its use and sharing.
- **personally identifiable information (PII)** – Any data that can be used to identify a specific individual, such as names, addresses, or Social Security numbers.
- **biological data** – Information derived from an individual's biological characteristics, including DNA, fingerprints, and other biometrics.
- **biometric identifiers** – Unique physical or behavioral traits, such as fingerprints, facial scans, or iris patterns, used for identification.
- **fingerprints** – Distinctive patterns on the tips of fingers, often used as a biometric identifier.
- **facial scans** – Digital representations of facial features used for identification or authentication.
- **DNA** – The genetic material that carries an individual's hereditary information, unique to each person.
- **Open-source software** – Software with publicly available source code that can be freely used, modified, and distributed by anyone.
- **personal computing resources** – Devices and infrastructure owned and controlled by individuals, enabling them to manage and store their own data locally.

9. Digital Communication, Social Media, Misinformation and Democracy

Social Media Ethics; Cyberbullying and Harassment; Deepfakes; Misinformation; Manipulation; Free Speech vs. Hate Speech; Influencer Culture; Media Literacy

The digital revolution has profoundly transformed the ways in which people connect, share ideas, and participate in civic life. This chapter explores how the tools and platforms that facilitate these interactions also raise complex ethical questions that touch on every aspect of our personal and collective existence. The rapid spread of information – and the ease with which it can be shaped or distorted – has forced societies to confront new challenges regarding trust, credibility, and the responsibilities of both individuals and institutions. These dynamics are deeply interwoven with our earlier discussions on privacy, data ethics, and the broader societal impacts of technology. This all serves to highlight the need for nuanced approaches to digital citizenship.

As digital spaces become central to public discourse, the boundaries between private expression and public consequence have blurred. The ethical dilemmas introduced here are not isolated; they are amplified by the same technological advancements that enable unprecedented connectivity and innovation. Issues explored in previous chapters – such as the responsibilities of tech developers and consumers, the vulnerabilities of digital identities, and the implications of surveillance – are now seen through the lens of how information is shared, consumed, and manipulated. This chapter examines the ways in which digital communication shapes social norms, influences decision-making, and can both *empower* as well as *undermine* democratic processes. It is here that the ethical frameworks introduced at the outset of this text are put to the test, as readers are invited to consider how technology mediates our relationships with each other and with the wider world.

Social Media Ethics

Social media has redefined how individuals engage with information and with one another, creating a dynamic environment where both users and platforms play crucial ethical roles. As consumers, people are constantly exposed to a vast array of content – news, opinions, entertainment, and more – often algorithmically curated and designed to **maximize engagement** rather than assure **accuracy**. This places a unique responsibility on users to critically evaluate the information they encounter. **Ethical participation** means more than simply sharing or reacting; it involves considering the potential impact of one's posts and interactions. Users must weigh the value of free expression against the potential harm caused by spreading **misinformation**, engaging in harmful rhetoric, or participating in online **harassment**. The rise of digital anonymity can sometimes embolden individuals to act in ways they would not in face-to-face interactions, underscoring the importance of empathy, respect, and **accountability** in online spaces.

Platforms, on the other hand, bear a distinct set of ethical responsibilities. While users must exercise personal judgment, social media companies are tasked with balancing the principles of free speech with the need to prevent harm and maintain a safe, inclusive environment – all while keeping their financial bottom line in mind. This balancing act often manifests in debates over **censorship** – where does **moderation** cross the line into undue **suppression** of ideas? Platforms must also grapple with the challenge of distinguishing between legitimate **satire** and deliberately **misleading content**. The expectation of **fact-checking** is a contentious issue: while some argue that platforms should take a more active role in verifying information, others warn of the dangers of overreach and the potential for **bias in content moderation**. Ultimately, both participants and platforms share an ethical obligation to foster an online ecosystem that encourages constructive dialogue, protects against harm, and upholds the integrity of public discourse – a challenge that grows ever more complex as the digital landscape continues to evolve.

Cyberbullying and Harassment

Cyberbullying and harassment are two closely related forms of harmful behavior that occur through digital channels. **Cyberbullying** is defined as the use of technology – such as social media, messaging apps, or online games – to harass, threaten, embarrass, or target another person. It often involves repeated actions intended to harm, and can include sending mean or aggressive messages, spreading rumors, posting embarrassing photos or videos, or deliberately excluding someone from online groups. **Harassment** is a broader term that encompasses any unwanted behavior intended to annoy, threaten, or intimidate another person, and in a digital context, this can range from persistent unwanted messages to explicit threats or hate speech. Both cyberbullying and harassment can have severe emotional and psychological consequences, especially since digital content can be widely and permanently distributed.

Examples of these behaviors are numerous and can include **cyberstalking**, where an individual monitors or follows someone's online activity obsessively, often with threatening intent; **doxxing**, which involves maliciously sharing someone's personal information online without consent; and the distribution of **inappropriate material**, such as **revenge porn**, which is the sharing of explicit images or videos without consent to humiliate or blackmail the victim. Other mechanisms include **impersonation** (creating fake profiles to harm someone's reputation), **trolling** (posting inflammatory or offensive comments to provoke a reaction), and **flaming** (sending hostile and insulting messages). These actions not only violate privacy but can also escalate into situations where victims feel unsafe in both digital and physical spaces.

From a young age, many children and adolescents may be exposed to digital environments where the culture of "trash-talking" – playful or aggressive banter often aimed at opponents in online games – is prevalent. While initially intended as harmless competition, such behavior can quickly escalate if not

moderated, leading to more serious forms of cyberbullying or harassment. The anonymity and distance provided by digital platforms can embolden individuals to cross ethical boundaries. As a result, what begins as teasing can easily spiral into targeted campaigns of abuse. Over time, repeated exposure to or participation in such behavior can desensitize young people to the harm caused by their words and actions, making it crucial for both individuals and platform providers to foster respectful and accountable online communities.

Deepfakes, Misinformation and Manipulation

Deepfakes, misinformation, and manipulation represent some of the most complex ethical challenges in today's digital landscape. **Deepfakes** – realistic, AI-generated images, videos, or audio – can blur the line between truth and fiction, with both creative and destructive potential. On the positive side, deepfake technology has been used to enhance public awareness campaigns, such as the "Malaria Must Die" initiative, where David Beckham appeared to speak in nine different languages, helping to reach a global audience. In media, Reuters has employed AI-generated presenters for personalized news summaries, making content more accessible and engaging. Other beneficial uses include voice cloning for individuals with speech impairments, de-aging actors for films, and creating immersive educational or historical experiences.

However, deepfakes have also led to significant legal and ethical controversies. Lawsuits have arisen over non-consensual use of individuals' likenesses – most notably in cases involving revenge porn, where deepfakes have been used to create explicit content without consent, leading to litigation and demands for stricter regulation. High-profile cases also include financial scams, where deepfake voices or videos **impersonated executives** to authorize fraudulent transactions, resulting in millions in losses and subsequent lawsuits. Celebrities and public figures have similarly pursued legal action against unauthorized deepfake impersonations that damaged their reputations or misled the public.

Misinformation and manipulation, meanwhile, are often amplified by automated tools such as **bots**, which can flood social media platforms with false or misleading content. Bots are designed to mimic human behavior, allowing them to interact with users, post comments, and even "like" or share content en masse. This orchestrated activity can artificially boost the visibility of certain narratives, pushing curated lists of users toward **trending** misinformation. The intent is often to manipulate public opinion, influence elections, or sow discord by making fringe ideas appear more widely accepted than they actually are. The combination of deepfakes and bot-driven misinformation creates a potent tool for manipulation, challenging both individuals and platforms to discern fact from fiction in an increasingly synthetic information environment.

Free Speech vs. Hate Speech

The legal definitions of "**free speech**" and "**hate speech**" have evolved through a complex interplay of constitutional principles, court decisions, and ongoing debates about ethics and public order. In the United States, the First Amendment protects freedom of speech as a foundational right, barring the government from restricting expression based on viewpoint, even when that expression is offensive or hateful. The intent behind this legal framework was to uphold robust public discourse and protect minority voices, recognizing that ethical considerations – such as the need to prevent harm and promote dignity – must be balanced against the imperative of **open debate**. Over time, courts have clarified that speech can only be restricted if it directly incites imminent lawless action or constitutes a true threat.

Despite these legal boundaries, ethical debates persist over what constitutes acceptable speech. Hate speech, while not legally defined in the U.S., is generally understood as expression intended to vilify, humiliate, or incite hatred against a group or class of people based on characteristics such as race, religion, gender, or sexual identity. The challenge arises because the same words or phrases can be interpreted differently depending on the observer's perspective, cultural background, or personal experience. Can you think of some phrases that have been used by one group as a rallying cry of 'free speech' while others attempt to vilify anyone who uses the exact same phrase with accusations of 'hate speech'?

When communities or governments attempt to define and regulate these terms, the result is often confusion, ambiguity, or outright contradiction. The subjective nature of what constitutes hate speech or offensive speech means that any attempt to codify these concepts risks either **overreach** – suppressing legitimate debate – or **underreach** – failing to protect vulnerable groups from harm. This tension is heightened in diverse societies, where different groups may have conflicting values and interpretations of what is ethical or acceptable. As a result, legal definitions *rarely* align perfectly with the full spectrum of ethical considerations, and the process of defining these terms remains a contentious and evolving challenge for both lawmakers and society at large.

Influencer Culture

Influencer Culture refers to the social phenomenon in which individuals – both online and off – build communities around themselves and exert significant commercial and non-commercial influence over their followers. This culture is not new: throughout history, prominent figures such as royalty, philosophers, political leaders, and celebrities have shaped public opinion, set trends, and influenced consumer behavior. In the digital age, however, the barriers to becoming an influencer have dropped dramatically, and the speed and reach of influence have expanded exponentially.

Before the rise of social media, influencers included figures like Eleanor Roosevelt, who used her newspaper column and radio appearances to shape public opinion and advocate for social causes. In the

20th century, celebrities such as The Beatles, Marilyn Monroe, and Audrey Hepburn became trendsetters whose choices in fashion, music, and lifestyle were widely emulated. Today, influencers are typically individuals who have built large followings on platforms like Instagram, YouTube, and TikTok. These influencers often arrive without credentials or any specific expertise. Rather, they excel at social media engagement and, perhaps, have a likable or convincing personality.

As influencer culture has grown, so too have debates about the responsibilities of influencers themselves. Some have faced backlash and legal repercussions for promoting harmful products, spreading misinformation, or engaging in unethical behavior. In response, there have been calls – and sometimes legal actions – to hold influencers accountable for the consequences of their actions, particularly when those actions mislead or harm their audiences. This includes demands for greater transparency in sponsored content, as well as accountability for endorsing products or ideas that may have negative real-world effects.

The rise of influencers goes beyond mere entertainment. For many followers, influencers fill voids left by traditional institutions, offering advice, companionship, or a sense of belonging that may be missing from their everyday lives. Influencers often create parasocial relationships – one-sided bonds where followers feel a personal connection to the influencer – which can be a source of comfort, inspiration, or even identity formation. This dynamic can make influencers powerful agents of change but also places significant responsibility on their shoulders.

Despite the potential for lasting impact, many influencers experience the ephemeral nature of fame. The phrase “15 minutes of fame” is especially apt, as viral success can be fleeting, and the public’s attention is fickle. Some influencers exhaust their popularity through overexposure, scandal, or controversial behavior, leading to a rapid loss of followers and influence. Others “crash and burn” more dramatically, facing public backlash or legal issues that end their careers as quickly as they began. This cycle highlights both the opportunities and the risks inherent in influencer culture, underscoring the need for ethical awareness and resilience in the digital age.

Media Literacy

Media Literacy is the ability to access, analyze, evaluate, create, and act using all forms of communication. It goes beyond simply understanding information; it involves critical thinking about the messages we encounter, their sources, and their impact. Media literacy empowers individuals to navigate the complex media landscape, discerning **credible information** from misinformation or manipulation.

A cornerstone of media literacy is the use of multiple sources to verify facts. By comparing information from various **reputable outlets**, consumers can identify patterns, inconsistencies, or biases. Evaluating the **credibility of sources** is also essential. This includes considering the reputation

of the publisher, the author's expertise, and the presence of citations or references to original research. Traditional methods also involve checking for **objectivity**, **transparency** about funding or affiliations, and whether the information is current and relevant.

