Navigating the Digital Frontier: Information Ethics and the Future of Information Science

Marlene A Holmner, African Centre of Excellence for Information Ethics, Department of Information Science, University of Pretoria, Pretoria, South Africa

Abstract

This entry offers an in-depth investigation of information ethics, tracing its historical evolution, examining its foundational works and notable authors, and emphasising the most important ethical and moral dilemmas of the information era. It clarifies how ethical judgements are made as well as the crucial role information scientists play in overcoming ethical obstacles, particularly those brought on by disruptive technology linked to the Fourth Industrial Revolution and Society 5.0. The entry also examines key international information ethics policies and guidelines, showing how they influence how information should be used ethically. It concludes with a look ahead at the information ethics trends of the future, stressing its ongoing importance in our increasingly digital society.

Glossary

Information Ethics Information ethics (IE) tackles information development, dissemination, storage, access, and appropriation. It examines how information generation, control, and access affect ethics. This includes digital rights, privacy, IP, access, and the ethical aspects of the digital divide. Given the exponential rise of information technology and their pervasive influence in society, IE guides the appropriate, fair, and just use of information resources and associated management systems.

Fourth Industrial Revolution The Internet of Things (IoT), robotics, virtual reality, and artificial intelligence are disrupting how people live, work, and interact, creating the Fourth Industrial Revolution (4IR). The Fourth Industrial Revolution is characterised by a variety of new technologies that are integrating the physical, digital, and biological worlds, touching all disciplines, economies, and sectors, and even threatening human nature.

Society 5.0 Society 5.0 is a Japanese government-proposed vision for human society's future evolution by merging cyberspace and physical space. AI, big data, robotics, and the Internet of Things are key to this. Society 5.0 seeks to develop a human-centered society that uses these technologies to solve healthcare for an ageing population, infrastructure, disaster resilience, and sustainable economic growth. It integrates technology into daily living and societal operations to improve citizens' quality of life, unlike prior societal models.

Disruptive technologies Innovative technologies that disrupt processes, goods, or industries are disruptive technologies. They often have new features, benefits, or pricing that make traditional techniques obsolete or less competitive. A disruptive technology may first appear inferior to majority of an incumbent's customers and not suit their needs. The industry paradigm shifts as the technology evolves and obtains acceptance. Digital photography replaced film photography, streaming services changed music and movie rental, and smartphones changed communication.

Key Points

- The History of Information Ethics, from freedom of speech in ancient Greece to the current 4IR.

- Prominent Authors and Seminal Works in the Field of Information Ethics, including the works of Norbert Wiener, Walter Maner, Tom Forester, Perry Morrison, James Moore, Terrell Bynum, Rafael Capurro, Helen Nissenbaum and Luciano Floridi.
- The main ethical issues of the information age, namely Privacy, Accuracy, Intellectual Property, Access and Security.
- Ethical Decision Making through the western ethical theories "lenses".
- The role of Information Scientist in the face of developing disruptive technologies of the 4IR.
- The need for a dynamic and inclusive discussion in information ethics is required due to the complexity of the ethical challenges created by disruptive technologies, including blockchain, digital health, genetic engineering, and AI and IoT.
- The significance of international policies and norms for information ethics cannot be over emphasised in the increasingly interconnected world of the digital age.
- The future of information ethics will be marked by a continuous need for vigilance and flexibility, as new technologies and future trends create new ethical quandaries and challenges.

Introduction

It is undisputable that the fourth industrial revolution (4IR) and its technologies are altering the manner that people work, live and communicate with each other. These technologies were coined "disruptive technologies" by Clayton M. Christensen and was introduced in his 1995 article Disruptive Technologies: Catching the Wave, co-written with Joseph Bower (Bower and Christensen, 1995). These technologies (or innovations) have led to dramatic changes in the manner consumers, businesses and industries operate. Within this relentlessly changing environment, it is important to constantly consider the impact that these technologies have on our daily lives. For this reason, it is important for Information Scientist to stay in touch with these technologies and to be able to understand the ethical issues that arise from the use thereof.

Within Information Science, information ethics (IE) is the branch of ethics that deals with the ethical concerns that arise in the creation, dissemination, and use of information through such technologies (Burgess and Knox, 2019; Ocholla, 2013; Floridi, 2008; Capurro, 2006). It is a comparatively new research field that has grown in prominence as the quantity of data accessible to us has increased exponentially in recent years. This data, whether it is created, captured, or replicated, is called the Global Datasphere, and it is experiencing incredible growth. According to the International Data Corporation (IDC), the overall global datasphere reached 64 zettabytes in 2020. In 2021, the overall amount of data created worldwide reached 79 zettabytes and by 2025, this amount is expected to double (Djuraskovic, 2021).

This mind-staggering amount of data combined with new and exciting technologies, has again highlighted the importance of the study of information ethics. By including IE in the curriculum, scholars are made aware of the need of professionalism, ensuring that information professionals abide by high ethical standards in their work, and are dedicated to the public good (Ocholla, 2013). Information ethics helps to ensure that the creation, dissemination and use of information is directed in a socially responsible manner, bearing in mind the possible influences on individuals and society as a whole (Burgess and Knox, 2019). By doing this, information ethics helps in the fortification of our basic human rights, such as our right to privacy and freedom of expression as IE helps to ensure that these rights are respected and protected (Nissenbaum, 2009). Furthermore, IE helps to safeguard non-discrimination and fairness by ensuring that information is made available to all individuals and groups, regardless of their circumstances and background, and that information systems and technologies do not perpetuate or exacerbate existing inequalities. Within the 4IR, as more businesses use these disruptive technologies across their operations and embed it in their products and services, they quickly realize that technology is only as good as the trust it engenders among all stakeholders, including, employees and customers (Kingsly, 2022). Information ethics helps to ensure that information systems and technologies are designed and used in ways that promote trust between individuals, organizations, and society as a whole.

This entry on Information Ethics is written with the intent to be a reference point for scholars on the topic of Information Ethics. It will give attention to the history of information ethics as well as the prominent authors and seminal works within the domain of information ethics. Furthermore, it will discuss the information ethical issues of the information age and discuss the roles and responsibilities that the Information Scientist must play in this domain. Principal's central to information ethics will be discussed as well as ways to analyse information ethical issues. The entry concludes by discussing the future trends within this domain.

History of Information Ethics

The history of information ethics (IE) has two opposing viewpoints, as it is said to be either a very long one or a relatively short one (Capurro, 2006). The long history of information ethics can be found when relating information ethics back to the broader philosophical context of ethics. In this fashion, ethical philosophy can be traced back to the fifth century BCE, with the appearance of the Greek philosopher Socrates, a profane prophet whose self-proclaimed undertaking was to promote the need for rational

criticism of people's beliefs and their practices (Dhillon and Lim, 2015). According to Capurro, (2006) information ethics can thus be traced back to the idea of freedom of speech in ancient Greece, called parrhesia. However, we can also consider it to having a relative short history, beginning in the 1950s and 1960 if considering when the field of Information Science began to emerge and when the first computers were developed. At that point in time, scholars and academics began to deliberate the ethical implications of the novel technology, specifically in relation to issues relating to information. When considering this shorter history of IE, it is necessary to consider that the foundation of IE lies in Computer Ethics (CE). This view is supported by Bynum and Rogerson (1996), who are of the opinion that CE went through two generations. The first generation of CE started with the coining of the word Computer Ethics by Walter Maner in the mid-1970s. This term was coined to refer to the application of ethical theories from philosophy to ethical problems created by the "new" technology. This developed into the second generation of CE, namely global information ethics, when authors such as Sojka (1996) argued that CE is perhaps less about computers and more about information flow.

