

PDF version of the entry  
Information Technology and Moral Values  
<https://plato.stanford.edu/archives/spr2021/entries/it-moral-values/>  
from the SPRING 2021 EDITION of the

## STANFORD ENCYCLOPEDIA OF PHILOSOPHY



Edward N. Zalta   Uri Nodelman   Colin Allen   R. Lanier Anderson  
Principal Editor   Senior Editor   Associate Editor   Faculty Sponsor

Editorial Board  
<https://plato.stanford.edu/board.html>

Library of Congress Catalog Data  
ISSN: 1095-5054

**Notice:** This PDF version was distributed by request to members of the Friends of the SEP Society and by courtesy to SEP content contributors. It is solely for their fair use. Unauthorized distribution is prohibited. To learn how to join the Friends of the SEP Society and obtain authorized PDF versions of SEP entries, please visit <https://leibniz.stanford.edu/friends/>.

*Stanford Encyclopedia of Philosophy*  
Copyright © 2021 by the publisher  
The Metaphysics Research Lab  
Center for the Study of Language and Information  
Stanford University, Stanford, CA 94305  
Information Technology and Moral Values  
Copyright © 2021 by the author  
John Sullins

All rights reserved.

Copyright policy: <https://leibniz.stanford.edu/friends/info/copyright/>

## Information Technology and Moral Values

*First published Tue Jun 12, 2012; substantive revision Fri Nov 9, 2018*

Every action we take leaves a trail of information that could, in principle, be recorded and stored for future use. For instance, one might use the older forms of information technologies of pen and paper and keep a detailed diary listing all the things one did and thought during the day. It might be a daunting task to record all this information this way but there are a growing list of technologies and software applications that can help us collect all manner of data, which in principle, and in practice, can be aggregated together for use in building a data profile about you, a digital diary with millions of entries. Some examples of which might be: a detailed listing of all of your economic transactions; a GPS generated plot of where you traveled; a list of all the web addresses you visited and the details of each search you initiated online; a listing of all your vital signs such as blood pressure and heart rate; all of your dietary intakes for the day; and any other kind of data that can be measured. As you go through this thought experiment you begin to see the complex trail of data that you generate each and every day and how that same data might be efficiently collected and stored though the use of information technologies. It is here we can begin to see how information technology can impact moral values. As this data gathering becomes more automated and ever-present, we must ask who is in control of collecting this data and what is done with it once it has been collected and stored? Which bits of information should be made public, which held private, and which should be allowed to become the property of third parties like corporations? Questions of the production, access, and control of information will be at the heart of moral challenges surrounding the use of information technology.

One might argue that the situation just described is no different from the moral issues revolving around the production, access, and control of any

basic necessity of life. If one party has the privilege of the exclusive production, access, and/or control of some natural resource, then that by necessity prohibits others from using this resource without the consent of the exclusive owner. This is not necessarily so with digital information. Digital information is nonexclusory, meaning we can all, at least theoretically, possess the same digital information without excluding its use from others. This is because copying digital information from one source to another does not require eliminating the previous copy. Unlike a physical object, theoretically, we can all possess the same digital object as it can be copied indefinitely with no loss of fidelity. Since making these copies is often so cheap that it is almost without cost, there is no technical obstacle to the spread of all information as long as there are people willing to copy it and distribute it. Only appeals to morality, or economic justice might prevent the distribution of certain forms of information. For example, digital entertainment media, such as songs or video, has been a recurring battleground as users and producers of the digital media fight to either curtail or extend the free distribution of this material. Therefore, understanding the role of moral values in information technology is indispensable to the design and use of these technologies (Johnson, 1985, Moore, 1985, Nissenbaum, 1998, Spinello, 2001). It should be noted that this entry will not directly address the phenomenological approach to the ethics of information technology since there is a detailed entry on this subject available (see the entry on phenomenological approaches to ethics and information technology).