Determining whether information is factual or opinion-based requires careful analysis. Facts are statements that can be objectively verified with evidence, while opinions reflect personal beliefs or interpretations. Facts are often presented with quantifiable data without qualification with an intent to inform. Whereas opinions are often subjectively presented with adjectives and adverbs intended to persuade, or in some other way elicit an emotional response. A simple way to consider whether some content is more **fact-based** or **opinion-based** is to simply count the parts of speech. If the piece has notably more numerals, nouns, and verbs (objective) than it has adjectives and adverbs (subjective) then the piece may be more fact-based than opinion-based. But if the piece has more subjective language than objective language, you already know that the piece is more opinion than fact.

Content creators bear the responsibility of producing accurate, transparent, and ethical media if they are, in fact, acting in an ethical framework. This means clearly distinguishing between facts and opinions, disclosing conflicts of interest, and correcting errors promptly. Creators should also be mindful of the potential impact of their messages on audiences, striving to avoid harm and promote informed understanding.

Content consumers, on the other hand, must approach media with a critical mindset. This includes **questioning the motives** behind messages, **recognizing bias**, and seeking out diverse perspectives. Consumers should also engage in reflection about how media influences their thoughts and behaviors, and take action – such as sharing reliable information or educating others – to contribute positively to public discourse. By embracing these practices, both creators and consumers can foster a media environment that supports truth, accountability, and informed civic participation.

Textbook Definitions – Digital Communication, Social Media, Misinformation and Democracy

- **Social Media Ethics** – The moral principles and guidelines that govern responsible, respectful, and ethical behavior on social media platforms.
- **Maximize engagement** – Strategies designed to increase user interaction, such as likes, shares, and comments, on digital content.
- **Accuracy** – The degree to which information is free from errors, distortions, or misrepresentations.
- **Ethical participation** – Engaging online in a manner that is respectful, honest, and mindful of the impact on others.

- **Misinformation** – False or inaccurate information that is spread, regardless of intent to deceive.
- **Harassment** – Unwanted behavior intended to annoy, threaten, or intimidate another person, especially repeatedly.
- **Accountability** – The obligation to take responsibility for one's actions and accept the consequences.
- **Censorship** – The suppression or prohibition of speech, writing, or other forms of expression considered objectionable or harmful.
- **Moderation** – The process of monitoring and managing online content to ensure it complies with rules or standards.
- **Suppression** – The deliberate act of preventing information or expression from being shared or seen.
- **Satire** – The use of humor, irony, or exaggeration to criticize or mock people, ideas, or institutions.
- **Misleading content** – Information that is designed or likely to deceive or misinform the audience.
- **Fact-checking** – The process of verifying the accuracy of claims made in content or statements.
- **Bias in content moderation** – Prejudiced or unfair treatment in the review and management of online content.
- **Cyberbullying** – The use of digital technology to harass, threaten, embarrass, or target another person.
- **Cyberstalking** – The repeated use of digital technology to monitor, follow, or harass someone.
- **Doxxing** – The malicious act of publicly revealing private or identifying information about an individual without their consent.
- **Inappropriate material** – Content that is offensive, explicit, or otherwise unsuitable for its intended audience.
- **Revenge porn** – The distribution of explicit images or videos without consent, often to humiliate or blackmail.
- **Impersonation** – Pretending to be someone else online, often for malicious or deceptive purposes.
- **Trolling** – Posting inflammatory, offensive, or disruptive comments or messages to provoke a reaction.

- **Flaming** – Sending hostile and insulting messages, often in online discussions or forums.
- **Deepfakes** – Realistic, AI-generated images, videos, or audio that can make it appear someone said or did something they did not.
- **Impersonated executives** – Individuals falsely represented as company leaders, often in scams or fraudulent schemes.
- **Bots** – Automated software programs designed to perform tasks online, such as posting messages or mimicking human behavior.
- **Trending** – The state of being widely discussed or shared on social media at a given time.
- **Free speech** – The right to express opinions and ideas without fear of government retaliation or censorship.
- **Hate speech** – Expression intended to vilify, humiliate, or incite hatred against a group or class of people.
- **Open debate** – The free exchange of ideas and perspectives in public discourse.
- **Overreach** – Excessive or unjustified restriction of rights, such as speech, beyond what is necessary or appropriate.
- **Underreach** – Failing to provide sufficient protection or regulation, resulting in harm or injustice.
- **Influencer Culture** – The social phenomenon in which individuals build communities and exert significant influence over their followers' opinions and behaviors.
- **Credible information** – Information that is trustworthy, reliable, and supported by evidence.
- **Reputable outlets** – Media sources known for accuracy, fairness, and reliability in reporting.
- **Credibility of sources** – The degree to which a source is considered trustworthy and authoritative.
- **Objectivity** – The practice of presenting information in a neutral and unbiased manner.
- **Transparency** – Openness and clarity about intentions, actions, and sources of information.
- **Fact-based** – Information that is grounded in verifiable evidence and data.
- **Opinion-based** – Information that reflects personal beliefs, interpretations, or judgments.
- **Questioning motives** – The act of critically examining the reasons behind someone's actions or statements.

- **Recognizing bias** – Identifying personal or systemic prejudices that may affect the presentation or interpretation of information.

10. Intellectual Property, Digital Art, and Emerging Economies

Intellectual Property; Patents and Copyright; Trade Secrets and National Security; Blockchain and Cryptocurrency; Digital Art and Generative-AI

The digital era has fundamentally transformed how we create, share, and profit from intellectual works. At the heart of this transformation are the concepts of **intellectual property** – **copyrights**, **patents**, and **trade secrets** – which were originally established to balance the interests of creators, inventors, and the broader public. These legal protections were ethically motivated: they aimed to reward creativity and innovation, ensuring that inventors and artists could benefit from their labor while ultimately enriching society as a whole. By granting **temporary monopolies**, societies hoped to incentivize the production of new knowledge, art, and technology, while eventually returning these works to the public domain for communal benefit.

However, as technology has evolved, so too have the ethical challenges surrounding ownership and control of ideas. Today, questions arise about the **fairness** and validity of these systems – especially when the legal owner of a creative work is not the original creator. For example, when a music label owns the rights to a song rather than the artist who composed and performed it, or when companies hold patents and trade secrets developed by employees, it prompts us to reconsider the original ethical justification for these protections. Are these arrangements still serving the public good, or have they shifted too far in favor of corporate interests? Do current laws adequately recognize the contributions of individual creators, or do they perpetuate **power imbalances** in the digital economy?

As you explore this chapter, consider:

- Who truly benefits from intellectual property laws in a digital, globalized world?
- Should the rights of creators be prioritized over those of corporations, or vice versa?
- How do emerging technologies like blockchain and generative AI challenge or reinforce traditional notions of ownership and authorship?
- What ethical responsibilities do companies have to the individuals whose innovations they profit from?

These questions invite you to critically examine not only the legal structures that govern intellectual property, but also the underlying ethical principles that justify – or challenge – them in today's rapidly changing technological landscape.

Intellectual Property

Intellectual property (IP) refers to creations of the mind – such as **inventions**, **literary and artistic works**, designs, symbols, names, and images used in commerce – that are legally protected from unauthorized use or reproduction. Unlike physical property such as real estate, vehicles, or consumable goods, intellectual property is intangible: it can be shared or copied without depriving the original owner of its use. For example, while only one person can drive a specific car or eat a particular loaf of bread at a time, an unlimited number of people could read the same digital book or listen to a song without exhausting the original asset.

The concept of ownership in intellectual property mirrors some aspects of tangible property – such as the ability to sell, license, or bequeath rights to others – but also differs in important ways. IP rights can be **transferred**, **inherited**, or **assigned**, much like physical property, allowing creators or owners to **grant permission** for use, sell their rights, or pass them on to heirs. However, the time-bound and territorial nature of most IP rights means that, unlike land or a house, these rights eventually **expire** and the protected works enter the **public domain**, becoming freely available to all.

There are also clear legal and ethical boundaries regarding what can be owned. For instance, ideas themselves, natural phenomena, and mathematical formulas are generally not subject to ownership, though their specific expressions or applications might be. This creates gray areas – such as disputes over genetic information, traditional knowledge, or the line between inspiration and infringement – where the boundaries of ownership are continually negotiated. The evolving landscape of IP law reflects ongoing debates about how best to balance private rights with public benefit in an era where intangible assets are increasingly valuable.

Patents and Copyright

Patents and **copyright** are two foundational forms of intellectual property protection, each with a long and evolving history rooted in the desire to encourage creativity and innovation. The earliest known patent-like rights date back to Ancient Greece. In medieval Europe, the concept matured: the Republic of Venice's 1474 Patent Statute is considered the first codified patent system, granting inventors exclusive rights to new devices for a limited time to encourage disclosure and public benefit. Similarly, early copyright law emerged in England with the 1710 Statute of Anne, which shifted the focus from publisher monopolies to author rights, aiming to promote learning and the progress of knowledge by granting authors exclusive rights for a limited period.

In the United States, these traditions were enshrined in the Constitution, empowering Congress to grant authors and inventors exclusive rights "for limited times" to promote the progress of science and useful arts. The first federal copyright law, enacted in 1790, protected books, maps, and charts for 14 years, renewable for another 14 years if the author was still alive. Today, U.S. patents generally last 20 years from the filing date and cannot be renewed, though certain extensions are possible in specific

cases (such as pharmaceuticals). Copyright protection for works created after January 1, 1978, typically endures for the life of the author plus 70 years. For works made for hire, anonymous, or pseudonymous works, the term is 95 years from publication or 120 years from creation, whichever is shorter. Copyrights cannot be "renewed" in the traditional sense, but older works under previous laws sometimes allowed for renewal terms.

The rapid pace of technological change raises important questions about whether these traditional time frames remain appropriate. In fields like software and digital technology, products and inventions can become obsolete within a few years, long before the expiration of a 20-year patent or multi-decade copyright. Shortening the protection period for rapidly evolving technologies could accelerate their entry into the public domain, fostering greater innovation and competition. For example, a system could be envisioned where software patents expire after 5–10 years, or where digital works have a reduced copyright term. This would allow society to benefit from shared knowledge and creative works more quickly, while still providing inventors and creators with a period of exclusive benefit. Such reforms would need to carefully balance the incentives for innovation with the broader public interest in access and progress.

Trade Secrets and National Security

Trade secrets are a powerful tool used by corporations to protect valuable information that gives them a competitive edge, such as formulas, algorithms, or business processes. Unlike patents or copyrights, which require public disclosure in exchange for legal protection, trade secrets are maintained through confidentiality and internal security measures. Famous examples include the Coca-Cola recipe and Google's search algorithm, both of which remain undisclosed to the public and are closely guarded to maintain their economic value.

However, this secrecy can sometimes conflict with the **public interest**, especially when withheld information – such as pharmaceutical data or environmental impact data – could benefit society at large. Corporations may claim trade secret status not only to protect legitimate business interests but also to avoid scrutiny or regulation, raising ethical questions about where to draw the line between proprietary knowledge and the public's right to know.

Similarly, governments often invoke "national security" as a reason to withhold information from the public, sometimes even when disclosure might serve the greater good. While there are legitimate reasons to keep certain details confidential – such as protecting citizens or critical infrastructure – the concept can be misused to obscure wrongdoing, prevent accountability, or stifle public debate. Both trade secrets and national security claims thus present a tension between the need for confidentiality and the ethical imperative for transparency. Striking the right balance is challenging: too much secrecy can erode trust and hinder oversight, while too much transparency can expose sensitive information to

misuse or harm.

These dilemmas prompt a range of critical ethical questions:

- Who gets to decide what qualifies as a trade secret or a matter of national security?
- What standards or rubrics are used to make these determinations, and are they consistent?
- How can these decisions be independently audited or reviewed to prevent abuse?
- Should there be time limits or periodic reviews for information classified as secret?
- Would greater transparency reduce the need for whistleblowers, or are some secrets always inevitable?
- How should the public interest be weighed against corporate or governmental interests in secrecy?
- What safeguards exist to ensure that claims of secrecy are not used to cover up misconduct or avoid accountability?
- Are there circumstances where the ethical imperative to disclose outweighs legal protections for secrecy?
- How can stakeholders – including employees, citizens, and regulators – challenge or appeal secrecy claims?
- What role should external watchdogs or independent panels play in overseeing decisions about secrecy?