During the 1980s and 1990s, the domain of Computer and Information Ethics(C&IE) started to solidify, as academics and scholars began to cultivate a more formalized approach to studying the ethical issues related to information technology. This period saw the publication of several influential books and articles, such as "Ethics and Information Technology" by Moor (1985), "Computer Ethics" by Johnson, (1985) and "Computer Ethics" by Forester and Morrison, (1994). From then on, C&IE was renowned as a recognized field in applied ethics with its own journals (journal of information ethics in 1992), conferences (Ethicomp conferences which started in 1995), research groups (Luciano Floridi's creation of the Information Ethics Research Group at Oxford University in the mid 1990) and professional organizations (Froehlich, 2004; Heersmink *et al.*, 2012).

During the 1990s and 2000s, the domain of IE started to thrive as the Internet was introduced and new technologies such as Web 2.0 technologies emerged. Scholars began to focus on issues such as privacy, intellectual property, accessibility and accuracy. These ethical issues of the information age were coined Mason's PAPA framework Mason, (2017) and will be discussed later in this entry. One of the first university academic departments to offer a regular course on IE was the School of Information Sciences at the University of Pittsburgh in 1990. During this same period, Kent State University started their offering of a Master's level course on "Ethical concerns for library and information professionals" and Simmons College offered a course, "Organizational/information ethics" (Froehlich, 2004). It is interesting to note that, as early as 1990, Information Ethics was being taught on undergraduate level, in South Africa at the University of Pretoria (Buchanan and Hvizdak, 2009).

In recent years (2000 onwards), the domain of information ethics is again placed in the spotlight with the rise of disruptive technologies such as Artificial Intelligence, Internet of Things, Big Data, Robotics, Augmented or Virtual Reality, etc. As the amount of information available to us grows exponentially and new, innovative but disruptive technologies emerge, new ethical issues and problems will continue to arise making IE increasingly relevant to policymakers, business leaders, and the general public. As aptly summarised by Bielby (2015): "Information Ethics has grown into a global phenomenon, and whether merely a discipline or a new 'world spirit', Information Ethics has now taken front stage in, for, and sometimes against all aspects of society.".

Prominent Authors and Seminal Works in the Field of Information Ethics

Although many scholars have made important contributions to the domain of IE as well as CE, there are several significant authors, and numerous seminal works. Following is a list of some of the most notable in chronological order.

"*Cybernetics" by Norbert* Wiener (1965): Norbert Wiener was a math and engineering professor at MIT in the United States. In this ground-breaking text, Wiener defines a new branch of applied ethics and acknowledges some social and ethical aspects of electronic computers. Seemingly, Wiener did not regard himself as founding a new field of ethics, and this resulted in him not coining the terms "computer ethics" or "information ethics." These phrases were only coined decades later.

"*Starter Kit in Computer Ethics"by* Walter Maner (1980): Walter Maner was a philosopher and lecturer who taught Computer Science at Bowling Green University. Unaware of the work by Wiener, Maner was determined that a new branch of applied ethics should be created. He defined the proposed new field as one that studies ethical problems "aggravated, transformed or created by computer technology". In 1978 he designed a curriculum on teaching CE which was later published in 1992 Bynum *et al.* (1992). For other useful computer ethics contributions by Maner also refer to Maner, (1980, 1996, 2002).

"Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing" by Forester and Morrison (1994): Tom Forester is a Lecturer in the, Division of Science and Technology at Griffith University in Australia. He is editor of The Microelectronics Revolution and The Information Technology Revolution and author of High-Tech Society. Perry Morrison lectures in psychology at the National University of Singapore. Their book is considered one of the first all-inclusive handlings of the subject of computer ethics. It offers a summary of the key ethical issues related to computer technology and suggested a framework for thinking about these issues.

"*Computer Ethics*" Johnson (1985): Deborah Johnson is the Anne Shirley Carter Olsson Professor of Applied Ethics and Chair of the Department of Science, Technology, and Society at the University of Virginia. Her work described computer ethics issues as old ethical problems that are "given a new twist" by computer technology. This was the field's first significant textbook, and it quickly became the key book used in computer ethics courses given at institutions in English-speaking countries (Bynum, 2020). For other useful computer ethics contributions by Johnson also refer to (Johnson, 1994, 1999, 2001).

"*What is Computer Ethics*?" by Moor (1985): James Moor is the Daniel P. Stone Professor of Intellectual and Moral Philosophy at Dartmouth College. He is known for coining the term "computer ethics". Moor has written numerous significant books, including "The Digital Phoenix: How Computers Are Changing Philosophy, with T W Bynum, Tomassi, (1999), "Cyberphilosophy: The Intersection of Philosophy and Computing", with Bynum and Moor, (2002). For other useful computer ethics contributions by Moor also refer to Moor, (1997, 1999, 2005, 1991, 2001).
"*Computer Ethics*" by Bynum, (1985): Bynum is an American philosopher, writer and editor. Bynum is a professor of philosophy and the director of the Research Center on Computing and Society at Southern Connecticut State University. Bynum believed that CE was a topic that was essential and should be expanded. This led to numerous publications relating to IE such as "Norbert Wiener and the Rise of Information Ethics" (Bynum, 2008) and "Historical Roots of Information Ethics" (Bynum, 2010).
"*Moral Issues in Information Science*"by Capurro, (1985). Rafael Capurro is a Uruguayan Philosopher and academic who has been at the forefront of IE research for several decades. Capurro is a proliferate author in the field and have written in a variety of languages namely German, French, Spanish and English, to name the dominant ones. In 1999 he founded the International Center for Information Ethics (ICIE). This center has initiated the progression of the field of Information Ethics, offering a platform for an intercultural exchange of ideas and information regarding worldwide teaching and research in the field. He and his wife Annette created the Capurro Fiek Foundation in 2010 as an independent, non-for-profit foundation dedicated to promoting the analysis and ethical evaluation of the social and cultural impact of new technologies. For other useful information ethics contributions by Capurro also refer to Capurro, (1985, 2006, 2008, 2017, 2010, 2009) , etc.
"Ethics and Information Technology" Nissenbaum (1999): Helen Nissenbaum is professor of Information Science at Cornell Tech. She is known for her work on privacy, trust, and security in the digital age, and she has written several influential books and articles on the ethics of information technology. For other useful information ethics contributions by Nissenbaum also refer to (Nissenbaum and Walker, 1998) (Nissenbaum, 1998, 2004, 2009, 2011, 2018).
"*The Ethics of Information*" by Floridi, (2013): Luciano Floridi is an Italian philosopher and professor of information ethics at the University of Oxford. He is well-known for his work on information philosophy and information ethics. He is the author of several notable books, including "The Philosophy of Information." These works investigate ethical issues in information philosophy and provide a framework for thinking about these topics. Floridi's additional useful information ethics contributions can be found in Floridi (2008, 2011, 2013, 2019).

These authors and publications are regarded as seminal in the field of information ethics, and they provide a thorough grasp of the information ethical quandaries linked with information technology, as well as numerous perspectives on how to approach and analyze these topics. It should be emphasized that this discipline is always evolving, and new works and research can be considered seminal.