- 1. Introduction
- 2. The Moral Challenges of Information Technology
  - 2.1 The Fundamental Character of Information Technologies
    - 2.1.1 Moral Values in Information Recording
    - 2.1.2 Moral Values in Communicating and Accessing Information
    - 2.1.3 Moral Values in Organizing and Synthesizing

## Information

- 2.2 The Moral Paradox of Information Technologies
- 3. Specific Moral Challenges at the Cultural Level
  - 3.1 Social Media and Networking
    - 3.1.1 Online Games and Worlds
    - 3.1.2 The Lure of the Virtual Game Worlds
    - 3.1.3 The Technological Transparency Paradox
  - 3.3 Malware, Spyware and Informational Warfare
  - 3.4 Future Concerns
    - 3.4.1 Acceleration of Change
    - 3.4.2 Artificial Intelligence and Artificial Life
    - 3.4.3 Robotics and Moral Values
- 4. Information Technologies of Morality
  - 4.1 Information Technology as a Model for Moral Discovery
  - 4.2 Information Technology as a Moral System
  - 4.3 Informational Organisms as Moral Agents
- Bibliography
- Academic Tools
- Other Internet Resources
- Related Entries

---

## 1. Introduction

Information technology is ubiquitous in the lives of people across the globe. These technologies take many forms such as personal computers, smart phones, internet technologies, as well as AI and robotics. In fact, the list is growing constantly and new forms of these technologies are working their way into every aspect of daily life. They all have some form of computation at their core and human users interface with them mostly through applications and other software operating systems. In some cases, such as massive multiplayer online games (see section 3.1.1 below), these

technologies are even opening up new ways for humans to interacting with each other. Information technologies are used to record, communicate, synthesize or organize information through the use of computer technologies. Information itself can be understood as any useful data, instructions, or meaningful message content. The word literally means to “give form to” or to shape one’s thoughts. A basic type of information technology might be the proverbial string tied around one’s finger that is used to remind, or inform, someone that they have some specific task to accomplish that day. Here the string stands in for a more complex proposition such as “buy groceries before you come home.” The string itself is not the information, it merely symbolizes the information and therefore this symbol must be correctly interpreted for it to be useful. Which raises the question, what is information itself?

Unfortunately there is not a completely satisfying and philosophically rigorous definition available, though there are at least two very good starting points. For those troubled by the ontological questions regarding information, we might want to simply focus on the symbols and define information as any meaningfully ordered set of symbols. Mathematicians and engineers prefer to focus on this aspect of information, which is called “syntax” and leave the meaningfulness of information or its “semantics” for others to figure out. Claude E. Shannon working at Bell Labs in the forties produced a landmark mathematical theory of communication (1948). In this work he utilized his experiences in cryptography and telephone technologies to work out a mathematical formulation describing how syntactical information can be turned into a signal that is transmitted in such a way as to mitigate noise or other extraneous signals which can then be decoded by the desired receiver of the message (Shannon 1948; Shannon and Weaver 1949). The concepts described by Shannon, (along with additional important innovations made by others who are too many to list), explain the way that information technology works, but we still have the deeper questions to resolve if we want to thoroughly trace the impact

of information technologies on moral values. Some philosophers noted the fact that information technologies had highlighted the distinction between syntax and semantics, and have been vocal critics about the inability of technologies to bridge the gap between the two concepts. Meaning that while information technologies might be adept at manipulating syntax, they would be incapable of ever understanding the semantics, or meanings, of the information upon which they worked.

One famous example can be found in the “Chinese Room Argument” (Searle 1980) in which the philosopher John Searle argued that even if one were to build a machine that could take stories written in Chinese as input and then output coherent answers to questions about those stories, it would not prove that the machine itself actually understood what it was doing. The argument rests on the claim that if you replaced the workings of the machine with a person who was not a native Chinese speaker who would then painstakingly follow a set of rules to transform the set of Chinese logograms input into other output symbols. The claim is that that person would not understand the input and also would not know what the system is saying as its output, it is all meaningless symbol manipulation to them. The conclusion is that this admittedly strange system could skillfully use the syntax of the language and story while the person inside would have no ability to understand the semantics, or meaning, of the stories (Searle 1980). Replace the person with electronics and it follows that the electronics also have no understanding of the symbols they are processing. This argument, while provocative is not universally accepted and has lead to decades worth of argument and rebuttal (see the entry on The Chinese Room Argument).