These questions highlight the ongoing need for robust debate and oversight to ensure that trade secrets and national security claims serve the public interest rather than merely protecting private or institutional power.

Blockchain and Cryptocurrency

Blockchain technology has been promoted as a transformative solution for protecting digital assets by providing a decentralized, transparent, and tamper-resistant ledger. Unlike traditional databases, blockchain distributes records across a network of computers, making it extremely difficult to alter or erase past transactions. This architecture is seen as a major step forward in safeguarding traditional digital works – such as audio, video, and images – by ensuring clear, immutable records of ownership and provenance.

Likewise, the rise of **Non-Fungible Tokens (NFTs)** exemplifies this: NFTs are unique digital tokens on a blockchain that verify ownership and authenticity of digital items, ranging from digital art and music to virtual real estate and collectibles. For instance, an artist can mint an NFT representing a digital painting, which can then be bought, sold, or traded with its ownership history securely tracked on the blockchain. Similarly, cryptocurrencies like Bitcoin and Ethereum use blockchain to secure financial transactions, while also enabling new forms of digital property and decentralized finance.

Despite these advantages, blockchain-based asset protection is not without significant risks. One of the most critical vulnerabilities is the risk of permanent loss if a user loses access to their private wallet keys or passwords. Unlike traditional banking systems, there is no central authority to recover lost credentials, and it is estimated that up to 25% of all Bitcoin in circulation may be permanently inaccessible due to lost keys. This highlights the importance of robust key management and secure custody solutions, especially as digital assets become more valuable and widely adopted.

Additionally, while blockchain is currently considered highly secure, the advent of **quantum computing** poses a potential existential threat. Quantum computers, once they reach sufficient power – a milestone sometimes referred to as "**Q-Day**" – could theoretically break *all* of the cryptographic algorithms that underpin blockchain security, making it possible to forge transactions or steal assets. While estimates for Q-Day vary, some experts believe it could occur within the next decade, prompting urgent research into quantum-resistant **cryptography** and other safeguards to ensure the long-term viability of blockchain-based protections. As a result, while blockchain and related technologies offer powerful tools for digital asset protection and new models of ownership, they also introduce new categories of risk and uncertainty that must be carefully managed as the technology and its threats continue to evolve.

Digital Art and Generative-AI

The digital revolution has dramatically expanded the possibilities for both creating and copying art, while also blurring the boundaries between original works, forgeries, and homages. In traditional terms, a **forgery** is an unauthorized imitation of an existing work, intended to deceive by passing off as the original. In the digital realm, the distinction between a forgery and a simple **digital copy** becomes less clear, as digital files can be reproduced perfectly and infinitely. Meanwhile, an **homage** refers to a new work that deliberately references or emulates the style of a particular artist, often as a form of respect or creative exploration rather

Figure 14: Picture of Dog using ChatGPT generated by Pixlr

than deception. The challenge lies in distinguishing between these categories, especially as generative AI tools can now produce images, music, or text that closely mimic the style of well-known creators.

Technological advances in forgery detection – using AI, blockchain, and watermarking – have made it possible to analyze digital artworks for inconsistencies, provenance, and originality. Yet, even with sophisticated tools, it can be difficult to determine whether a digital piece is a genuine original, a direct copy, a forgery, or a legitimate homage, particularly when AI-generated works are involved. This ambiguity complicates questions of **ownership**: if an AI model is trained on thousands of works by a specific artist and then generates a new piece "in their style," who owns the result? Is it the person who provided the prompt, the creators of the AI tool, or the original artists whose work was used to train the model?

These complexities raise a host of ethical questions, especially when considering the perspectives of art creators, tool/platform providers, and those whose works are used as models:

- Is it ethical for AI tools to be trained on copyrighted works without the original creator’s consent?
- Should the person who provides a prompt to a generative-AI model be considered the creator or owner of the resulting artwork?
- What rights, if any, should the original artists have when their styles or works are used to train generative models?
- If a platform profits from AI-generated art, should it compensate the creators whose works were used as training data?
- How can we distinguish between homage and unauthorized imitation in the age of generative AI?
- Should digital forgeries be treated differently from physical forgeries in terms of legal and ethical consequences?
- Who is responsible if generative-AI art is used to deceive or defraud others?
- Can or should ownership of AI-generated art be transferred, inherited, or sold like traditional artworks?
- What mechanisms should exist for artists to opt in or out of having their works used as AI training data?
- How do we ensure that innovation and creative freedom are not stifled by overly restrictive ownership rules in digital and AI art?

These questions highlight the evolving landscape of digital art and generative AI, where traditional notions of authorship, authenticity, and ownership are being fundamentally reexamined.

Textbook Definitions – Intellectual Property, Digital Art, and Emerging Economies

- **intellectual property** – Creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images, that are protected by law and can be owned, transferred, or licensed.
- **copyrights** – Legal rights granted to creators for their original literary, artistic, or musical works, allowing them to control reproduction, distribution, and adaptation of those works.
- **patents** – Exclusive rights granted for new inventions, processes, or designs, giving inventors control over the use and commercialization of their inventions for a limited period.
- **trade secrets** – Confidential business information, such as formulas, practices, or processes, that provide a competitive advantage and are protected by secrecy rather than public registration.
- **temporary monopolies** – Time-limited exclusive rights granted to creators or inventors to control the use of their intellectual property, intended to incentivize innovation before works enter the public domain.
- **fairness** – The ethical principle of treating all parties justly and equitably, especially in the distribution and enforcement of rights and benefits.
- **power imbalances** – Situations where one party holds significantly more influence or control over resources, decisions, or rights than others, often leading to ethical concerns.
- **Intellectual property (IP)** – A category of property that includes intangible creations of human intellect, such as inventions, works of art, and symbols, protected by law.
- **inventions** – Novel devices, methods, or processes resulting from creativity and ingenuity, often eligible for patent protection.
- **literary works** – Original written creations, such as books, poems, and articles, protected by copyright law.
- **artistic works** – Creative visual or performance pieces, including paintings, sculptures, music, and films, covered by copyright protection.
- **transferred** – The act of legally moving ownership or rights from one party to another, such as through sale or assignment.

- **inherited** – The process by which ownership or rights are passed down from one person to another, typically upon the original owner's death.
- **assigned** – The legal transfer of rights or interests in intellectual property from one party to another, often through a formal agreement.
- **grant permission** – To authorize another party to use, reproduce, or otherwise exploit a work or invention under specified conditions.
- **expire** – To come to the end of a legally defined period of protection, after which exclusive rights are no longer enforceable.
- **public domain** – The status of a work or invention whose intellectual property rights have expired or never existed, making it freely available for public use.
- **public interest** – The welfare or well-being of the general public, often considered in legal and ethical decisions about access to information or resources.
- **Blockchain** – A decentralized, distributed digital ledger technology that records transactions securely and transparently across multiple computers.
- **Non-Fungible Tokens (NFTs)** – Unique digital tokens recorded on a blockchain that certify ownership and authenticity of a specific digital asset, such as art, music, or collectibles.
- **quantum computing** – A field of computing that uses quantum-mechanical phenomena, such as superposition and entanglement, to perform calculations far beyond the capabilities of classical computers.
- **Q-Day** – The anticipated future date when quantum computers will be powerful enough to break current cryptographic systems, potentially compromising blockchain security.
- **cryptography** – The practice and study of techniques for securing communication and information through encoding, ensuring confidentiality, integrity, and authenticity.
- **forgery** – The act of creating a false or unauthorized imitation of a work, typically with the intent to deceive others about its authenticity.
- **digital copy** – An exact reproduction of a digital file or work, which can be duplicated without loss of quality or originality.
- **homage** – A new work created in deliberate imitation or tribute to the style or influence of another artist, usually as a sign of respect rather than deception.
- **ownership** – The legal right to possess, use, control, and transfer a property or asset, including intellectual property.

11. Artificial Intelligence (AI), Automation and Robotics, and Algorithmic Ethics

Levels of AI; AI Moral Agency; Autonomous Vehicles; Chatbots; Robotics and Robot Ethics; Algorithmic Bias; Automation; Predictive Policing

The story of **automation** is one of both disruption and transformation, shaping the very fabric of society from the earliest days of agriculture to the dawn of the **Information Age**. In the **agricultural era**, simple tools and animal-driven machines revolutionized food production, freeing human labor for other pursuits. The **Industrial Revolution** brought mechanized factories and assembly lines, dramatically increasing productivity but also displacing traditional crafts and altering social structures. The advent of computers in the 20th century marked another, automating complex calculations and data management, and laying the groundwork for the digital revolution. Today, as we enter the era of **artificial intelligence (AI)**, automation, and **robotics**, the pace of change is accelerating at an unprecedented rate, touching every aspect of our economic, social, and personal lives.

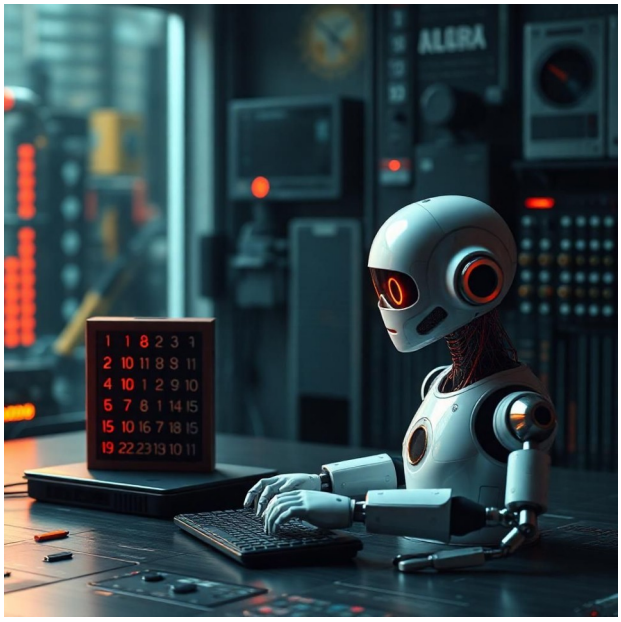


Figure 15: Robot typing at computer.

Technologies such as advanced AI, **autonomous vehicles**, **chatbots**, and robotics are no longer confined to research labs or science fiction – they are rapidly becoming integral to how we work, communicate, and make decisions. AI systems now perform tasks ranging from diagnosing medical conditions to driving cars and moderating online content. Automation is transforming industries, from manufacturing and logistics to finance and customer service, while algorithmic decision-making increasingly shapes everything from **hiring practices** to law enforcement through **predictive policing**. This growing ubiquity brings both promise and peril: while these technologies offer the potential for greater efficiency, safety, and convenience, they also raise profound ethical questions about **bias**, **accountability**, and the **distribution of power and opportunity**.

As these innovations continue to evolve, we must grapple with the **sustainability** of our current economic and social systems. Will the continued rise of AI, automation, and robotics lead to widespread **job displacement**, deepen existing inequalities, or erode **human agency**? Or can these technologies be harnessed to create a more just, equitable, and sustainable society? The answers to

these questions will depend not only on technical advancements, but also on the ethical frameworks and policies we establish to guide their development and deployment.

Levels of AI

Artificial Intelligence (AI) exists along a spectrum of complexity and capability, often described in terms of "levels." Early AI systems, such as **expert systems**, were designed to mimic the decision-making abilities of human specialists within narrow **domains** – think medical diagnosis or troubleshooting technical issues. These systems rely on **predefined rules and logic**, and while they can outperform humans in specific, well-defined tasks, they lack the flexibility and adaptability of broader intelligence. At the other end of the spectrum is **Artificial General Intelligence (AGI)**, a theoretical form of AI that can understand, learn, and apply knowledge across a wide range of tasks at a human-like level. Beyond AGI lies **Artificial Superintelligence (ASI)**, which would surpass human intelligence in virtually every field, including creativity, problem-solving, and social intelligence.

Most of what is marketed as "AI" today – such as **large language models (LLMs)** and **natural language processing (NLP)** systems – falls *far* short of AGI or ASI. These models, including popular chatbots and content generators, are trained on vast, **curated datasets** but do not actively or continuously learn from new data once deployed. Instead, they are periodically "**tuned**" by their creators, often for specific domains or applications, which can introduce or **reinforce biases** and inaccuracies present in the training data. The curated nature of these datasets means that AI outputs can reflect the perspectives, limitations, and prejudices of the data and those who select it, leading to **algorithmic bias** and fairness issues. Despite rapid advances, none of today's mainstream AI systems possess the autonomy, adaptability, or self-awareness associated with AGI.