The Main Ethical Issues of the Information age

After the abundance of information and computer ethics publications since 1985, it become clear that the field of IE was here to stay. In the information age, numerous ethical issues stemmed from the nature of information itself. In 1986, Richard Mason published a social framework for addressing the major ethical issues of the information age in his pivotal 1986 article "Four Ethical Issues of the Information Age" (Mason, 1986). This framework consisted of four broad categories of ethical issues namely privacy, accuracy, property and accessibility (PAPA). This PAPA framework is still relatively germane in studying the ethical issues in information technology (Woodward *et al.*, 2011). Due to the increasing prevalence of digital data and the inherent dangers connected with its storage and transfer, security becomes a crucial ethical concern in the information age. It is the responsibility of information security to protect data integrity, confidentiality, and accessibility, immediately affecting ethical concepts like privacy, trust, and accountability (Bishop, 2003). When taking into account the possible harm brought on by data breaches, such as identity theft, financial loss, or privacy invasion, the ethical implications of security become clear. These violations can damage the public's trust and violate people's rights (Solove, 2006). Therefore, it is the responsibility of information professionals to safeguard the integrity of the digital ecosystem, protect stakeholders, and follow ethical standards in their security practises. It has thus become vital to include a 'S' to the PAPAS acronym.

These five ethical issues will now briefly be discussed:

(1) Privacy: Personal information is being gathered, saved, and shared on a huge scale as a result of the expansion of digital technology and the internet (Djuraskovic, 2021). This raises ethical considerations about who has access to and uses this information, as well as concerns about the possibility of surveillance and manipulation. In 1996, Johannes Britz elaborated on this category by categorizing private information into four categories namely; private communication, privacy of the body, personal information, and information about one's possessions (Britz, 1996).
(2) Accessibility: While digital technologies have greatly increased access to information, not everyone has equal access to these resources. This raises questions about how to ensure that everyone has access to the information they need to make informed decisions and participate fully in society. As Mason, (1986) points out, literacy is essential for one's participation in the growth of any society. However, literacy encompasses much more than just the ability to read. Intellectual skills, such as reasoning must be cultivated through education. Second, access to the essential technologies is required, and finally information must be available in order to be used and consumed.

(3) Property: Intellectual property is a complex ethical issue that has gained increasing attention in recent years. The internet and digital technologies have made it easy to share and distribute information, including copyrighted material. This raises questions about how to protect the rights of creators and owners of this material, while also allowing for the free flow of information. At its core, intellectual property refers to the ownership of ideas and creative works, including patents, trademarks and copyrights. Intellectual property rights encompass a wide range of methods to protect this intellectual property. Each of these instruments of protection is governed by a set of laws and regulations. However, some of these rules are not universal and they only apply in a single country.
(4) Accuracy: Data integrity becomes increasingly important, as massive databases grow more interconnected. Technology have made it easy for false or misleading information to spread quickly and widely, which can have serious consequences for individuals and society as a whole. This raises questions about how to combat misinformation and disinformation, and how to ensure that people have access to accurate and reliable information. Accurate, accurate, and trustworthy information is critical for decision-making in practically every element of human endeavour, whether conducted by individuals, communities, organizations, or governments.
(5) Security: Security is a crucial ethical issue in our digital age since it involves such a broad variety of concerns in the context of the information age, from data breaches to cyberattacks. Information security, in its most basic form, aims to protect the availability, confidentiality, and integrity of data (Vacca, 2009). When these goals are violated, ethical issues develop, frequently leading to serious costs like privacy violations, identity theft, financial losses, and reduced trust in digital systems (Solove, 2006). For instance, data breaches frequently result in unauthorised access and misuse of personal data, which violates a person's right to privacy (Dhillon and Torkzadeh, 2006). Similar concerns about the moral limits of state behaviour in the digital sphere are brought up by problems like cyber espionage and cyber warfare (Dunn Cavelty, 2014). Artificial intelligence and other emerging technologies provide new vulnerabilities and the possibility of abuse, greatly complicating the security picture (Russell *et al.*, 2015).

After discussing the critical ethical challenges facing the information age, including Privacy, Accuracy, Intellectual Property, Access, and Security, it is obvious that these topics are connected with difficult moral conundrums. The pursuit of accuracy can clash with concerns about intellectual property; the need for security can occasionally impinge on the rights to privacy or access; and the rights to privacy and access frequently find themselves at war with one another. The significance of competent decision-making techniques in the realm of information ethics is highlighted by these moral conundrums. We will explore ethical decision-making procedures in more detail when we move into the following section and apply them to the problems we've already covered. We can help information professionals traverse these ethical difficulties efficiently and ensure the proper use and management of information in our quickly changing digital ecosystem by utilising several ethical theories like Deontological, Consequentialist, and Virtue Ethics.

Ethical Decision Making

When considering ethical decision-making, it is important to understand that there are three types of ethical enquiries or studies, namely: Normative Ethics, Descriptive Ethics and Meta-ethics. Normative ethics is the study of ethical behaviour that examines the inquiries that arise concerning how an individual ought to act. Thus, what is right or wrong, good or bad, acceptable or unacceptable? Meta-ethics is the study of the landscape, scope, and significance of moral judgment, thus understanding the language of morality. Descriptive ethics is the study of people's beliefs about morality, thus, what people think about morality. As ethical decision making within Information Ethics is more concerned about what is right or wrong, or acceptable or not, we are more concerned with the normative ethical inquiry.

When the question is asked: "How do I make an ethical decision?" normative ethical theories come into play. Ethical theories offer support for the decision maker as these ethical theories represent the viewpoints from which individuals seek guidance as they make decisions. Authors such as Burgess and Knox, (2019) view these theories as "lenses" through which an individual can view a certain situation and then make a decision from this perspective. It is important to note that not everyone makes decisions in the same way, using the same information and applying the same ethical theory or "lens".

There are several important western ethical theories. Some of the most commonly used theories include:

(1) Deontology: This approach holds that moral obligations and rules are independent of their consequences and that certain actions are inherently right or wrong. In the context of information ethics, this approach would focus on the moral obligations of those who create, disseminate, and use information, such as the duty to protect privacy or to respect intellectual property rights. This approach, which has its roots in Immanuel Kant's intellectual writings, contends that morality is defined by obedience to norms and obligations, independent of results. Deontologists emphasise the moral significance of protecting private rights, defending truthfulness, and ensuring data integrity in the context of information science. They contend that these principles are unbreakable, regardless of any possible advantages that may result from bending or breaking them. For instance, a deontologist would argue against a data breach even though it could reveal corruption since it violates the right to privacy. The relevance of moral absolutes amid the continually shifting sands of the digital realm is highlighted by this approach, which urges information professionals to always evaluate the underlying rightness or wrongness of their acts.

(2) Consequentialist: This approach holds that the morality of an action should be judged based on its consequences. In the context of information ethics, this approach would focus on the potential consequences of different actions related to information, such as the potential harm caused by the spread of false or misleading information. According to consequentialist ethics, which includes utilitarianism, a well-known subset of it, the morality of a course of action is determined by how it turns out. This viewpoint focuses on the advantages and disadvantages that may come from decisions on data management, privacy, and access in the field of information science. A consequentialist would weigh prospective benefits against principles like data privacy rather than viewing them as inviolable. A consequentialist might, for example, acknowledge the value of privacy but nevertheless defend a data breach if it revealed serious corruption on the grounds that the overall result is advantageous. Consequentialism encourages information professionals to evaluate the potential effects of their decisions on all stakeholders as we negotiate the digital frontier, taking into account not only the regulations but also the larger social context in which data and information are used.
(3) Virtue ethics approach: This approach holds that the goal of ethical behaviour is to develop virtues such as honesty, kindness, and fairness. In the context of information ethics, this approach would focus on the character and behaviour of those who create, disseminate, and use information, rather than on specific rules or consequences. This approach, which Aristotle inspired, places more emphasis on the actor's moral character than it does on the actual event. This refers to putting a higher priority on helping information workers develop virtues like honesty, responsibility, and empathy in the context of information science. Making decisions based on a moral character that aspires to the "highest good" is required by virtue ethics. For instance, a moral information professional might abstain from participating in privacy-invading data mining practises not only because they are inherently right or wrong (according to deontology) or because of the consequences they may have (according to consequentialism), but also because they go against their own sense of morality and commitment to respect for others. This strategy emphasises the value of developing moral character and values in order to ensure ethical behaviour in the uncharted waters of the digital age.