Information technology has also had a lasting impression on the philosophical study of logic and information. In this field logic is used as a way to understand information as well as using information science as a

way to build the foundations of logic itself (see the entry on logic and information).

The issues just discussed are fascinating but they are separate arguments that do not necessarily have to be resolved before we can enter a discussion on information technology and moral values. Even purely syntactical machines can still impact many important ethical concerns even if they are completely oblivious to the semantic meaning of the information that they compute.

The second starting point is to explore the more metaphysical role that information might play in philosophy. If we were to begin with the claim that information either constitutes or is closely correlated with what constitutes our existence and the existence of everything around us, then this claim means that information plays an important ontological role in the manner in which the universe operates. Adopting this standpoint places information as a core concern for philosophy and gives rise to the fields philosophy of information and information ethics. In this entry, we will not limit our exploration to just the theory of information but instead look more closely at the actual moral and ethical impacts that information technologies are already having on our societies. Philosophy of Information will not be addressed in detail here but the interested reader can begin with Floridi (2010b, 2011b) for an introduction. Some of the most important aspects of Information Ethics will be outlined in more detail below.

## 2. The Moral Challenges of Information Technology

The move from one set of dominant information technologies to another is always morally contentious. Socrates lived during the long transition from a largely oral tradition to a newer information technology consisting of writing down words and information and collecting those writings into

scrolls and books. Famously Socrates was somewhat antagonistic to writing and scholars claim that he never wrote anything down himself. Ironically, we only know about Socrates' argument against writing because his student Plato ignored his teacher and wrote them down in a dialogue called "Phaedrus" (Plato). Towards the end of this dialogue Socrates discusses with his friend Phaedrus the "...conditions which make it (writing) proper or improper" (section 274b–479c). Socrates tells a fable of an Egyptian God he names Theuth who gives the gift of writing to a king named Thamus. Thamus is not pleased with the gift and replies,

If men learn this, it will implant forgetfulness in their souls; they will cease to exercise memory because they rely on that which is written, calling things to remembrance no longer from within themselves, but by means of external marks. (Phaedrus, section 275a)

Socrates, who was adept at quoting lines from poems and epics and placing them into his conversations, fears that those who rely on writing will never be able to truly understand and live by these words. For Socrates there is something immoral or false about writing. Books can provide information but they cannot, by themselves, give you the wisdom you need to use or deeply understand that information. Conversely, in an oral tradition you do not simply consult a library, you are the library, a living manifestation of the information you know by heart. For Socrates, reading a book is nowhere near as insightful as talking with its author. Written words,

...seem to talk to you as though they were intelligent, but if you ask them anything about what they say, from a desire to be instructed, they go on telling you the same thing forever. (Phaedrus, section 275d).

His criticism of writing at first glance may seem humorous but the temptation to use recall and call it memory is getting more and more prevalent in modern information technologies. Why learn anything when information is just an Internet search away? In order to avoid Socrates' worry, information technologies should do more than just provide access to information; they should also help foster wisdom and understanding as well.

## 2.1 The Fundamental Character of Information Technologies

Early in the information technology revolution Richard Mason suggested that the coming changes in information technologies, such as their roles in education and economic impacts, would necessitate rethinking the social contract (Mason 1986). He worried that they would challenge privacy, accuracy, property and accessibility (PAPA) and to protect our society we "... must formulate a new social contract, one that insures everyone the right to fulfill his or her own human potential" (Mason 1986 P. 11) What he could not have known then was how often we would have to update the social contract as these technologies rapidly change. Information technologies change quickly and move in and out of fashion at a bewildering pace. This makes it difficult to try to list them all and catalog the moral impacts of each. The very fact that this change is so rapid and momentous has caused some to argue that we need to deeply question the ethics of the process of developing emerging technologies (Moor 2008). It has also been argued that the ever morphing nature of information technology is changing our ability to even fully understand moral values as they change. Lorenzo Magnani claims that acquiring knowledge of how that change confounds our ability to reason morally "...has become a duty in our technological world" (Magnani 2007, 93). The legal theorist Larry Lessig warns that the pace of change in information technology is so rapid

that it leaves the slow and deliberative process of law and political policy behind and in effect these technologies become lawless, or extralegal. This is due to the fact that by the time a law is written to curtail, for instance, some form of copyright infringement facilitated by a particular file sharing technology, that technology has become out of date and users are on to something else that facilitates even more copyright infringement (Lessig 1999). But even given this rapid pace of change, it remains the case that information technologies or applications can all be categorized into at least three different types – each of which we will look at below.