The path to AGI – and, by extension, ASI – remains uncertain, but many experts believe that once AGI is achieved, an immediate, unavoidable and unstoppable transition to ASI will follow. Given the potential for self-improvement and **recursive learning** (without curated input, interruption, and without specified domain limitations) this prospect raises profound questions about control and safety. The assumption that AGI or ASI could be reliably "controlled" is widely regarded as hubristic, given the unpredictable nature and potential power of such systems.

Compounding these concerns is the lack of universal ethical definitions or standards in the data used to train AI, making it impossible to predict what kind of "**ethical center**" an advanced AI might develop. As a result, society faces urgent questions about how to guide the development of increasingly capable AI systems in ways that align with shared values and long-term human interests.

AI Moral Agency

Current AI systems – including expert systems, large language models, and other advanced tools – are best understood as sophisticated instruments rather than **independent moral agents**. These systems currently lack consciousness, intentionality, and the capacity for ethical judgment, so **moral agency** and **culpability** remain with the humans who design, deploy, and use them. Developers are responsible for building systems that are safe and fair, operators must ensure proper oversight, and users must understand the tool's limitations and risks. Attributing moral agency to these tools can lead to confusion, misplaced accountability, and the dangerous illusion that ethical responsibility can be delegated to technology.

The conversation shifts dramatically when considering the hypothetical emergence of Artificial General Intelligence (AGI) or Artificial Superintelligence (ASI). If an AI system were to achieve human-level understanding, autonomy, and the ability to make independent decisions (which a number of AI researchers and companies are *actively pursuing*), the question of moral agency becomes more complex and contentious. Would such a system deserve to be treated as a moral agent, or even as a legal entity, responsible for its actions?

This debate is reminiscent of the gradual transfer of moral agency from parent to child: children initially lack full moral responsibility, which is, instead, held by their parents or guardians. But as children develop autonomy and understanding, they gradually assume agency for their own actions.

Similarly, if AGI or ASI were to demonstrate genuine autonomy and ethical reasoning, there could be a case for shifting some degree of responsibility from the creators or users to the AI itself. However, this transition would be fraught with uncertainty, as we currently lack clear ethical rubrics, legal frameworks, or even a consensus on what would constitute an "ethical center" for such entities.

Autonomous Vehicles

Autonomous vehicles (AVs) are rapidly transforming transportation, with trucking and freight leading the way in the adoption of high-level autonomy. The Society of Automotive Engineers (SAE) defines six levels of vehicle autonomy, from Level 0 (no automation) to Level 5 (full automation, with no human intervention required at any point). Most consumer vehicles today feature Level 2 or Level 3 autonomy, offering driver assistance and partial automation. However, the most groundbreaking developments are occurring at Levels 4 and 5, where vehicles can operate independently in specific conditions or, eventually, in all environments.

In the United States, fully autonomous trucking is no longer a distant vision. Aurora Innovation launched driverless trucks on the I-45 corridor between Dallas and Houston in 2025. Other companies

such as Kodiak Robotics, Gatik, and Waabi are also advancing hub-to-hub autonomous trucking, particularly in states like Texas, Arizona, and Florida, where regulations are more permissive.

Internationally, China's Inceptio Technology and Germany's on-road trials are pushing the envelope in large-scale autonomous truck deployment. These trucks promise to address driver shortages, increase operational efficiency, and reduce costs, with the potential to revolutionize logistics and supply chains globally.

One of the most compelling arguments for autonomous vehicles is their potential to dramatically reduce vehicular crashes. **Human error** is responsible for over 90% of traffic accidents; by removing fatigue, distraction, and impaired driving from the equation, AVs could save thousands of lives annually.

However, the transition is not without challenges. Legal and ethical questions loom large: when an autonomous vehicle is involved in a crash, who is responsible – the manufacturer, the software developer, the fleet operator, or the owner? Current legal frameworks are struggling to keep pace, and there is ongoing debate about how to assign liability and ensure accountability as vehicles become more autonomous. These questions will only grow in importance as AV technology becomes more ubiquitous, raising fundamental issues about trust, transparency, and the future of transportation.

Chatbots

Chatbots have evolved dramatically from their origins as simple, rule-based programs designed for entertainment or to answer basic questions. Early chatbots, like ELIZA in the 1960s, relied on scripted responses and could only handle straightforward, predictable interactions. As technology advanced, chatbots became popular in business settings for providing 24/7 customer service, automating frequently asked questions, and reducing the workload for human agents. The introduction of natural language processing (NLP) and machine learning (ML) allowed chatbots to better understand context and intent, leading to more sophisticated conversational agents that could manage more complex queries. Today, chatbots are widely used not only for customer service but also for telemarketing, sales, and customer engagement, often serving as the first point of contact between companies and their customers.

Despite these advancements, significant limitations persist. Most chatbots, even those powered by large language models, are trained on curated datasets and operate within restricted domains; they struggle to adapt when conversations deviate from expected patterns, often resulting in user frustration when the system cannot process nuanced or evolving requests. Additionally, modern chatbots increasingly use synthesized voice recordings, complete with intonations and inflections, to **simulate emotion** and create a more "human-like" interaction. This can enhance user experience but also blurs the line between machine and human, raising important ethical questions:

- Is it ethical to replace human customer service jobs with chatbots, especially when the technology is still imperfect?
- Should companies be required to disclose when a customer is interacting with a chatbot rather than a real person?
- What are the risks of chatbots providing false, misleading, or "hallucinated" information to users?
- How can companies ensure that chatbots do not exploit users by establishing artificial relationships or manipulating emotions?
- Who is responsible if a chatbot causes harm, either through misinformation or inappropriate interactions?
- Should there be regulations governing the use of voice synthesis to prevent deception or emotional manipulation?
- How can biases and inaccuracies in chatbot responses be effectively identified and corrected?
- What safeguards should be in place to protect vulnerable populations from exploitation by automated systems?
- How can transparency and accountability be maintained as chatbots become more autonomous and integrated into everyday life?

These questions highlight the ethical complexities that accompany the rapid integration of chatbots into business and society, underscoring the need for thoughtful oversight and responsible development as the technology continues to advance.

Robotics and Robot Ethics

Robotics is the interdisciplinary field of engineering and computer science focused on the design, construction, operation, and use of programmable machines – robots – that can replicate, substitute, or assist human actions in various tasks. Some of the earliest robots were ancient **automata**, such as mechanical birds in ancient Greece and water clocks in China, but the modern concept of the robot emerged in the 20th century with inventions like George Devol's Unimate, the first industrial robotic arm, which began operating at a General Motors facility in 1959. The field of robotics was further defined by Isaac Asimov's introduction of the "**Three Laws of Robotics**," which have influenced ethical thinking about robots ever since.

Asimov's three laws of robotics were defined as follows:

Isaac Asimov's Three Laws of Robotics are:

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

Although begun as a work of science fiction, these three laws have become a foundational starting-point for very many philosophical and ethical positions regarding how robotics should be ethically developed and utilized.

Most industrial robots today are fully programmed using **programmable logic controllers (PLCs)** or **computer numerical control (CNC)** systems, enabling them to perform repetitive tasks such as welding, assembly, and painting within tightly controlled environments. These robots are typically limited to their pre-programmed domains and cannot adapt to new tasks without human intervention or reprogramming.

However, advances in robotics have produced machines capable of operating in more diverse and less structured environments, such as autonomous mobile robots, **manufacturing and warehouse automation** systems, and even robots that can assist in surgery or explore hazardous locations. These more advanced robots use sensors, AI, and machine learning to make decisions and adapt to changing conditions, reducing the need for direct human oversight and expanding the potential applications of robotics.

Some ethical questions raised by the increasing use of robotics include:

- What are the societal consequences of job displacement caused by robotics without corresponding changes in the existing economic model?
- Should robots be used for police or military operations, and what are the risks of delegating lethal force to machines?
- Is it ethical to use robots to administer medicines or perform medical procedures, and who is responsible if something goes wrong?
- Should robots be permitted to manufacture or design other robots, potentially accelerating automation and reducing human oversight?
- How do we ensure safety and accountability when robots operate in public or shared spaces?
- What rights, if any, should humans have to intervene in or override robot decisions in critical situations?

- How can we prevent bias or discrimination in robots programmed for social or service roles?
- Should there be universal standards or regulations for the ethical design and deployment of robots?
- How do we balance innovation with the need to protect vulnerable populations from unintended harm caused by robotics?

These questions highlight the complex ethical landscape that accompanies the rapid advancement and integration of robotics into society.

Algorithmic Bias

Algorithmic bias arises because AI systems are fundamentally shaped by the data used to train them, the domains they are intended to operate within, and the objectives set by their developers. Most AI is trained on **curated datasets** that reflect the perspectives, limitations, and sometimes the prejudices of those who collect and label the data. These models are typically fixed within a specific domain, meaning their understanding and decision-making are limited to the patterns present in their training environment. Furthermore, the **intended outcomes** – what the AI is supposed to optimize or predict – are defined in advance by the tool's creators, embedding their assumptions and priorities into the system. This results in inherent biases, which can become **self-perpetuating** as the AI consistently produces outputs that reinforce the patterns and disparities present in its training data.

Imagine a hypothetical, national healthcare system that adopts an AI-powered tool to help prioritize patients for specialist referrals. The model is trained on historical data from urban hospitals, where access to care and patient demographics differ significantly from rural areas. Because the data underrepresents rural patients and overrepresents certain ethnic groups, the AI learns to prioritize urban, majority-population patients for referrals. Over time, this bias is amplified: rural and minority patients are **systematically deprioritized**, leading to poorer health outcomes and widening existing disparities. The system's recommendations are trusted as "objective" because they come from an advanced AI, making it difficult for affected groups to challenge the results or for administrators to recognize the underlying bias.

If machine learning environments begin to "learn on their own" – continuously updating their models based on new data – the risk of algorithmic bias may become even more pronounced. Without explicit mechanisms to recognize and correct for bias, an AI could reinforce and amplify prejudices present in both its initial and ongoing data streams. How would such a system recognize that its data is incomplete or skewed? Could it ever truly understand the social and ethical context behind the data it consumes? Would it be able to distinguish between **correlation** and **causation**, or between **majority patterns** and **minority needs**? If an AI is left to self-train, who is responsible for monitoring and

correcting its outputs, and how can we ensure transparency and accountability in such a dynamic system?

These questions highlight the risk that algorithmic bias may be inevitable unless there is continuous human **oversight**, robust **auditing**, and deliberate efforts to diversify and scrutinize training data. But how will this be accomplished if the creators of the AI systems are allowed to claim 'trade secrets' or 'national security' and then withhold this information? As AI systems become more autonomous, the challenge of ensuring fairness and ethical outcomes will only grow more complex – demanding vigilance, innovation, and a commitment to equity at every stage of development and deployment.

Automation

Automation refers to the use of technology to perform tasks without human intervention, marking a fundamental shift from humans merely *using* tools to tools independently executing work. The earliest automation can be traced back to inventions like water mills and mechanical clocks, which reduced the need for constant human oversight. The Industrial Revolution accelerated this trend with machines such as the Jacquard loom and assembly line systems, which automated textile production and manufacturing processes. Over time, automation evolved from simple mechanical aids to sophisticated systems capable of performing complex, repetitive, or hazardous tasks with minimal human input.

The primary drivers for automation include improving health and safety by removing humans from dangerous environments, surpassing human physical and cognitive limitations, increasing speed and productivity, reducing fatigue and stoppages, and enhancing accuracy and consistency. Automation also allows for 24/7 operation, minimizes waste, and ensures higher quality control, all of which contribute to significant cost savings and increased profits for businesses. While these benefits are often framed in terms of operational efficiency, flexibility, and safety, they are ultimately subordinate to economic motivations: the adoption of automation is primarily justified by its potential to reduce labor costs, increase output, and boost competitiveness in the marketplace.

Today, automation extends far beyond manufacturing. In logistics, automated warehouses and self-driving delivery vehicles streamline supply chains. In healthcare, robotic surgery and automated diagnostics improve precision and efficiency. Financial services use **algorithmic trading** and automated fraud detection, while agriculture benefits from **autonomous tractors** and **drones** for planting and crop monitoring. Even creative industries are seeing automation in content generation and design.