In conclusion, the complexity of ethical decision-making in the field of information ethics necessitates a thorough investigation of moral principles, consequences, and character strengths. The consequentialist viewpoint directs us to take into account the wide-ranging effects of our actions on all stakeholders. Deontological ethics, on the other hand, emphasise the importance of responsibility and unwavering moral principles. The need of developing virtues in our professional conduct is emphasised by virtue ethics, which further exhorts us to strive for moral excellence. Information scientists can use the complementary interactions of these three Western ethical theories—deontological, consequentialist, and virtue ethics—to navigate the challenges of the digital frontier. They work together to provide a solid ethical framework that supports the responsible, equitable, and rights-respecting implementation of information science in the future. We now focus on the crucial role of information scientists, whose actions and choices influence this future in the dynamically changing information science world, using this ethical compass as our guide.

The Role of Information Scientists

The dynamic nexus of information, technology, and ethics poses complicated difficulties that call for specialised knowledge to successfully traverse. Information scientists, who serve as the link between the technological world and ethical considerations, are at the centre of tackling these issues. With their in-depth knowledge of technology, its uses, and its potential repercussions, these experts play a crucial role in the area of information ethics by ensuring the ethical production, dissemination, and use of information. This section will examine the various functions that information scientists perform within the field of information ethics, highlighting their multifaceted contributions, which range from defining principles and identifying ethical dilemmas to facilitating research, advising legislators, encouraging interdisciplinary collaborations, and educating the public.

(1) Identifying Ethical Issues: Information scientists are in a good position to identify any ethical issues that may come up while designing, using, and utilising information systems and technologies because they are specialists in the subject (Brey, 2010). They are skilled in spotting ambiguous situations that might not be obvious to someone without a thorough understanding of the underlying technology, such as privacy concerns, data misuse, or the digital divide.
(2) Definition of Ethical Principles: According to Mingers and Walsham (2010), information scientists play a crucial part in developing ethical principles and best practises for the use of information systems and technology. These regulations may address topics including data handling, user privacy, software development, and dissemination of digital content. They make certain that information technology is produced and used properly by merging technical and ethical factors.
(3) Facilitating Research: Information scientists can carry out research to probe deeper into the ethical implications of information systems and technology, as mentioned by Capurro (2010). This may entail investigating the potential effects of a new technology, coming up with creative solutions to ethical problems, or determining how well-established ethical rules are working. Their work can help inform ethical judgements in the sector and advance the creation of more morally sound technologies.
(4) Advising Policy-Makers: Information scientists can help policy-makers understand the ethical implications of new technologies, which can have an impact on the creation of rules and laws that control their usage (Stahl, 2011). They aid in ensuring

that rules and regulations reflect a nuanced understanding of the technology in question by bridging the gap between the technical and policy worlds.

(5) Interdisciplinarity: Information scientists frequently work with experts from a variety of domains, including philosophy, sociology, law, and computer science, in order to successfully address the complex ethical issues that arise in relation to the use of technology (Introna, 2007). The development of well-rounded answers and a more thorough analysis of ethical problems are both made possible by this interdisciplinary approach.

(6) Raising Awareness: According to Brenner, (2010), information scientists play a crucial role in advancing the ethical understanding of information technology. To educate the general people on the moral ramifications of their technology use, they could participate in public outreach. Instilling in the upcoming generation of information workers the ethical values and concerns that will direct their future work in the industry is another vital duty they have. Information scientists are crucial players in information ethics, to sum up. They use their technical know-how to identify moral dilemmas, create moral standards, direct research, offer policy advice, encourage interdisciplinary cooperation, and raise ethical awareness in regard to information technology.

It becomes more and more obvious that information scientists' function is crucial in the face of developing disruptive technologies as we delve deeper into the crucial role of information scientists in controlling and reducing ethical dilemmas. These cutting-edge technologies, like blockchain, the Internet of Things, and artificial intelligence, are revolutionising our world while simultaneously posing a number of new ethical dilemmas. In the section that follows, we'll go into greater depth about these disruptive technologies, emphasising the particular ethical issues they raise and how information scientists might successfully address them.

Information Ethical Concerns Related to Disruptive Technologies

By definition, disruptive technologies bring about new methods of doing things that have a considerable impact on the markets and societal institutions that are now in place. As a result, they frequently bring distinct ethical difficulties that demand careful thought. The following are some of the main moral issues with numerous disruptive technologies:

1. Many industries have embraced the use of artificial intelligence (AI) and machine learning (ML), which has improved our quality of life but also brought up important ethical questions. Data-driven technologies like artificial intelligence and machine learning (ML) need a lot of data to work properly. Privacy risks arise from this reliance on data, particularly personal data. Individuals can be identified when personal data is used to train AI systems, which may expose or misuse personal information without the owner's consent (Russell *et al.*, 2015). These worries highlight the significance of laws like the General Data Protection Regulation (GDPR) in preserving people's right to privacy in the age of AI and ML.

The ethical implications of algorithmic prejudice are also very important for AI and ML. Since machine learning algorithms are trained on real-world data, they frequently reproduce or even exacerbate pre-existing biases. According to Mittelstadt *et al.* (2016), if an AI system is trained on past hiring data that reveals racial or gender bias, it may reinforce that bias by omitting particular demographics from job recommendations. The possibility of bias in algorithmic decision-making highlights the necessity of transparency in AI systems and a dedication to identifying and eradicating any flaws.

Due to its capacity for self-determination, AI also raises the issue of accountability. Determining who is to blame for an AI's actions that cause hurt or damage can be difficult. As judgements made by AI could have a substantial impact on human life, this is especially pertinent for AI systems employed in autonomous vehicles or healthcare applications (Bryson, 2016). Clear standards and frameworks for AI accountability are therefore required.

2. The Internet of Things a network of physical objects including home appliances, wearable technology, and automobiles that link to the internet in order to collect and share data, offers many advantages but also raises a number of ethical concerns. Privacy is one of the main issues. Data breaches are more likely as more personal and sensitive data is collected and transmitted by IoT devices. Hackers with unauthorised access to these devices run the risk of abusing personal data for fraudulent or destructive activities including identity theft (Roman *et al.*, 2013). The amount of personal data that is at danger keeps increasing as IoT devices are incorporated into more facets of daily life.

IoT security issues include the potential for physical harm as well. For instance, if an IoT device linked to a vital infrastructure system—like the electricity grid or a medical equipment—is compromised, it may have catastrophic, even fatal, repercussions. IoT also raises concerns regarding data consent and ownership in addition to privacy and security. Users' comprehension of the scope of data collected by their IoT devices may be obscured by complicated data sharing agreements that are frequently buried in terms and conditions. Users find it challenging to provide informed consent for data collection and use as a result of this lack of transparency, prompting moral questions regarding who genuinely "owns" the data acquired by these devices (Roman *et al.*, 2013).

3. While facilitating innovation across a wide range of industries, blockchain technology and cryptocurrencies do in fact present particular ethical difficulties. The regulatory monitoring of these technologies is one ethical dilemma. Regulators may find it challenging to keep an eye on transactions and enact rules because blockchain technology is intended to be decentralised and largely anonymous (Tapscott and Tapscott, 2016). Governments and organisations responsible with stopping criminal acts like money laundering and fraud face difficulties as a result.