All information technologies record (store), transmit (communicate), organize and/or synthesize information. For example, a book is a record of information, a telephone is used to communicate information, and the Dewey decimal system organizes information. Many information technologies can accomplish more than one of the above functions and, most notably, the computer can accomplish all of them since it can be described as a universal machine (see the entry on Computability and Complexity), so it can be programmed to emulate any form of information technology. In section 2 we will look at some specific example technologies and applications from each of the three types of information technology listed above and track the moral challenges that arise out of the use and design of these particular technologies. In addition to the above we will need to address the growing use of information environments such as massive multiplayer games, which are environments completely composed of information where people can develop alternate lives filled with various forms of social activities (see section 3.3). Finally we will look at not only how information technology impacts our moral intuitions but also how it might be changing the very nature of moral reasoning. In section 4, we will look at information as a technology of morality and how we might program applications and robots to interact with us in a more morally acceptable manner.

### 2.1.1 Moral Values in Information Recording

The control of information is power, and in an information economy such as we find ourselves today, it may be the ultimate form of political power. We live in a world rich in data and the technology to produce, record, and store vast amounts of this data has developed rapidly. The primary moral concern here is that when we collect, store, and/or access information, it is vital that this be done in a just manner that can reasonably be seen as fair and in the best interests of all parties involved. As was mentioned above, each of us produces a vast amount of information every day that could be recorded and stored as useful data to be accessed later when needed. But moral conundrums arise when that collection, storage and use of our information is done by third parties without our knowledge or done with only our tacit consent. The social institutions that have traditionally exercised this power are things like, religious organizations, universities, libraries, healthcare officials, government agencies, banks and corporations. These entities have access to stored information that gives them a certain amount of power over their customers and constituencies. Today each citizen has access to more and more of that stored information without the necessity of utilizing the traditional mediators of that information and therefore a greater individual share of social power (see Lessig 1999).

One of the great values of modern information technology is that it makes the recording of information easy and almost automatic. Today, a growing number of people enter biometric data such as blood pressure, calorie intake, exercise patterns, etc. into applications designed to help them achieve a healthier lifestyle. This type of data collection could become almost fully automated in the near future. Through the use of smart watches or technologies such as the “Fitbit,” or gathered through a users smartphone, such as applications that use the GPS tracking to track the

length and duration of a user’s walk or run. How long until a smartphone collects a running data stream of your blood pressure throughout the day perhaps tagged with geolocation markers of particularly high or low readings? In one sense this could be immensely powerful data that could lead to much healthier lifestyle choices. But it could also be a serious breach in privacy if the information got into the wrong hands, which could be easily accomplished, since third parties have access to information collected on smartphones and online applications. In the next section (2.1.2) we will look at some theories on how best to ethically communicate this recorded information to preserve privacy. But here we must address a more subtle privacy breach – the collection and recording of data about a users without their knowledge or consent. When searching on the Internet, browser software records all manner of data about our visits to various websites which can, for example, make webpages load faster next time you visit them. Even the websites themselves use various means to record information when your computer has accessed them and they may leave bits of information on your computer which the site can use the next time you visit. Some websites are able to detect which other sites you have visited or which pages on the website you spend the most time on. If someone were following you around a library noting down this kind of information, you might find it uncomfortable or hostile, but online this kind of behavior takes place behind the scenes and is barely noticed by the casual user.

According to some professionals, information technology has all but eliminated the private sphere and that it has been this way for decades. Scott McNealy of Sun Microsystems famously announced in 1999: “You have zero privacy anyway. Get over it” (Sprenger, 1999). Helen Nissenbaum observes that,

[w]here previously, physical barriers and inconvenience might have discouraged all but the most tenacious from ferreting out

information, technology makes this available at the click of a button or for a few dollars (Nissenbaum 1997)

and since the time when she wrote this the gathering of personal data has become more automated and cheaper. Clearly, earlier theories of privacy that assumed the inviolability of physical walls no longer apply but as Nissenbaum argues, personal autonomy and intimacy require us to protect privacy nonetheless (Nissenbaum 1997).