If automation continues unchecked across all sectors, it could potentially replace most traditional forms of human employment, fundamentally challenging the status quo of the current economic model. The question remains: can our existing economic systems – rooted in wage labor and job-based income

– sustain the rapid pace of automation adoption? Or, will we need to rethink how value, work, and livelihood are distributed in a world where machines do most of the work?

Predictive Policing

Before the existence of formal laws, societies were governed by shared ethical norms – unwritten rules about right and wrong that guided individual and collective behavior. Laws and legal systems only emerged after these societal ethics were violated, requiring a codification of values into enforceable rules to maintain order and address breaches. **Policing**, as a profession and practice, arose to uphold these laws, maintain social order, and protect the community through the prevention, detection, and investigation of crime. The role of policing has always been closely tied to ethics, as officers are entrusted with significant power and discretion, and their actions can profoundly affect life, liberty, and public trust.

Policing, however, has not always been a force for good. Throughout history, the institution has been subject to abuse – ranging from **corruption** and **discrimination** to **excessive use of force** and the protection of political interests over public welfare. These abuses highlight the ongoing tension between the ideals of ethical policing – courage, respect, empathy, and public service – and the realities of institutional culture and **unchecked discretionary power**. The evolution of policing models, from crime control to social peacekeeping, reflects an ongoing struggle to balance **authority**, **accountability**, and the ethical imperative to serve the public fairly and justly.

Predictive policing is a recent development that uses algorithms and data analysis to forecast where crimes are *likely* to occur or who *might* be involved, with the aim of deploying resources more efficiently and preventing crime before it happens. Proponents argue that predictive policing can improve efficiency, reduce crime rates, and help allocate police resources more effectively. However, critics warn that these systems can amplify existing biases, lack transparency, and lead to over-policing of already marginalized communities. The risks of algorithmic bias, lack of oversight, and ethical ambiguity – discussed in previous sections – are especially acute in predictive policing, where flawed data or unchecked models can result in large-scale injustices, erode public trust, and perpetuate cycles of discrimination.

As predictive policing becomes more prevalent, the amplification of these risks could manifest in widespread surveillance, unfair targeting, and diminished civil liberties. Without rigorous ethical standards, transparency, and accountability, predictive policing could undermine the very societal values and ethical foundations that laws and policing were meant to protect.

Textbook Definitions – Artificial Intelligence (AI), Automation and Robotics, and Algorithmic Ethics

- **Automation** – The use of technology, machines, or systems to perform tasks with minimal or no human intervention, streamlining processes and increasing efficiency.
- **Information Age** – The current era characterized by the rapid transmission, processing, and accessibility of information through digital technology and computing.
- **agricultural era** – A historical period when societies were primarily based on farming and the cultivation of crops and livestock.
- **Industrial Revolution** – The period of major industrialization during the late 18th and early 19th centuries marked by the shift from hand production to machines and factory systems.
- **artificial intelligence (AI)** – The development of computer systems capable of performing tasks that typically require human intelligence, such as reasoning, learning, and problem-solving.
- **Robotics** – The branch of technology that deals with the design, construction, operation, and application of robots to perform automated tasks.
- **Autonomous vehicles (AVs)** – Vehicles equipped with technology that enables them to navigate and operate without direct human control.
- **Chatbots** – Software applications that simulate human conversation using text or voice, often for customer service or information retrieval.
- **hiring practices** – The methods and criteria organizations use to recruit, select, and employ personnel.
- **Predictive policing** – The use of data analysis and algorithms to forecast potential criminal activity and inform law enforcement strategies.
- **bias** – A systematic inclination or prejudice in favor of or against certain outcomes, groups, or data, often leading to unfair or inaccurate results.
- **accountability** – The obligation to explain, justify, and take responsibility for one's actions or decisions.
- **distribution of power and opportunity** – The way authority, resources, and chances for advancement are allocated among individuals or groups in a society.
- **sustainability** – The capacity to maintain or support processes, systems, or resources over the long term without depleting them.

- **job displacement** – The loss of employment opportunities due to technological change, automation, or other factors.
- **human agency** – The capacity of individuals to act independently and make their own free choices.
- **expert systems** – Computer programs that emulate the decision-making abilities of human experts in specific domains using predefined rules.
- **domains** – Specific areas of knowledge, activity, or expertise within which a system or individual operates.
- **predefined rules and logic** – Explicitly programmed instructions and decision criteria that govern the behavior of a system or process.
- **Artificial General Intelligence (AGI)** – A theoretical form of AI capable of understanding, learning, and applying knowledge across a wide range of tasks at a human-like level.
- **Artificial Superintelligence (ASI)** – A hypothetical AI that surpasses human intelligence in all respects, including creativity, reasoning, and problem-solving.
- **large language models (LLMs)** – Advanced AI models trained on extensive text data to generate, summarize, and understand human language.
- **natural language processing (NLP)** – The field of AI focused on enabling computers to interpret, process, and generate human language.
- **curated datasets** – Carefully selected and organized collections of data used to train or evaluate AI models.
- **tuned** – Adjusted or refined by developers to improve a model's performance or adapt it to specific tasks or domains.
- **reinforce biases** – To perpetuate or amplify existing prejudices or patterns present in training data through repeated outputs.
- **Algorithmic bias** – Systematic and repeatable errors in AI outputs that result from biases in the data, design, or implementation of algorithms.
- **recursive learning** – A process where AI systems iteratively update and improve themselves by learning from their own outputs or new data.
- **ethical center** – The core set of moral principles or values that guide decision-making and behavior in an individual or system.

- **independent moral agents** – Entities capable of making ethical decisions and being held responsible for their actions without external control.
- **moral agency** – The ability to discern right from wrong and to be held accountable for one's actions.
- **culpability** – The degree to which an individual or entity is responsible for a fault or wrong.
- **Human error** – Mistakes or failures in judgment, perception, or action made by people, often leading to unintended consequences.
- **simulate emotion** – The act of mimicking or reproducing emotional expressions or responses using technology.
- **automata** – Self-operating machines or mechanisms, often designed to follow a predetermined sequence of operations.
- **Three Laws of Robotics** – A set of ethical rules devised by science fiction writer Isaac Asimov to govern the behavior of robots.
- **programmable logic controllers (PLCs)** – Industrial digital computers used to control manufacturing processes or machinery.
- **computer numerical control (CNC)** – The automated control of machining tools and 3D printers by means of a computer.
- **manufacturing and warehouse automation** – The use of automated systems and robots to perform tasks in production and storage facilities with minimal human involvement.
- **intended outcomes** – The specific goals or results that a system or process is designed to achieve.
- **self-perpetuating** – Capable of continuing or reinforcing itself without external input or intervention.
- **systematically deprioritized** – Consistently assigned lower importance or priority in a structured or organized manner.
- **correlation** – A statistical relationship or association between two or more variables.
- **causation** – The action of causing something to happen; a direct cause-and-effect relationship.
- **majority patterns** – Trends or behaviors that are most common within a given dataset or population.
- **minority needs** – The specific requirements or interests of less-represented groups within a population.

- **oversight** – The act of supervising, monitoring, or regulating processes or organizations to ensure proper conduct.
- **auditing** – The systematic examination and evaluation of processes, systems, or data to ensure accuracy, compliance, and integrity.
- **algorithmic trading** – The use of computer algorithms to automatically execute financial trades at high speed and volume.
- **autonomous tractors** – Self-driving agricultural vehicles capable of performing tasks such as plowing, planting, and harvesting without human intervention.
- **drones** – Unmanned aerial vehicles operated remotely or autonomously for various purposes, including surveillance, delivery, and data collection.
- **Policing** – The activities and responsibilities of maintaining public order, enforcing laws, and preventing and investigating crime.
- **corruption** – Dishonest or unethical conduct by those in power, typically involving bribery or the abuse of authority for personal gain.
- **discrimination** – Unfair or prejudicial treatment of individuals or groups based on characteristics such as race, gender, or age.
- **excessive use of force** – The application of more physical power than is necessary or justified in a given situation, often by law enforcement.
- **unchecked discretionary power** – Authority exercised without sufficient oversight, limits, or accountability, increasing the risk of abuse.
- **authority** – The legitimate power to make decisions, enforce rules, and command obedience.
- **accountability** – The requirement to answer for one's actions and decisions, especially in positions of power or responsibility.

12. Bioethics and Human Enhancement

Genetic Engineering and CRISPR; Human Augmentations; Neuroethics and Brain-Computer Interfaces; Biotechnology; Cloning

From the earliest days of recorded history, humans have striven to overcome injury, disease, and the limitations imposed by nature. Ancient civilizations developed rudimentary forms of **medicine**, using **herbal remedies**, ritualistic healing, and early surgical techniques to treat wounds and illnesses. Over centuries, the figure of the healer evolved into the **professional doctor**, as societies formalized the study of **anatomy**, **pharmacology**, and **hygiene**. The establishment of medical institutions and the codification of ethical standards, such as the original **Hippocratic Oath** as well as the current versions as it has evolved over the years, marked significant milestones in the professionalization of medicine. These advancements, coupled with improvements in **sanitation**, **nutrition**, and **public health**, contributed to dramatic increases in birth rates and steadily rising life expectancies across much of the world.

In the modern era, the fusion of medicine and technology has ushered in a new age of **diagnostics** and **treatment**. Innovations such as **magnetic resonance imaging (MRI)**, **robotic-assisted surgery**, **gene sequencing**, and targeted therapies have become accessible – and even commonplace – in many developed regions. These breakthroughs have enabled earlier detection of disease, more precise interventions, and improved outcomes for patients. Technologies like **wearable health monitors**, **telemedicine** platforms, and **personalized medicine** are reshaping the patient experience, making healthcare more efficient and, in some cases, more equitable. Yet, these advances are not uniformly distributed, and significant disparities in access to care persist both within and between nations.

Today, the frontier of technology and human biology is rapidly expanding *beyond* traditional treatment. Emerging capabilities in **genetic engineering** allow for the possibility of *designing* offspring with selected traits, raising profound ethical questions about **autonomy**, **consent**, and the very definition of humanity. **Human augmentation** – whether through biological enhancements, **neural interfaces**, or **hybrid bio-robotic systems** – challenges our understanding of ability, identity, and fairness. **Cloning** and advanced biotechnologies further blur the boundaries between natural and artificial life. These developments amplify longstanding issues of ethics and equity, as access to cutting-edge interventions often remains limited by socioeconomic status, geography, and policy. As we look to the future, society must grapple with how to ensure that the benefits of bioethical innovation are shared broadly, while safeguarding individual rights and addressing the risks of deepening inequality.

Genetic Engineering and CRISPR

For millennia, humans have shaped the natural world through **selective breeding** and **cross-breeding**, long before the discovery of **DNA** or the advent of modern biotechnology. Early agriculturalists learned to cultivate plants and animals with desirable traits – such as higher yields, resistance to disease, or improved taste – by intentionally mating individuals that exhibited these characteristics. **Hybridization**, the crossing of different species or varieties, produced vigorous new crops like hybrid grains and apples, while grafting and cloning techniques allowed for the propagation of seedless fruits such as bananas and larger, juicier varieties of produce. The transformation of wild teosinte (a Mexican grass) into modern maize (corn) is a striking example of how traditional breeding practices could fundamentally alter a species over generations. Similarly, the development of hybrid corn in the early 20th century revolutionized agriculture by increasing crop productivity.

As scientific understanding deepened, especially following the discovery of DNA's structure, genetic manipulation became more precise. By the mid-20th century, plant breeders were using radiation and chemicals to induce **random mutations**, further expanding the genetic toolkit available for crop improvement. The real turning point came in the 1970s, when researchers developed techniques to directly modify DNA – splicing genes from one organism into another, regardless of species boundaries. Early successes included the creation of recombinant bacteria and the first genetically modified plants, such as tobacco engineered for antibiotic resistance. In animals, transgenic mice paved the way for more complex genetic research and applications.

The mapping of the human genome at the turn of the 21st century marked a watershed moment, providing a comprehensive blueprint of human genetic information. This achievement set the stage for the development of **CRISPR**, a revolutionary gene-editing technology that allows scientists to precisely "cut and paste" sections of DNA within living organisms. Today, CRISPR is being used in a wide range of applications – from developing disease-resistant crops and livestock to exploring potential cures for genetic disorders in humans. Researchers are even investigating the possibility of resurrecting extinct species by editing the genomes of living relatives.