In addition, the intrinsic anonymity of blockchain technology has potential drawbacks. On the one hand, it can safeguard users' privacy and foster trust because the technology permits transparency and guards against tampering. However, this

anonymity itself can be used to support criminal acts like the purchase of unlawful products or services, tax evasion, or money laundering (Mougayar, 2016).

The stability of the economy is a further ethical issue. Due to their high volatility, cryptocurrencies might cause financial markets to become unstable. Extreme price swings in the cryptocurrency market could have a negative impact on global financial institutions and possibly economies if they are not effectively controlled (Böhme *et al.*, 2015). Finally, even if blockchain technologies promise to increase accountability and transparency, they also raise moral concerns about fair access and the digital divide. Concerns regarding who can use and benefit from these technologies grow increasingly urgent as their adoption rises.

4. While having the potential to completely change the way healthcare is provided, digital health technologies also raise important ethical issues that need to be addressed. One of the most important ethical concerns with digital health technologies is privacy. Numerous sensitive health data points are gathered by wearable technology and health apps, potentially granting access to private health data to third parties, often without the user's awareness or agreement (Mittelstadt and Floridi, 2016). Due to the possibility of this information being misused, such as for discriminatory practises by insurers or employers, concerns have been raised about data security (Price and Cohen, 2019).

A major obstacle in the world of digital health is informed consent, a cornerstone of moral medical practise. Users may find it difficult to give really informed permission due to the complexity of data sharing, the obscurity of data use, and the opaqueness of privacy regulations (Mittelstadt and Floridi, 2016). Therefore, there is a need for clear, intelligible, and open communication regarding the purposes for which health data are used as well as the individuals who have access to it. Finally, the use of digital health technologies may exacerbate inequalities in the delivery of healthcare. Although these technologies have the potential to increase access to care, especially for communities that are difficult to reach, they also run the risk of escalating inequality. The elderly or people from lower socioeconomic categories may not have access to the essential devices or may have insufficient digital literacy abilities, which can lead to the digital divide (Chen and Zhu, 2019).

5. Advances in gene editing methods and the gathering of genomic data, in particular, create a broad range of ethical conundrums that society must address. In the case of genetic engineering, consent—a crucial ethical issue—becomes complex. It can be challenging to gain informed permission for all possible applications of genetic data because the potential future uses are not always obvious at the time of data collection (Knoppers and Thorogood, 2017). Further complicating the concept of permission is the familial implications of genomic information, which go beyond the individual to include biological relations (Bunnik *et al.*, 2013).

Another significant issue in the field of genetics is privacy. Inappropriate management or access to sensitive genetic data could lead to harmful uses, such as genetic discrimination on the part of employers or insurance companies. The security of genetic data is significantly at risk from data breaches, both deliberate and unintentional (Greenbaum *et al.*, 2011).

The ethical concerns raised by genetic engineering also heavily emphasise equity. Inequalities in the use of genetic technologies and their advantages could worsen already-existing societal injustices. Additionally, there are issues with "genetic exceptionalism," which refers to the idea that genetic information is fundamentally distinct from other types of health information. This idea might cause an excessive emphasis to be placed on genetic disorders or the allocation of resources to them at the expense of other health issues (Juengst *et al.*, 2012).

In conclusion, a dynamic and inclusive discussion in information ethics is required due to the complexity of the ethical challenges created by disruptive technologies, including blockchain, digital health, genetic engineering, and AI and IoT. While reshaping the world and accelerating development, these technologies are also escalating moral conundrums related to privacy, accountability, equity, and security. They urge us to reconsider established moral standards and modify them to take into account the specifics of the digital age.

These issues coming together emphasise the need for comprehensive international policies and norms. A cooperative worldwide strategy that crosses country boundaries and cultural gaps is necessary to strike a balance between technology progress and ethical considerations. Our following section looks at these international rules and regulations in the area of information ethics, highlighting how important they are for guiding moral behaviour in a globalised society that is being continuously altered by disruptive technology.

International Policies and Guidelines Related to Information Ethics

The significance of international policies and norms for information ethics cannot be over emphasised in the increasingly interconnected world of the digital age. Our reliance on technology is growing and changing, and with it the ethical issues that go along with it. The United Nations Educational, Scientific, and Cultural Organisation (UNESCO) contends that in order to manage the ethical issues that develop as information and communication technology (ICT) advances, it is essential to have universally accepted rules. Intellectual property rights, data protection, and privacy are all governed by ethical norms, which also have an impact on government policy, research methods, and human behaviour. As we advance further into the information age, international regulations and guidelines—such as the OECD's data privacy guidelines or the EU's General Data Protection Regulation (GDPR)—set the stage for standardised practises, ensuring that we do so in an ethical and responsible manner.

1. The fundamental rights and liberties to which all people are entitled are outlined in the Universal Declaration of Human Rights (UDHR), which was adopted by the UN General Assembly in 1948. Articles 12 and 19 are particularly important in the context of information ethics.

The right to privacy is proclaimed in Article 12 of the UDHR, which also states that no one shall be the target of arbitrary interference with their family, home, or correspondence or attacks on their honour or reputation. This has significant ramifications in the context of the digital era, particularly when taking into account concerns like data gathering, surveillance, and data protection. These areas are currently partially governed by privacy legislation, such as the General Data Protection Regulation (GDPR) of the EU, which reflects the UDHR's stated principles (EU, 2016).

The right to freedom of thought and expression is outlined in Article 19 and includes the ability to have opinions without interference as well as the freedom to seek, receive, and share information and ideas through any media, regardless of boundaries. The current interpretation of this clause includes digital liberties, addressing issues with censorship, net neutrality, and information access in the digital era. Guidelines and principles promoting open access to information and the free flow of information online are inspired by this idea (UNESCO, 2011).

The Universal Declaration of Human Rights (UDHR) continues to be a cornerstone of international human rights law and acts as an essential ethical standard in the field of information ethics, continuing to direct and inspire ethical principles and policies around the world.

2. A key step in creating global standards for data protection was the 1980 introduction of the Organisation for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These recommendations were made in response to the increased awareness of the threats to privacy and data protection posed by technical breakthroughs, particularly with the expanding mobility of personal data across international borders (OECD, 1980).

The standards offer a thorough set of rules to control how personal data is handled, including data collection, use, and dissemination. Limitations on the collection of personal data, obligations for data quality, openness about policies and practises, individual rights to access and correct data, data security precautions, and restrictions on the transfer of data to nations with insufficient data protection are just a few of the fundamental principles outlined in the guidelines. Many national and international legislation and regulations pertaining to data protection, including the EU's General Data Protection Regulation (GDPR), have been based on these principles (Greenleaf, 2012).

The rules also place a strong emphasis on striking a balance between information freedom and data protection, reflecting the interconnectedness of the world's information environment. In the digital age, where information travels quickly and continuously across borders and where privacy concerns must be evaluated against the advantages of the global information economy, this balance is vital.

3. The "Convention 108" of the Council of Europe, which protects individuals from the automated processing of their personal data, went into effect in 1981. It was the first legally binding international agreement to safeguard people against misuses that could result from the gathering and processing of personal data, and it strikes a balance between these rights and the unrestricted exchange of information between nations (Council of Europe, 1981).

The Convention emphasises, among other things, the principles of accurate data collection, fair and lawful processing, and data security. Notably, it emphasises that significant technical breakthroughs in the sphere of data processing must not violate individual rights while explicitly acknowledging these developments (Regan, 1995).

This Convention has a significant impact on the development of data protection regulations in Europe and worldwide. Convention 108 is the source of the General Data Protection Regulation (GDPR) adopted by the EU. Furthermore, because any nation is welcome to accede, the Convention's influence is universal. The promotion of privacy standards around the globe is significantly aided by their broad applicability (Kuner, 2007).