A final concern in this section is that information technologies are now storing user data in “the cloud” meaning that the data is stored on a device remotely located from the user and not owned or operated by that user, but the data is then available from anywhere the user happens to be, on any device they happen to be using. This ease of access has the result of also making the relationship one has to one’s own data more tenuous because of the uncertainty about the physical location of that data. Since personal data is crucially important to protect, the third parties that offer “cloud” services need to understand the responsibility of the trust the user is placing in them. If you load all the photographs of your life to a service like Flickr and they were to somehow lose or delete them, this would be a tragic mistake that might not be impossible to repair.

### 2.1.2 Moral Values in Communicating and Accessing Information

Information technology has forced us to rethink earlier notions of privacy that were based on print technologies, such as letters, notes, books, pamphlets, newspapers, etc. The moral values that coalesced around these earlier technologies have been sorely stretched by the easy way that information can be shared and altered using digital information technologies and this has required the rapid development of new moral theories that recognize both the benefits and risks of communicating all

manner of information using modern information technologies. The primary moral values that seem to be under pressure from these changes are privacy, confidentiality, ownership, trust, and the veracity of the information being communicated in these new ways.

Who has the final say whether or not some information about a user is communicated or not? Who is allowed to sell your medical records, your financial records, your email, your browser history, etc.? If you do not have control over this process, then how can you enforce your own moral right to privacy? For instance Alan Westin argued in the very early decades of the advance of digital information technologies that control of access to one’s personal information was the key to maintaining privacy (Westin, 1967). It follows that if we care about privacy, then we should give all the control of access to personal information to the individual. Most corporate entities resist this notion for the simple reason that information about users has become a primary commodity in the digital world boosting the vast fortunes of corporations like Google or Facebook. Indeed, there is a great deal of utility each of us gains from the services provided by internet search companies like Google and social networks such as Facebook. It might be argued that it is actually a fair exchange we receive since they provide search results and other applications for free and they offset the cost of creating those valuable serviced by collecting data from individual user behavior that can be monetized in various lucrative ways. A major component of the profit model for these companies is based on directed advertising where the information collected on the user is used to help identify advertising that will be most effective on a particular user based on his or her search history and other online behaviors. Simply by using the free applications offered, each user tacitly agrees to give up some amount of privacy that varies with the applications they are using. Even if we were to agree that there is some utility to the services users receive in this exchange, there are still many potential moral problems with this arrangement. If we follow the argument

raised by Westin earlier that privacy is equivalent to information control (ibid.), then we do seem to be ceding our privacy away little by little given that we have almost no control or even much understanding of the vast amounts of digital information that is collected about us.

There is a counterargument to this. Herman Tavani and James Moor (2004) argue that in some cases giving the user more control of their information may actually result in greater loss of privacy. Their primary argument is that no one can actually control all of the information about oneself that is produced every day by our activities. If we focus only on the fraction of it that we can control, we lose sight of the vast mountains of data we cannot (Tavani and Moor, 2004). Tavani and Moor argue that privacy must be recognized by the third parties that do control your information and only if those parties have a commitment to protecting user privacy, will we actually acquire any privacy worth having. Towards this end, they suggest that we think in terms of restricted access to information rather than strict personal control of information (ibid).

Information security is another important moral value that impacts the communication and access of user information. If we grant the control of our information to third parties in exchange for the services they provide, then these entities must also be responsible for restricting the access to that information by others who might use it to harm us (See Epstein 2007; Magnani 2007; Tavani 2007). With enough information, a person's entire identity can be stolen and used to facilitate fraud and larceny. This type of crime has grown rapidly since the advent of digital information technologies. The victims of these crimes can have their lives ruined as they try to rebuild such things as their credit rating and bank accounts. This has led to the design of computer systems that are more difficult to access and the growth of a new industry dedicated to securing computer systems. Even with these efforts the economic and social impact of cybercrime is growing at a staggering rate. In February of 2018 the cyber-

security company McAfee released a report that estimated the world cost in cybercrime was up from \$445 billion in 2014 to \$608 billion dollars or 0.8 of the global GDP in 2018, and that is not counting the hidden costs of increased friction and productivity loss in time spent trying to fight cybercrime (McAfee 2018).