As we have done previously, let's consider some ethical questions surrounding the concepts of genetic engineering:

- Who should decide which genetic traits are considered "normal," "desirable," or "disorders" when it comes to genetic engineering in humans, plants, or animals?
- Is it ethical to use gene editing technologies like CRISPR for human enhancement (such as increasing intelligence or physical ability), rather than solely for treating diseases?
- How can society ensure fair and equitable access to genetic engineering technologies, so that benefits are not limited to the wealthy or privileged?

- What are the potential long-term and unintended consequences of editing the human genome, given that changes could be passed to future generations who cannot consent?
- Should it be permissible to patent genetically engineered organisms, genes, or gene-editing techniques, and what are the implications for intellectual property, innovation, and access?
- How might widespread use of gene editing affect societal acceptance of people with disabilities or differences, and could it lead to new forms of discrimination or **eugenics**?
- What responsibilities do scientists and companies have to ensure **transparency**, **informed consent**, and **environmental stewardship** when releasing genetically engineered organisms into the environment?
- Is it morally acceptable to genetically engineer animals for human benefit, such as for food production or medical research, and what are the welfare considerations for these animals?
- Where should the line be drawn between **therapeutic** uses of genetic engineering and non-therapeutic, **elective**, or **cosmetic** applications?
- How should regulatory frameworks evolve to address the rapid pace of genetic engineering technology, especially given current ambiguities in law and policy?

Legal and ethical frameworks have struggled to keep pace with these rapid advancements. In the United States, it was once legal to patent isolated human genes, a practice that sparked significant controversy over ownership and access to genetic information. However, a 2013 Supreme Court decision ruled that naturally occurring human genes could not be patented, though synthetic DNA (cDNA) remains patentable. The legal landscape for genetic engineering in plants, animals, and humans remains ambiguous, with regulations varying widely by country and often lagging behind technological capabilities. This uncertainty raises pressing questions about equity, access, and the responsible use of genetic technologies as society moves deeper into the era of bioengineering.

Human Augmentations

Throughout history, humans have sought ways to restore lost function and even enhance their bodies, as evidenced by archaeological discoveries of ancient **prosthetics** and artificial enhancements. Remains from ancient Egypt reveal prosthetic toes dating back nearly 3,000 years, crafted from wood and leather, suggesting both practical and possibly symbolic purposes. In China, a 2,200-year-old man of modest means was discovered having a prosthetic leg made from poplar wood, ox horn, and horse hoof. This limb was designed to help its owner – who suffered from a fused knee – walk more easily. Similarly, in medieval Europe, prosthetic hands and legs have been unearthed, some simple and

functional, others more elaborate, reflecting both the medical ingenuity of the time and the social significance attached to bodily integrity and appearance.

These early prosthetics were primarily functional, aiming to restore lost mobility or utility. However, some may have also served as markers of status, identity, or resilience, particularly when crafted with care or adorned with valuable materials. Over centuries, the evolution of prosthetic technology has mirrored advances in materials science, medicine, and engineering – from wood and metal devices fastened with leather straps to today's lightweight **carbon fiber** limbs and sophisticated **bionic prosthetics** that can be controlled by **neural signals**.

Modern human augmentation has moved beyond mere replacement of lost function. Today's prosthetics can not only restore, but also enhance, physical abilities – sometimes surpassing what is considered "normal" human performance. Athletes with advanced **running blades**, for example, challenge conventional definitions of ability and fairness. **Neural implants**, **exoskeletons**, and **sensory enhancements** are pushing the boundaries of what it means to be human, raising profound questions about identity, equity, and the future of human evolution.

Consider these ethical questions surrounding the topic of human augmentation:

- Should there be limits on augmentations that enhance abilities beyond the typical human range, such as strength, speed, or cognition?
- Who should have access to advanced augmentations – should they be available to all, or only to those who can afford them?
- Could widespread augmentation create new forms of inequality or discrimination between "augmented" and "non-augmented" individuals?
- How should society regulate the use of neural implants or brain-computer interfaces that could alter **thought**, **memory**, or **personality**?
- If a person replaces most or all of their biological body with artificial parts, are they still the same person – philosophically or legally?
- Should children be allowed or required to receive certain augmentations to compete or participate in society?
- What responsibilities do designers and manufacturers have if an augmentation malfunctions or is hacked?
- How might human augmentation affect the value society places on natural abilities or disabilities?

- Should employers or governments be allowed to require or incentivize certain augmentations for work or public service?
- What rights and protections should individuals have regarding the data generated by their augmented bodies?

This last set of questions echoes the ancient philosophical thought experiment known as the Ship of Theseus: if every board of a ship is replaced over time, is it still the same ship? Applied to human augmentation, if all parts of a person are gradually replaced with artificial components, does their identity persist – or does something fundamentally change? This debate sits at the heart of the ethical, legal, and existential challenges posed by the future of human enhancement.

Neuroethics and Brain-Computer Interfaces

Neuroethics and **brain-computer interfaces (BCIs)** represent one of the most rapidly evolving frontiers in both neuroscience and technology. At the core of this field are neurological sensors, which can be broadly categorized as active or passive. **Active sensors**, such as deep brain stimulators and **implanted electrodes**, not only record neural activity but can also deliver electrical stimulation to targeted brain regions. **Passive sensors**, including **electroencephalography (EEG)** caps and **functional MRI (fMRI)**, non-invasively monitor the brain's electrical or metabolic activity for diagnostic and research purposes. These technologies have become invaluable in understanding neurological disorders, mapping brain function, and developing treatments for conditions such as epilepsy, Parkinson's disease, and severe paralysis.

Figure 16: Exaggeration of brain-computer-interface

Brain-computer interfaces leverage these advances to create direct communication pathways between the brain and external devices. The most promising use cases include restoring movement or communication for individuals with paralysis, enabling control of prosthetic limbs, and providing new ways for people with severe disabilities to interact with the world. BCIs are also being explored for **cognitive enhancement**, mental health interventions, and even immersive gaming experiences. The ability to decode neural signals and translate them into digital commands holds transformative potential for medicine, rehabilitation, and human-computer interaction.

However, the scale and complexity of data collected by neurological sensors and BCIs present significant challenges. Current technology cannot isolate individual thoughts or intentions with

precision; instead, it captures vast streams of brain activity, resulting in the collection of far more data about a person than is necessary for a specific research or clinical goal. This phenomenon mirrors broader concerns previously discussed in the chapter on *Privacy, Surveillance, and Data Ethics*. In that chapter we discussed how 'big data', the aggregation and analysis of massive datasets, can inadvertently expose sensitive personal information, create privacy risks, and lead to unintended uses of data. Just like with big data, the capture, storage, and analysis of neurological data repeats the same ethical concerns which include informed consent, data ownership, potential misuse of neural data, and the risk of surveillance or discrimination based on brain activity patterns.

Neuralink, a leading company in the BCI space, has recently achieved a major milestone by successfully implanting its "Telepathy" device in a human subject. This coin-sized implant uses ultra-fine threads equipped with thousands of electrodes to record neural activity at a high resolution. The device has demonstrated the ability to detect neuron spikes and correlate brain signals with **intended motor actions**, allowing users to control computers or external devices directly through thought. Neuralink's approach combines advanced neurosurgical robotics for precise implantation with custom electronics that process and transmit **neural data**. Neuralink is currently engaged in human trials, offering hope for individuals with severe neurological conditions and opening new possibilities for human-computer integration.

Here, again, are several ethical questions surrounding neuroethics and BCIs:

- To what extent could brain-computer interfaces (BCIs) be used to read or decode private thoughts and memories, and what safeguards should be in place to protect mental privacy?
- If a BCI could send signals to the brain that override or contradict a person's intended actions (such as controlling movement or behavior), who is responsible for the outcome, and how should consent be managed?
- What ethical concerns arise if technology advances to the point where data can be written to the brain – potentially altering memories, perceptions, or even personality traits – rather than just reading from it?
- How can individuals maintain autonomy and freedom of thought in a future where neurotechnology might make it possible for others to access or influence their mental states?
- Should there be limits on the collection and analysis of neural data, given that current BCIs capture far more information than is needed for specific tasks, raising big-data privacy and consent issues?
- In the event of a malfunction, hack, or unauthorized access to a BCI, what protections and recourse should users have if their thoughts or actions are affected without their consent?

- How should society address the possibility of BCIs being used for enhancement or manipulation, such as boosting cognitive abilities or influencing decisions, especially if access is unequal or coerced?

As BCI technology advances, the ethical landscape will require ongoing scrutiny, balancing the immense potential for benefit with the need to protect individual rights and societal values.

Biotechnology

Biotechnology is a broad field that encompasses the use of living organisms, cells, and biological systems to develop products and processes that benefit society. Many of the topics previously discussed – such as genetic engineering, CRISPR, brain-computer interfaces, and bioethics – are all integral parts of the biotechnology landscape. However, the reach of biotechnology extends even further, touching on a range of emerging technologies and applications that are reshaping medicine, agriculture, industry, and environmental management.

Beyond gene editing and medical diagnostics, biotechnology now includes advanced innovations like **nanotechnology** for direct cell repair and targeted cancer therapies. Nanotech-enabled particles can be engineered to seek out and destroy cancer cells without harming healthy tissue, offering more precise and less invasive treatments. In addition, biotechnology has enabled the development of **bioengineered organisms** – microbes or plants designed to clean up pollution through processes like **bioremediation** and **phytoremediation**. These organisms can break down toxic substances in soil and water, helping to restore contaminated environments and improve public health.

Another rapidly growing area is the production of **bio-printed** or lab-grown food. Using 3D printing technology and cell culture techniques, scientists can now create meat, organs, and other tissues in the lab, potentially reducing the environmental impact of traditional agriculture and providing new sources of nutrition. This technology is also being explored for medical applications, such as printing skin, bone, or even entire organs for transplantation.

While the benefits of biotechnology are substantial, significant risks and uncertainties remain. One major concern is the possibility of **unintended release** of engineered organisms or nanotech agents into the environment. Once released, these entities may not be easily converted from active to dormant or inert states, raising fears about long-term ecological impacts or the creation of new, hard-to-control forms of pollution. The microscopic or nanoscale nature of many biotech interventions also makes transparency and oversight difficult, complicating efforts to monitor their behavior and effects.

For example, bioengineered microbes used to clean up oil spills or toxic waste could themselves become hazardous if they mutate or interact with other organisms in unexpected ways. While the pros of such applications include cleaner water and soil, the cons may involve the organisms becoming toxic

to humans or disrupting local ecosystems. Similarly, lab-grown foods promise sustainability and food security, but raise questions about safety, labeling, and the social and economic impacts on traditional farming communities.

Biotechnology is revolutionizing how we approach health, food, and environmental challenges, but it also demands careful consideration of the risks, especially regarding safety, transparency, and long-term sustainability. As these technologies become more integrated into daily life, ongoing ethical, legal, and societal debates will be essential to ensure they are used responsibly and equitably.

Cloning

Cloning, as a concept, has long fascinated humanity, appearing in ancient myths, literature, and modern entertainment as the idea of creating identical copies of organisms. The scientific journey toward cloning began in the late 19th century, when researchers like Hans Driesch demonstrated artificial embryo twinning in sea urchins, showing that separated embryonic cells could each develop into whole organisms. In the 20th century, landmark experiments included the cloning of frogs by nuclear transfer in the 1950s and the cloning of mammals from embryonic and adult cells in the 1980s and 1990s. The most famous breakthrough came in 1996 with the birth of Dolly the sheep, the first mammal cloned from an adult somatic cell, announced by Ian Wilmut and his team at the Roslin Institute in Scotland. Dolly's creation proved that specialized adult cells could be reprogrammed to create an entire organism, igniting both scientific excitement and ethical debate. Other notable milestones include the cloning of cows, cats, and even monkeys, as well as the cloning of animals for agriculture, research, and pet reproduction.