As of 2018, a revised version known as Convention 108 +, which added new principles like privacy by design, the idea of a data protection officer, and more specific rights for data subjects, was made available for signature (Council of Europe, 2018). This version further improved the framework for the protection of personal data.

4. A foundational text that outlines a wide spectrum of human rights is the International Covenant on Civil and Political Rights (ICCPR), which was adopted by the United Nations General Assembly in 1966. The United Nations General Assembly adopted it in 1966. It is a significant international convention that protects civil and political rights, including, among other things, the right to freedom of expression (Article 19) and the right to privacy (Article 17).

The freedom to express one's beliefs openly and to seek, receive, and share knowledge via any media without respect to geographical boundaries is guaranteed by Article 19. This article defends the free exchange of ideas and information, both of which are essential in the digital era and have significant consequences for information ethics.

Contrarily, Article 17 guarantees that no one's privacy, family, home, or correspondence shall be subjected to arbitrary or unlawful interference and safeguards people's honour and reputation. With the development of digital technology and the processing of personal data, which pose serious hazards to privacy if not handled morally and lawfully (Mendel, 2008), this subject assumes increasing importance.

The ICCPR provides an important global benchmark for evaluating organisational and governmental practises, notably in the area of information ethics. In the era of information and digital technology, it is crucial for establishing normative standards for individual rights.

5. The landscape of personal data protection within and outside of Europe has been drastically changed by the General Data Protection Regulation (GDPR), which was adopted in 2016 and became effective on May 25, 2018. The GDPR established a comprehensive set of guidelines for the processing and protection of personal data of EU citizens, affecting all organisations that handle such data, regardless of where they are physically located (Voigt and Von dem Bussche, 2017).

The right to access personal data, the right to correct mistakes, the right to have data erased (the "right to be forgotten"), and the right to restrict or object to data processing are some of the fundamental articles of the GDPR. The regulation further strengthened the penalties for non-compliance and added stricter criteria for getting express, informed consent for data collection and processing (Kuner, 2017).

The GDPR's introduction of the notion of "privacy by design," which requires organisations to include data privacy issues into the design and operation of their systems from the beginning rather than as an afterthought, may be its most revolutionary aspect (Kuner, 2017). Thus, the GDPR represents a turning point in the development of strong, thorough data protection rules, dramatically raising the bar for personal data protection on a global scale.

6. The UN Human Rights Council approved the "Ruggie Principles," or United Nations Guiding Principles on Business and Human Rights, in 2011. They created a global standard for mitigating and minimising the danger of unfavourable human rights effects associated with corporate operations (Ruggie, 2013). The guiding principles are founded on three pillars: the responsibility of the state to uphold human rights, the obligation of corporations to uphold human rights, and the necessity of providing victims of business-related abuses with access to the legal system.

These concepts have important implications for information ethics, especially in light of the growing digitization of trade and the crucial place that technology plays in modern business structures. For instance, these principles suggest that companies must take the necessary steps to safeguard individuals' right to privacy and freedom of expression throughout their supply chains and commercial operations (Methven O'Brien *et al.*, 2019). They must use due diligence in determining, preventing, mitigating, and accounting for their impacts on human rights, particularly those connected to information and communication technologies (ICTs), as well as how they resolve those impacts.

The UN Guiding Principles have influenced business advocacy for human rights and have been integrated into numerous pieces of national law and business practises. However, putting them into practise continues to be extremely difficult, especially in the digital age when human rights impacts can be intricate and wide-ranging.

7. In 2003, the UNESCO General Conference approved the organization's recommendation about the use of multilingualism and the promotion of universal access to the internet. This recommendation lays out guidelines for laws governing how people can acquire knowledge and information online. In addition to ensuring that everyone has access to information, it also strives to foster equal access to software and creative content (UNESCO, 2003).

The suggestion acknowledges that language is a key component of communication and is crucial for maintaining and enhancing the material and intangible legacy of human communities. It emphasises how communities and individuals may be empowered by having access to information in their own language. Languages that are underrepresented in the digital sphere run the risk of being marginalised as the internet and digital technology grow across the globe. As a result, the advice promotes the creation of local content in native tongues as well as the use of multilingual tools and services, including the creation and utilisation of software in native tongues (UNESCO, 2003).

The recommendation also highlights the significance of promoting open access to scientific knowledge and educational resources, notably for individuals with disabilities, and the necessity of universal access to digital and information resources (UNESCO, 2003).

In November 2021, the UNESCO Recommendation on the Ethics of Artificial Intelligence was approved, setting a key international benchmark for moral issues in the creation and application of AI. It offers a thorough set of rules and principles to make sure AI technologies uphold democracy, the rule of law, and human rights.

The advice emphasises how crucial it is to make sure AI systems are human-centric, fostering wellbeing, and upholding human dignity. It demands that AI should be utilised to promote fairness and non-discrimination, emphasising that everyone should have an equal opportunity to benefit from AI technology (UNESCO, 2021). It also emphasises transparency, accountability, and responsibility in AI applications.

The paper also supports the design, development, and application of AI in a way that respects security and privacy. Additionally, it emphasises the value of education and digital literacy to enable everyone to participate in and navigate an AI-driven society. The guideline also emphasises the need of open data and open-source software in AI development to increase openness and enable greater public scrutiny. To ensure that AI systems adhere to ethical and technical standards, it also demands for comprehensive assessment and auditing methods (UNESCO, 2021). This recommendation offers a crucial global framework for the ethical governance of AI that will direct legislators, researchers, and practitioners in creating laws, regulations, and practises that guarantee the creation and use of ethical AI.

We have examined numerous worldwide policies, guidelines and recommendations that aim to address the ethical ramifications of our increasingly digital society as we navigate the changing information ethics landscape. These rules offer the guiding principles for protecting personal information, human rights, and equality. We will use these fundamental ideas as a foundation for projecting and planning for the upcoming trends in information ethics as we move into the following part. We must take into account how current regulations may shape, and in turn, be affected by these emerging ethical landscapes in information science as a result of the introduction of cutting-edge technologies like artificial intelligence and machine learning as well as the ethical dilemmas they raise. Let's examine these upcoming prospects and difficulties as well as their effects on the future of information ethics as we move forward.

Future Trends

Information Ethics will continue to evolve and become more complex as the digital frontier expands. Several key trends are predicted to shape the future of Information Ethics:

Advanced AI Ethics: With the growth of AI and machine learning across various sectors, we foresee an increase in the need for comprehensive and sophisticated ethical guidelines surrounding their use (Russell *et al.*, 2015). The ethical implications of autonomous systems and advanced machine learning techniques will become ever more important as the technology advances (Bryson, 2016).
Data Privacy and Cybersecurity: As our world becomes increasingly digital, privacy and security concerns are expected to become even more crucial. Developments in cybersecurity strategies, technologies, and policies will aim to protect sensitive information in the face of evolving threats (White et al., 2012).
IoT Ethics: As the Internet of Things (IoT) expands with an increasing number of connected devices, the need for ethical guidelines specific to IoT will grow. Questions surrounding data privacy, security, and ownership will become more complex with the rise of interconnected devices in various facets of daily life (Roman *et al.*, 2013).
Online and Social Media Ethics: The exponential growth of social media and online platforms necessitates the ongoing development of ethical guidelines to manage issues such as hate speech, misinformation, and privacy (Van Dijck, 2013). As new platforms and technologies emerge, so too will new ethical considerations.
Digital Health Ethics: The increase in health-related data and digital health solutions will amplify the need for specific ethical considerations in health information management, focusing on issues such as data privacy, informed consent, and equitable access to health technologies (Mittelstadt and Floridi, 2016).
Blockchain and Cryptocurrency Ethics: The growing adoption of blockchain technologies and cryptocurrencies present a unique set of ethical challenges, including transparency, security, and potential impacts on global financial systems (Mougayar, 2016). These challenges will necessitate new ethical considerations and regulatory efforts.