The difficulty in obtaining complete digital security rests on the fact that the moral value of security can be in conflict with the moral values of sharing and openness, and it is these later values that guided many of the early builders of information technology. Steven Levy (1984) describes in his book, "Hackers: Heroes of the Computer Revolution," a kind of "Hacker ethic," that includes the idea that computers should be freely accessible and decentralized in order to facilitate "world improvement" and further social justice (Levy 1984; see also Markoff 2005). So it seems that information technology has a strong dissonance created in the competing values of security and openness that is worked right into the design of these technologies and this is all based on the competing moral values held by the various people who designed the technologies themselves.

This conflict in values has been debated by philosophers. While many of the hackers interviewed by Levy argue that hacking is not as dangerous as it seems and that it is mostly about gaining access to hidden knowledge of how information technology systems work, Eugene Spafford counters that no computer break-in is entirely harmless and that the harm precludes the possibility of ethical hacking except in the most extreme cases (Spafford 2007). Kenneth Himma largely agrees that the activity of computer hacking is unethical but that politically motivated hacking or "Hacktivism" may have some moral justification, though he is hesitant to give his complete endorsement of the practice due to the largely anonymous nature of the speech entailed by the hacktivist protests (Himma 2007b). Mark Manion and Abby Goodrum agree that hacktivism



could be a special case of ethical hacking but warn that it should proceed in accordance to the moral norms set by the acts of civil disobedience that marked the twentieth century or risk being classified as online terrorism (Manion and Goodrum 2007).

A very similar value split plays out in other areas as well, particularly in the field of intellectual property rights (see entry on Intellectual Property/) and pornography and censorship (see entry on Pornography and Censorship). What information technology adds to these long standing moral debates is the nearly effortless access to information that others might want to control such as intellectual property, dangerous information and pornography (Floridi 1999), as well as providing technological anonymity for both the user and those providing access to the information in question (Nissenbaum 1999; Sullins 2010). For example, even though cases of bullying and stalking occur regularly, the anonymous and remote actions of cyber-bullying and cyberstalking make these behaviors much easier and the perpetrator less likely to be caught. Given that information technologies can make these unethical behaviors more likely, then it can be argued that the design of cyberspace itself tacitly promotes unethical behavior (Adams 2002; Grodzinsky and Tavani 2002). Since the very design capabilities of information technology influence the lives of their users, the moral commitments of the designers of these technologies may dictate the course society will take and our commitments to certain moral values will then be determined by technologists (Brey 2010; Bynum 2000; Ess 2009; Johnson 1985; Magnani 2007; Moor 1985; Spinello 2001; Sullins 2010).

Assuming we are justified in granting access to some store of information that we may be in control of, there is a duty to ensure that that information is truthful, accurate, and useful. A simple experiment will show that information technologies might have some deep problems in this regard. Load a number of different search engines and then type the same search

terms in each of them, each will present different results and some of these searches will vary widely from one another. This shows that each of these services uses a different proprietary algorithm for presenting the user with results from their search. It follows then that not all searches are equal and the truthfulness, accuracy, and usefulness of the results will depend greatly on which search provider you are using and how much user information is shared with this provider. All searches are filtered by various algorithms in order to ensure that the information the search provider believes is most important to the user is listed first. Since these algorithms are not made public and are closely held trade secrets, users are placing a great deal of trust in this filtering process. The hope is that these filtering decisions are morally justifiable but it is difficult to know. A simple example is found in “clickjacking.” If we are told a link will take us to one location on the web yet when we click it we are taken to some other place, the user may feel that this is a breach of trust. This is often called “clickjacking” and malicious software can clickjack a browser by taking the user to some other site than what is expected; it will usually be rife with other links that pay the clickjacker for bringing traffic to them (Hansen and Grossman, 2008). Again the anonymity and ease of use that information technology provides can facilitate deceitful practices such as clickjacking. Pettit (2009) suggests that this should cause us to reevaluate the role that moral values such as trust and reliance play in a world of information technology. Anonymity and the ability to hide the authors of news reports online has contributed to the raise of “fake news” or propaganda of various sorts posing as legitimate news. This is a significant problem and will be discussed in section (2.2.3) below