Attempts at human cloning have been more controversial and less successful. In 2001, scientists at Advanced Cell Technology in Massachusetts cloned human embryos for the first time, aiming for therapeutic rather than reproductive purposes. In 2013, a team led by Shoukhrat Mitalipov achieved a breakthrough in human cloning by creating embryonic stem cells from cloned human embryos. While some fringe groups and individuals have claimed to have cloned humans, there is no verified scientific evidence of a live human clone. News of human cloning efforts has generally been met with skepticism and concern within the scientific and medical communities, and has sparked strong opposition from religious, ethical, and political groups around the world. Reactions have ranged from moral outrage and calls for bans to cautious support for therapeutic cloning aimed at treating disease.

Currently, **human reproductive cloning** is illegal or heavily restricted in the United States and many other countries. **Therapeutic cloning** – using cloned embryos to derive stem cells for research or medical treatment – remains a gray area, with regulations varying by state and ongoing debates about its ethical and legal status. The technology continues to raise profound questions about identity, individuality, and the boundaries of human intervention in nature.

Consider these ethical questions surrounding the concept of cloning:

- Is it ethical to create a human clone for reproductive purposes, knowing the potential risks and uncertainties involved?
- Should cloning be allowed for therapeutic purposes, such as generating tissues or organs for transplantation?
- What rights and status would a human clone have in society – would they be treated as individuals or property?
- Could the widespread use of cloning undermine the value of genetic diversity or lead to new forms of discrimination?
- How should society regulate or oversee cloning technology to prevent abuse or unintended consequences?
- Would the existence of human clones challenge traditional notions of family, parenthood, and identity?
- What are the long-term psychological and social impacts on clones and their families?

Textbook Definitions – Bioethics and Human Enhancement

- **medicine** – The science and practice of diagnosing, treating, and preventing disease and injury in humans.
- **herbal remedies** – Treatments derived from plants and plant extracts used for their medicinal properties.
- **professional doctor** – A person formally trained and licensed to practice medicine and provide healthcare.
- **anatomy** – The study of the structure of living organisms, especially their internal systems and organs.
- **pharmacology** – The branch of medicine concerned with the study of drugs and their effects on the body.
- **hygiene** – Practices and conditions that promote health and prevent disease, especially through cleanliness.
- **Hippocratic Oath** – An ancient ethical code historically taken by physicians, emphasizing medical ethics and patient care. The current accepted version of this oath (as of 2017) is:

    - AS A MEMBER OF THE MEDICAL PROFESSION:
        - I SOLEMNLY PLEDGE to dedicate my life to the service of humanity;
        - THE HEALTH AND WELL-BEING OF MY PATIENT will be my first consideration;
        - I WILL RESPECT the autonomy and dignity of my patient;
        - I WILL MAINTAIN the utmost respect for human life;
        - I WILL NOT PERMIT considerations of age, disease or disability, creed, ethnic origin, gender, nationality, political affiliation, race, sexual orientation, social standing or any other factor to intervene between my duty and my patient;
        - I WILL RESPECT the secrets that are confided in me, even after the patient has died;
        - I WILL PRACTICE my profession with conscience and dignity and in accordance with good medical practice;
        - I WILL FOSTER the honor and noble traditions of the medical profession;
        - I WILL GIVE to my teachers, colleagues, and students the respect and gratitude that is their due;
        - I WILL SHARE my medical knowledge for the benefit of the patient and the advancement of healthcare;
        - I WILL ATTEND TO my own health, well-being, and abilities in order to provide care of the highest standard;
        - I WILL NOT USE my medical knowledge to violate human rights and civil liberties, even under threat;
        - I MAKE THESE PROMISES solemnly, freely, and upon my honor.

- **sanitation** – Measures and practices that maintain cleanliness and prevent the spread of disease, especially through waste management.
- **nutrition** – The process by which living organisms obtain and use food to support growth, health, and maintenance.
- **public health** – The science and practice of protecting and improving the health of communities through education, policy, and preventive measures.
- **diagnostics** – Techniques and tools used to identify diseases or medical conditions in individuals.
- **treatment** – Medical care or intervention given to manage or cure illness or injury.
- **magnetic resonance imaging (MRI)** – A non-invasive imaging technique that uses magnetic fields and radio waves to create detailed images of internal body structures.
- **robotic-assisted surgery** – Surgical procedures performed with the aid of robotic systems to enhance precision and control

- **gene sequencing** – The process of determining the exact order of nucleotides in a DNA molecule.
- **wearable health monitors** – Electronic devices worn on the body that track health metrics such as heart rate, activity, or sleep.
- **telemedicine** – The remote diagnosis and treatment of patients using telecommunications technology.
- **personalized medicine** – Medical care tailored to an individual's genetic, environmental, and lifestyle factors.
- **genetic engineering** – The direct manipulation of an organism's DNA to alter its characteristics or functions.
- **autonomy** – The right or condition of self-government, especially in making informed decisions about one's own body and health.
- **consent** – Permission for something to happen or agreement to do something, especially after being informed of the risks and benefits.
- **Human augmentation** – The use of technology to enhance or extend human physical or cognitive abilities.
- **neural interfaces** – Devices or systems that enable direct communication between the brain and external devices.
- **hybrid bio-robotic systems** – Integrated systems combining biological and robotic components to enhance function or performance.
- **Cloning** – The process of producing genetically identical copies of an organism, cell, or DNA sequence.
- **selective breeding** – The intentional mating of organisms with desirable traits to produce offspring with those traits.
- **cross-breeding** – The process of mating individuals from different breeds or species to produce hybrid offspring.
- **DNA** – Deoxyribonucleic acid, the molecule that carries genetic information in living organisms.
- **Hybridization** – The process of combining different varieties or species to produce a hybrid with traits from both parents.

- **random mutations** – Unplanned changes in DNA that can result in new traits or variations in organisms.
- **CRISPR** – A gene-editing technology that allows precise modifications to DNA sequences in living organisms.
- **eugenics** – The controversial practice or belief in improving the genetic quality of a human population through selective breeding or genetic intervention.
- **transparency** – Openness and clarity about processes, decisions, and data, especially in science and ethics.
- **informed consent** – The process of providing individuals with sufficient information to make knowledgeable decisions about participation in medical or research activities.
- **environmental stewardship** – The responsible management and care of the environment and natural resources.
- **therapeutic** – Intended to heal or treat disease or medical conditions.
- **elective** – Chosen or optional, especially referring to medical procedures that are not medically necessary.
- **cosmetic** – Intended to improve appearance rather than health or function.
- **prosthetics** – Artificial devices that replace missing body parts to restore function or appearance.
- **carbon fiber** – A strong, lightweight material commonly used in advanced prosthetics and other high-performance applications.
- **bionic prosthetics** – Artificial limbs or devices enhanced with electronic or mechanical components to mimic or surpass natural function.
- **neural signals** – Electrical impulses generated by neurons that transmit information within the nervous system.
- **running blades** – Curved, spring-like prosthetic limbs designed to enable or enhance running performance.
- **Neural implants** – Devices surgically placed in the brain or nervous system to restore or enhance function.
- **exoskeletons** – Wearable robotic frameworks that support or augment human movement and strength.

- **sensory enhancements** – Technologies or interventions that improve or extend human sensory perception.
- **thought** – A mental process involving ideas, reasoning, or imagination.
- **memory** – The mental capacity to store, retain, and recall information or experiences.
- **personality** – The combination of characteristics or qualities that form an individual's distinctive character.
- **Neuroethics** – The study of ethical, legal, and social issues arising from neuroscience and neurotechnology.
- **brain-computer interfaces (BCIs)** – Systems that enable direct communication between the brain and external devices, often for control or interaction.
- **Active sensors** – Devices that both detect and interact with biological signals, often by sending or receiving electrical impulses.
- **implanted electrodes** – Electrodes surgically placed in the body or brain to monitor or stimulate neural activity.
- **Passive sensors** – Devices that detect and record biological signals without actively interacting with the system.
- **electroencephalography (EEG)** – A non-invasive method for recording electrical activity of the brain using electrodes placed on the scalp.
- **functional MRI (fMRI)** – An imaging technique that measures brain activity by detecting changes in blood flow.
- **cognitive enhancement** – The use of technology or interventions to improve mental functions such as memory, attention, or intelligence.
- **intended motor actions** – Movements or actions that a person consciously plans or attempts to perform.
- **neural data** – Information collected from the nervous system, especially brain activity signals.
- **Biotechnology** – The use of living organisms, cells, or biological systems to develop products and technologies for human benefit.
- **nanotechnology** – The manipulation and application of materials at the molecular or atomic scale, often for medical or technological purposes.
- **bioengineered organisms** – Living organisms whose genetic material has been deliberately modified for specific purposes.

- **bioremediation** – The use of living organisms, such as microbes or plants, to clean up environmental pollutants.
- **phytoremediation** – The use of plants to absorb, remove, or neutralize contaminants from soil or water.
- **bio-printed** – Created using 3D printing techniques with biological materials, often for medical or food applications.
- **unintended release** – The accidental escape or spread of engineered organisms or substances into the environment.
- **human reproductive cloning** – The creation of a human being that is genetically identical to another individual through cloning techniques.
- **Therapeutic cloning** – The creation of cloned embryos for the purpose of generating stem cells for medical research or treatment.

13. Technological Disruption and the Paradox of Progress

Obsolescence – Planned vs. Inevitable; Tech Lock-In and 3D Printing; AR/VR & Tech Progress; Erosion of Economic Sustainability

Throughout history, the greatest leaps forward in human civilization have often been catalyzed by **technological disruption**. From the invention of the printing press, which democratized knowledge and upended centuries-old power structures, to the assembly line that revolutionized manufacturing and made goods accessible to millions, each wave of innovation has brought both profound progress and significant upheaval.

These disruptions are rarely met with universal enthusiasm; while some individuals and industries embrace, adopt, and expand upon new technologies, others resist, fearing loss of livelihood, status, or control. The introduction of the personal computer, for example, was welcomed by early adopters and visionaries but met skepticism by those invested in mainframe computing or manual record keeping. Similarly, the rapid rise of the Internet in the 1990s transformed everything from commerce to communication, sparking both excitement and anxiety about its societal implications.

Looking back at the past 50 to 75 years, many of the most notable disruptions align with the topics explored in earlier chapters. The **digital revolution** – driven by personal computers, the Internet, and later, mobile devices – has fundamentally altered how we work, learn, and connect. Advances in genetics and biotechnology, such as the mapping of the human genome and the development of CRISPR, have opened new frontiers in medicine and ethics. The rise of artificial intelligence, automation, and robotics has transformed industries, from manufacturing to healthcare, while also raising concerns about job displacement and algorithmic bias. In recent years, technologies like **3D printing**, **spatial computing**, and **wearable and embedded devices** have further blurred the boundaries between the physical and digital worlds, creating new opportunities and challenges.

A defining feature of modern technological disruption is its exponential, rather than linear, rate of change. Innovations that once took decades to diffuse now reach global scale in a matter of years – or even months. The **adoption curve** for technologies like smartphones, streaming services, and generative AI has been breathtakingly steep, leaving little time for societies to adapt before the next wave arrives. As we stand on the cusp of further disruption, the window between major breakthroughs grows ever shorter, and the potential impacts – both positive and negative – become more profound.

Looking to the near horizon, several major technological breakthroughs seem poised to reshape our world. These may include:

- Widespread deployment of advanced AI systems capable of autonomous decision-making in critical sectors.

- Quantum computing breakthroughs that render current encryption obsolete and enable new scientific discoveries.
- Scalable, affordable bioengineering solutions for disease treatment, food production, and environmental restoration.
- Mainstream adoption of brain-computer interfaces, enabling direct neural interaction with digital systems.
- The rise of fully immersive spatial computing environments, transforming work, education, and entertainment.
- Next-generation energy technologies, such as fusion or advanced battery storage, that could disrupt global energy markets.

The paradox of progress is that while technological disruption drives unprecedented advancement, it also brings new challenges – **planned and inevitable obsolescence**, **tech lock-in**, erosion of economic participation, and environmental consequences – that demand thoughtful navigation in the decades ahead.

Obsolescence – Planned vs. Inevitable

The story of technological progress is often told through the lens of **obsolescence**, where each new leap forward renders a previous standard obsolete: the abacus gave way to the calculator, which was then eclipsed by the computer; buggy-whips disappeared as automobiles replaced horse-drawn carriages, soon followed by windshield wipers as standard equipment; the telegraph was overtaken by telephones, which themselves have been transformed by digital and VoIP communication; vinyl records yielded to cassette tapes, then CDs, and now streaming audio; and film cameras faded as digital photography became the norm. Each of these transitions highlights how new technologies not only replace old ones but also reshape industries, economies, and daily life.