Overall, the future of information ethics will be marked by a continuous need for vigilance and flexibility, as new technologies create new ethical quandaries and challenges. The key will be to maintain a focus on safeguarding privacy, promoting transparency, and ensuring equitable access in all aspects of information technology and science (Floridi, 2019).

Conclusion

Information ethics is a vital and important area that dynamically entwines with our developing digital world, in conclusion. This entry presents a view of the ethical issues by tracing its origins from the early discourse to more contemporary advancements. The discourse has been shaped by influential authors and foundational works, which have given us the theoretical frameworks we need to analyse the ethical conundrums related to information. Important ethical challenges like privacy, accuracy, intellectual property, access, and security have come to light in the information era, underscoring the importance of making wise ethical decisions.

As they navigate this environment, recognising ethical issues, developing guidelines, carrying out research, and raising awareness among others, information scientists' important role becomes clear. In addition, we saw how unique ethical problems are brought about by disruptive technologies like artificial intelligence (AI), the internet of things (IoT), blockchain, and digital health technologies.

We have witnessed the significance of international laws and regulations that establish the world's norms for information ethics, like the Universal Declaration of Human Rights, the EU General Data Protection Regulation, and UNESCO's recommendations. These legal frameworks serve as a testament to society's shared commitment to defending privacy and human rights in an interconnected world.

We found developing trends that point to the upcoming boundaries of information ethics by looking to the future. The complexity of ethical issues will increase as the information era advances, with potentially significant societal repercussions. Thus, information ethics continues to be a vital field that will influence how we interact with information and technologies in the years to come.

References

Future Directions in Digital Information: Predictions, 2021a. In: Baker, D., Ellis, L. (Eds.), Future Directions in Digital Information: Predictions Practice, Participation. Oxford: Chandos-Elsevier.
Baker, D., Ellis, L. (Eds.), 2021b. Libraries, Digital Information, and COVID: Practical Approaches to Challenge and Change. Oxford: Chandos-Elsevier.
Bielby, J., 2015. Comparative philosophies in intercultural information ethics. Confluence: Journal of World Philosophies. 2.
Bishop, M., 2003. What is computer security? IEEE Security & Privacy 1 (1), 67–69.
Böhme, R., Christin, N., Edelman, B., Moore, T., 2015. Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives 29 (2), 213–238.
Bower, J.L., Christensen, C.M., 1995. Disruptive technologies: Catching the wave.
Brenner, J.E., 2010. A logic of ethical information. *Knowledge*. technology & policy 23 (1–2), 109–133.
Brey, P., 2010. Philosophy of technology after the empirical turn. Techné: Research in philosophy and technology 14 (1), 36–48.
Britz, J.J., 1996. Technology as a threat to privacy: ethical challenges to the information profession. Microcomputers for Information Management 13 (3–4), 175–193.
Bryson, J., 2016. Artificial Intelligence and Pro-Social Behaviour. In Proceedings of the 2016 International Conference on Social Computing, Behavioral-Cultural Modeling & Prediction and Behavior Representation in Modeling and Simulation (pp. 1–6).
Buchanan, E.A., Hvizdak, E.E., 2009. Online survey tools: Ethical and methodological concerns of human research ethics committees. Journal of empirical research on human research ethics 4 (2), 37–48.
Bunnik, E.M., de Jong, A., Nijsingh, N., de Wert, G.M., 2013. The new genetics and informed consent: differentiating choice to preserve autonomy. Bioethics 27 (6), 348–355.
Burgess, T.F., Knox, J.M, 2019. Foundations of information ethics."Journal of Electronic Resources Librarianship 32 (4), 342–343.
Bynum, T. W., ed. 1985. Computers and Ethics. Blackwell. (Published as the October 1985 issue of *Metaphilosophy*).