Inevitable obsolescence is a natural byproduct of technological disruption, as newer, better, or more efficient solutions emerge and make older versions less useful or even unserviceable. This cycle is accelerating, with product and component life cycles growing shorter as innovation speeds up and consumer expectations rise. The ethical implications of this relentless churn are complex.

While much attention is paid to job displacement and the need to support those affected by disruption, a deeper question arises: should our ethical frameworks focus solely on preserving the status quo, or should they also empower us to reimagine the very structure of work, value, and participation in society? As automation and AI threaten to upend traditional employment models, it

may be time to challenge the assumption that widespread employment is the only path to economic security and personal fulfillment.

In response to the threat of inevitable obsolescence, some businesses have adopted the strategy of **planned obsolescence** – intentionally designing products with limited lifespans or incremental improvements to encourage repeated purchases and maintain brand relevance. This approach allows companies to attempt to control the *pace* of change and manage consumer expectations, but it also raises ethical concerns about waste, resource use, and consumer manipulation. Ultimately, the interplay between inevitable and planned obsolescence shapes not only the technology landscape but also the broader social and ethical context in which innovation unfolds.

Tech Lock-In and 3D Printing

As a facet of planned obsolescence, many companies have increasingly adopted the practice of **tech lock-in** – designing products and systems that require vendor-specific components, consumables, or software, and sometimes even restricting or disabling functionality to ensure ongoing customer dependence. Classic examples include printer manufacturers requiring proprietary ink cartridges, smartphone ecosystems that only accept certified accessories, and enterprise software platforms that limit interoperability or export options. In the digital realm, cloud-based services and **software-as-a-service (SaaS)** solutions often lock users into proprietary file formats, APIs, or user experiences, making it difficult and costly to migrate to alternative providers. Major vendors like Apple, Salesforce, and Amazon Web Services are well-known for creating tightly integrated ecosystems that discourage switching by making data migration complex, costly, or incomplete. These strategies are further reinforced by contractual constraints, such as multi-year commitments, tiered pricing, and auto-renewals, which add financial friction to any potential move.

This lock-in effect is exacerbated by the concepts of **sunk costs** and high **conversion costs**. Organizations and individuals invest significant time, money, and training into a particular platform or ecosystem, making the prospect of switching even more daunting. The more customized and integrated a solution becomes, the harder it is to leave – creating a cycle where users tolerate limitations or incremental upgrades rather than face the disruption and expense of change. As a result, tech lock-in not only prolongs the viability of existing brands and products but also shapes the pace and direction of technological progress. But this tech lock-in also results in diminished innovation, and often a resignation to accepting inferior products due to lack of reasonable options.

Enter **3D printing**, or additive manufacturing, which is the process of creating three-dimensional objects from digital models by layering material – such as plastics, metals, ceramics, or even biological substances – one layer at a time. Since its inception in the 1980s, 3D printing has rapidly evolved from a prototyping tool to a transformative manufacturing technology. Today, it encompasses everything from nano-scale components to large-scale construction, including the printing of custom medical implants, automotive parts, aerospace components, and even entire homes. The technology's versatility is evident in applications such as on-demand spare parts, personalized prosthetics, bio-printed tissues, and rapid prototyping for innovation across industries.

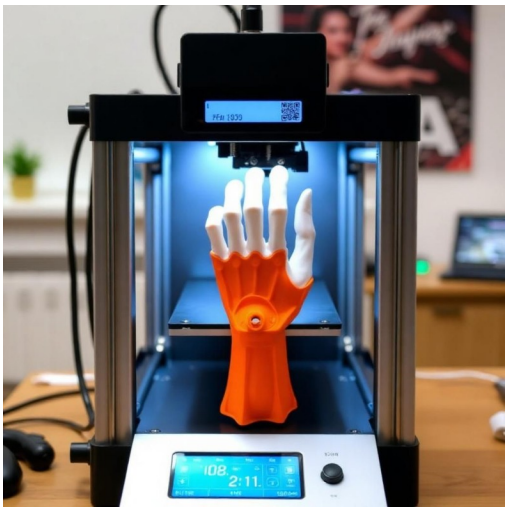


Figure 17: 3D Printer creating prosthetic

If the full potential of 3D printing were unleashed, it could disrupt several major status quos:

- Traditional manufacturing and supply chains could be decentralized, with goods produced locally or even at home, reducing the need for mass production and global shipping.
- Proprietary replacement parts and consumables could be bypassed, undermining tech lock-in strategies and empowering consumers to repair or modify products independently.
- The barriers to entry for new inventors and small businesses would be dramatically lowered, fostering innovation and competition.
- Entire industries, from construction to healthcare, could be transformed by the ability to produce complex, customized items on demand.
- Environmental impacts could be mitigated by reducing waste, transportation emissions, and excess inventory.

Ultimately, widespread adoption of 3D printing has the potential to challenge both the economic and ethical foundations of planned obsolescence and tech lock-in, shifting power from centralized producers to distributed creators and consumers.

AR/VR & Tech Progress

From the earliest days of photography and moving pictures, humanity has sought to capture, replicate, and even enhance reality through technology. The journey from static images to immersive

digital environments has been marked by continual innovation: stereoscopes in the 1800s introduced three-dimensional imagery, while the 20th century brought movies, television, and eventually holography, each step deepening our ability to simulate and augment the world around us.

By the late 1960s, the first head-mounted display, "The Sword of Damocles," laid the groundwork for both **virtual reality (VR)** and **augmented reality (AR)**, offering users computer-generated graphics that blended with or replaced their sensory experience of the real world. Over the decades, milestones such as flight simulators, interactive "artificial reality" labs, and data gloves paved the way for today's **spatial computing** – where AR and VR converge to create interactive, immersive environments that respond to users in real time.

Today, AR and VR technologies are transforming a wide range of industries. In entertainment, VR headsets and AR mobile games like Pokémon Go have redefined gaming and storytelling. Aerospace and automotive companies use VR for prototyping and immersive design, while AR assists with maintenance and training. In education, students explore historical sites or conduct virtual science experiments. The medical field employs VR for surgical training and pain management, and AR for overlaying critical information during procedures. Retailers offer virtual try-ons, architects visualize buildings at scale, and therapists use immersive simulations for mental health treatments. Even manufacturing and logistics benefit from AR overlays that guide workers or optimize warehouse operations.

Looking ahead, the fusion of AR/VR with machine learning and other emerging technologies promises to disrupt even more status quos. Imagine:

- Virtual prototyping of clothing or products, allowing users to "try before they print" with 3D printing.
- Entire public spaces transformed through AR, offering personalized information, art, or advertising on demand.
- Realistic VR/AR simulations for social skills training, therapy, or remote collaboration.
- Educational experiences that adapt in real time to student performance, providing personalized learning paths.
- Remote medical consultations using AR overlays to guide both patient and provider.
- Urban planning tools that let communities visualize and interact with proposed changes before they happen.
- Fully immersive remote workspaces, blurring the line between physical presence and digital collaboration.

As these technologies accelerate, several forward-looking questions arise that tie together themes from previous chapters:

- How do we ensure equitable access to immersive technologies, so benefits aren't limited to the privileged?
- In what ways might AR/VR amplify existing biases, privacy concerns, or misinformation challenges?
- What ethical responsibilities do creators and users have when virtual experiences become indistinguishable from reality?
- How can we balance the immense potential for progress with the risks of addiction, surveillance, or deepening digital divides?
- Will the next wave of disruption redefine not just how we interact with technology, but how we understand identity, agency, and community itself?

Embracing technological progress means not only harnessing these tools for innovation and growth, but also facing the ethical challenges they bring – ensuring that the future we build is both immersive and inclusive.

Erosion of Economic Sustainability

Earlier in this chapter, we looked at obsolescence and how it could be considered either inevitable or planned. Now let's consider our current **economic models**, specifically their sustainability. The most prevalent model globally is **capitalism**, which is defined by private ownership of resources and means of production, with goods and services exchanged in markets driven by supply and demand. Another model is **socialism**, where the state or community owns the means of production and aims to distribute wealth more equally. There are also mixed economies, which blend elements of both systems to varying degrees. Each of these models has evolved to address the needs and challenges of their times, but all are fundamentally shaped by the dynamics of labor, consumption, and resource allocation.

The accelerating rate of technological change, coupled with the disruptive nature of tech progress, poses significant challenges to the sustainability of these economic systems. Automation, artificial intelligence, and digital platforms are rapidly transforming industries, often rendering traditional jobs obsolete faster than new roles can be created. This disruption threatens the foundation of **economic participation** in models like capitalism, which rely on widespread employment and consumer spending to drive growth. To counteract these effects, societies have experimented with artificial supports such as **subsidies**, **retraining programs**, and **universal basic income (UBI)**. However, these measures often fail to address the root causes of disruption, serving as only temporary fixes rather than sustainable solutions.

It is important to recognize that Maslow's hierarchy of needs – a foundational theory of human motivation – does not include "make a lot of money" as a requirement at any level. Instead, Maslow's pyramid begins with physiological needs (food, water, shelter), followed by safety, belonging, esteem, and ultimately self-actualization. While money can help secure basic needs, research shows that happiness and fulfillment plateau once a certain level of financial security is achieved.

If we imagine a world where technological advancements – automation, AI, biotechnology, and beyond – are harnessed *intentionally* to meet all of Maslow's needs directly, the necessity for traditional economic systems would need to be fundamentally reevaluated. In such a scenario, access to food, shelter, healthcare, education, and even opportunities for personal growth could be decoupled from employment and income, challenging us to envision new models of economic and social organization that prioritize human well-being over perpetual economic growth.

Textbook Definitions – Technological Disruption and the Paradox of Progress

- **technological disruption** – A fundamental change that occurs when a new technology radically alters the way consumers, businesses, or industries operate, often making existing products or processes obsolete.
- **digital revolution** – The transition from analogue devices to digital technology, marking the beginning of the Information Era and profoundly transforming societies and economies worldwide.
- **3D printing** – A manufacturing process that creates three-dimensional objects by layering materials according to digital models, enabling rapid prototyping and customized production.
- **spatial computing** – The use of digital technology to interact with and manipulate physical space, blending real and virtual environments for immersive experiences.
- **wearable and embedded devices** – Electronic gadgets designed to be worn on the body or integrated into physical objects, often to collect data or enhance functionality.
- **adoption curve** – A graphical representation of how new technologies or products are adopted over time by different segments of a population.
- **planned obsolescence** – The deliberate design of products with a limited useful life so that they will need to be replaced, driving ongoing consumption.
- **inevitable obsolescence** – The natural process by which products or technologies become outdated due to advancements and innovation, regardless of intentional design.

- **tech lock-in** – A situation where users are dependent on a specific technology, vendor, or ecosystem, making it difficult or costly to switch to alternatives.
- **obsolescence** – The process by which something becomes outdated or no longer used, typically due to newer alternatives.
- **software-as-a-service (SaaS)** – A software distribution model in which applications are hosted by a provider and accessed by users over the internet, typically via subscription.
- **sunk costs** – Investments of time, money, or resources that cannot be recovered once made, often influencing future decision-making.
- **conversion costs** – The expenses and effort required to switch from one product, service, or system to another.
- **virtual reality (VR)** – A computer-generated simulation of a three-dimensional environment that users can interact with, typically through specialized headsets and controllers.
- **augmented reality (AR)** – Technology that overlays digital information or images onto the real world, enhancing the user's perception of their environment.
- **economic models** – Frameworks or systems that describe how resources are allocated, goods and services are produced, and wealth is distributed within a society.
- **capitalism** – An economic system characterized by private ownership of the means of production and operation for profit within competitive markets.
- **socialism** – An economic system in which the means of production are owned and controlled collectively or by the state, with an emphasis on equal distribution of wealth.
- **economic participation** – The involvement of individuals or groups in the production, distribution, and consumption of goods and services within an economy.
- **subsidies** – Financial assistance provided by governments to support businesses, industries, or individuals, often to promote economic activity or stabilize prices.
- **retraining programs** – Initiatives designed to teach new skills to workers, especially those displaced by technological or economic changes.
- **universal basic income (UBI)** – A policy proposal in which all citizens receive a regular, unconditional sum of money from the government to cover basic living expenses.