Bynum, T.W., 2008. Norbert Wiener and the rise of information ethics. Information technology and moral philosophy. 8–25.
Bynum, T.W., 2010. Historical Roots of Information Ethics. In: *Handbook of Information and Computer Ethics*. Cambridge University Press, pp. 20–38. ISBN 978-0-521-88898-1.
Bynum, T.W., 2020. The historical roots of information and computer ethics. In: *The Ethics of Information Technologies*. Routledge, pp. 43–61.
Bynum, T.W., Maner, W., Fodor, J.L. (Eds.), 1992. *Teaching computer ethics*. Southern Connecticut State University.
Cyberphilosophy: the intersection of philosophy and computing. Bynum, T.W., Moor, J. (Eds.), Blackwell.
Bynum, T.W., Rogerson, S., 1996. Introduction and overview: Global information ethics. Science and Engineeringethics 2, 131–136.
Capurro, R. (2009). Digital ethics. In *2009 Global Forum on Civilization and Peace. Seoul, Dec*.
Capurro, R., 2010. Digital Ethics. Ethics and Information Technology.
Capurro, R., 1985. Moral issues in information science. Journal of information science 11 (3), 113–123.
Capurro, R., 2006. Towards an ontological foundation of information ethics. Ethics and Information Technology 8, 175–186.
Capurro, R., 2008. Intercultural information ethics: Foundations and applications. Journal of Information, Communication and Ethics in Society 6 (2), 116–126.
Capurro, R., 2017. Digitization as an ethical challenge. Ai & Society 32 (2), 277–283.
Chen, Y., Zhu, S., 2019. Demystifying the role of mobile technology in the patient's healthcare experience: a reference net perspective. Information & Management 56 (5), 705–719.
Council of Europe,1981. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.
Council of Europe, 2018. Modernised Convention for the protection of individuals with regard to the processing of personal data.
Dhillon, N.C., Lim, J., 2015. Socrates: The Father of Ethics and Inquiry. The Rosen Publishing Group, Inc.
Dhillon, G., Torkzadeh, G., 2006. Value-focused assessment of information system security in organizations. Information Systems Journal 16 (3), 293–314.
Van Dijck, J., 2013. The Culture of Connectivity: A Critical History of Social Media. Oxford University Press.
Djuraskovic, O., 2021. 30+ Big Data Statistics (2022) - Amount of Data Generated in The World. [online] Available at: https://firstsiteguide.com/big-data-stats/.
Dunn Cavelty, M., 2014. Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. Science and Engineering Ethics 20, 701–715.
EU, 2016. General Data Protection Regulation .
Floridi, L., 2011. The informational nature of personal identity. Minds and machines 21, 549–566.
Floridi, L., 2013. *The ethics of information*. USA: Oxford University Press.
Floridi, L., 2019. Translating principles into practices of digital ethics: Five risks of being unethical. Philosophy & Technology 32 (2), 185–193.
Floridi, L., 2008. Foundations of information ethics. The Handbook of Information and Computer Ethics. 1–23.
Froehlich, T., 2004. A brief history of information ethics.
Forester, T., Morrison, P., 1994. *Computer ethics: Cautionary tales and ethical dilemmas in computing*. Mit Press.
Greenbaum, D., Sboner, A., Mu, X.J., Gerstein, M., 2011. Genomics and privacy: Implications of the new reality of closed data for the field. PLOS Computational Biology 7 (12), e1002278.
Greenleaf, G., 2012. The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. International Data Privacy Law 2 (2), 68–92.
Heersmink, R., Van den Hoven, J., Van Eck, N., Van den Berg, J., 2012. Bibliometric mapping of computer and information ethics. Ethics and Information Technology 13 (3),
Introna, L.D., 2007. Maintaining the reversibility of foldings: Making the ethics (politics) of information technology visible. Ethics and Information Technology 9, 11–25.
Johnson, D.G., (1999). Sorting out the uniqueness of computer-ethical issues.
Johnson, D.G., 1985. Computer Ethics. Englewood Cliffs: Prentics-Hall.
Johnson, D.G., 1994. Computer ethics. Prentice-Hall, Inc.
Johnson, D.G., 2001. Computer Ethics. New Jersey: Prentice Hall. Inc.
Juengst, E.T., Flatt, M.A., Settersten Jr, R.A., 2012. Personalized genomic medicine and the rhetoric of empowerment. Hastings Center Report 42 (5), 34–40.
Kingsly, K.M., 2022. Disruptive Technology: Blockchain: The Crystal Ball: Advancing Financial Trust, Inclusion, and Simplicity Through the Blockchain. Christian Faith Publishing, Inc.
Knoppers, B.M., Thorogood, A.M., 2017. Ethics and big data in health. Current Opinion in Systems Biology 4, 53–57.
Kuner, C., 2007. European Data Protection law: Corporate Compliance and Regulation. Oxford University Press.
Kuner, C., 2017. The European Union General Data Protection Regulation: What it is and what it means. Information & Communications Technology Law 26 (1), 65–98.
Maner, W., 1980. Starter kit in Computer Ethics. Hyde Park, NY: Helvetia Press and the National Information and Resource Center for Teaching Philosophy, p. 3.
Maner, W., 1996. Unique ethical problems in information technology. Science and Engineering Ethics 2, 137–154.
Maner, W., 2002. Heuristic methods for computer ethics. Metaphilosophy 33 (3), 339–365.
Mason, R.O., 1986. Four Ethical Issues of the Information Age. MIS Quarterly 10 (1), 5–12. https://doi.org/10.2307/248873.
Mason, R.O., 2017. Four ethical issues of the information age. In: *Computer ethics*. Routledge, pp. 41–48.
Mendel, T., 2008. Freedom of Information: A Comparative Legal Survey, vol. 59. Paris: UNESCO.
Methven O'Brien, C., Hayes, A.R., Shin, I., 2019. Incorporating the guiding principles on business and human rights into the corporate DNA. Corporate Obligations Under International Law. Oxford University Press,. pp. 69–110.
Mingers, J., Walsham, G., 2010. Toward ethical information systems: The contribution of discourse ethics. MIS Quarterly. 833–854.
Mittelstadt, B.D., Allo, P., Taddeo, M., Wachter, S., Floridi, L., 2016. The ethics of algorithms: Mapping the debate. Big Data & Society 3 (2), 2053951716679679.
Mittelstadt, B.D., Floridi, L., 2016. The ethics of big data: current and foreseeable issues in biomedical contexts. The Ethics of Biomedical big Data. 445–480.
Moor, J.H., 1985. What is computer ethics? Metaphilosophy 16 (4), 266–275.
Moor, J.H., 1997. Towards a theory of privacy in the information age. "Computers and Society 27 (3), 27–32.
Moor, J.H., 1999. Just Consequentialism and Computing. "Ethics and Information Technology 1, 65–69.
Moor, J. H. (1991). The Ethics of Privacy Protection, "Library Trends", 39 (1 & 2)pp. 69–82.
Moor, J. H. (2001). The future of computer ethics: You ain't seen nothin' yet! "Ethics and Information Technology" 3. pp.2 89-91 https://doi.org/10.1023/A:1011881522593
Moor, J.H., 2005. Why we need better ethics for emerging technologies. "Ethics Inf Technol 7, 111–119. https://doi.org/10.1007/s10676-006-0008-0.
Mougayar, W., 2016. The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons.
Nissenbaum, H. Editorial. *Ethics and Information Technology* **1**, 171–172 (1999). https://doi.org/10.1023/A:1010068218051
Nissenbaum, H., 1998. Protecting Privacy in an Information Age: The Problem of Privacy in Public. Law and Philosophy 17, 559–596.
Nissenbaum, H., 2004. Privacy as contextual integrity. *Wash*. L. Rev. 79, 119.
Nissenbaum, H., 2009. Privacy in context: Technology, policy, and the integrity of social life. Redwood City: Stanford University Press, https://doi.org/10.1515/9780804772891.
Nissenbaum, H., 2011. A contextual approach to privacy online. Daedalus 140 (4), 32–48.
Nissenbaum, H., 2018. Respecting context to protect privacy: Why meaning matters. Science and engineering ethics 24 (3), 831–852.
Nissenbaum, H., Walker, D., 1998. A grounded approach to social and ethical concerns about technology and education. Journal of Educational Computing Research 19 (4), 411–432.
Ocholla, D.N., 2013. What is African Information Ethics. Information Ethics in Africa: Cross-Cutting Themes. 21–28.
OECD, 1980. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.Organization for the Economic Co-operation and Development. 2013. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
Price, W.N., Cohen, I.G., 2019. Privacy in the age of medical big data. Nature medicine 25 (1), 37–43.

Regan, P.M., 1995. Legislating Privacy: Technology, Social Values, and Public Policy. The University of North Carolina Press
Roman, R., Zhou, J., Lopez, J., 2013. On the features and challenges of security and privacy in distributed internet of things. Computer networks 57 (10), 2266–2279.
Ruggie, J.G., 2013. Just business: Multinational corporations and human rights (Norton global ethics series). WW Norton & Company.
Russell, S., Dewey, D., Tegmark, M., 2015. Research priorities for robust and beneficial artificial intelligence. AI Magazine 36 (4), 105–114.
Sojka, J., 1996. Business ethics and computer ethics: The view from Poland. Science and engineering ethics 2, 191–200.
Solove, D.J., 2006. A taxonomy of privacy. University of Pennsylvania Law Review 154 (3), 477–560.
Stahl, B.C., 2011. IT for a better future: How to integrate ethics, politics and innovation. Journal of Information, Communication and Ethics in Society 9 (3), 140–156.
Tapscott, D., Tapscott, A., 2016. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin.
Tomassi, P., 1999. Terrell Ward Bynum and James H. Moor (eds), The Digital Phoenix: How Computers are Changing Philosophy. BRITISH JOURNAL FOR THE PHILOSOPHY OF SCIENCE 50, 514–519.
UNESCO, 2021. Preliminary report on the first draft of the recommendation on the ethics of artificial intelligence.
UNESCO, 2011. The Media World after WikiLeaks and News of the World.
UNESCO, 2003. Recommendation Concerning the Promotion and use of Multilingualism and Universal Access to Cyberspace. Paris,France: UNESCO. Availableat:http://portal.unesco.org/en/ev.phpURL_ID=17717&URL_DO=DO_TOPIC&URL_SECTION=201.html
Vacca, J.R., 2009. Computer and Information Security Handbook. Burlington, MA: Morgan Kauffman, p. 208.
Voigt, P., Von dem Bussche, A., 2017. The EU General Data Protection Regulation (GDPR). A Practical Guide, A Practical Guide, 1st Ed, first ed., 10. Cham: Springer International Publishing, pp. 10–5555. 3152676.
White, J. D., Clarke, R. A., & Knake, R. K. (2012). Information Technology and Homeland Security.
Wiener, N., 1965. Perspectives in cybernetics. Progress in Brain Research 17, 399–415.
Woodward, B., Martin, N.L., Imboden, T., 2011. Expansion and validation of the PAPA framework. Information Systems Education Journal 9 (3), 28.