Lastly in this section we must address the impact that the access to information has on social justice. Information technology was largely developed in the Western industrial societies during the twentieth century. But even today the benefits of this technology have not spread evenly around the world and to all socioeconomic demographics. Certain

societies and social classes have little to no access to the information easily available to those in more well off and in developed nations, and some of those who have some access have that access heavily censored by their own governments. This situation has come to be called the “digital divide,” and despite efforts to address this gap it may be growing wider. It is worth noting that as the cost of smart phones decreases these technologies are giving some access to the global internet to communities that have been shut out before (Poushter 2016). While much of this gap is driven by economics (see Warschauer 2003), Charles Ess notes that there is also a problem with the forces of a new kind of cyber enabled colonialism and ethnocentrism that can limit the desire of those outside the industrial West to participate in this new “Global Metropolis” (Ess 2009). John Weckert also notes that cultural differences in giving and taking offence play a role in the design of more egalitarian information technologies (Weckert 2007). Others argue that basic moral concerns like privacy are weighed differently in Asian cultures (Hongladarom 2008; Lü 2005).

### 2.1.3 Moral Values in Organizing and Synthesizing Information

In addition to storing and communicating information, many information technologies automate the organizing of information as well as synthesizing or mechanically authoring or acting on new information. Norbert Wiener first developed a theory of automated information synthesis which he called *Cybernetics* (Wiener 1961 [1948]). Wiener realized that a machine could be designed to gather information about the world, derive logical conclusions about that information which would imply certain actions, which the machine could then implement, all without any direct input from a human agent. Wiener quickly saw that if his vision of cybernetics was realized, there would be tremendous moral concerns raised by such machines and he outlined some of them in his

book *the Human Use of Human Beings* (Wiener 1950). Wiener argued that, while this sort of technology could have drastic moral impacts, it was still possible to be proactive and guide the technology in ways that would increase the moral reasoning capabilities of both humans and machines (Bynum 2008).

Machines make decisions that have moral impacts. Wendell Wallach and Colin Allen tell an anecdote in their book “Moral Machines” (2008). One of the authors left on a vacation and when he arrived overseas his credit card stopped working, perplexed, he called the bank and learned that an automatic anti-theft program had decided that there was a high probability that the charges he was trying to make were from someone stealing his card and that in order to protect him the machine had denied his credit card transactions. Here we have a situation where a piece of information technology was making decisions about the probability of nefarious activity happening that resulted in a small amount of harm to the person that it was trying to help. Increasingly, machines make important life changing financial decisions about people without much oversight from human agents. Whether or not you will be given a credit card, mortgage loan, the price you will have to pay for insurance, etc., is very often determined by a machine. For instance if you apply for a credit card, the machine will look for certain data points, like your salary, your credit record, the economic condition of the area you reside in, etc., and then calculate the probability that you will default on your credit card. That probability will either pass a threshold of acceptance or not and determine whether or not you are given the card. The machine can typically learn to make better judgments given the results of earlier decisions it has made. This kind of machine learning and prediction is based on complex logic and mathematics (see for example, Russell and Norvig 2010), this complexity may result in slightly humorous examples of mistaken predictions as told in the anecdote above, or it might be more eventful. For example, the program may interpret the data regarding the identity of

one's friends and acquaintances, his or her recent purchases, and other readily available social data, which might result in the mistaken classification of that person as a potential terrorist, thus altering that person's life in a powerfully negative way (Sullins 2010). It all depends on the design of the learning and prediction algorithm, something that is typically kept secret, so that it is hard to justify the veracity of the prediction.

## 2.2 The Moral Paradox of Information Technologies

Several of the issues raised above result from the moral paradox of Information technologies. Many users want information to be quickly accessible and easy to use and desire that it should come at as low a cost as possible, preferably free. But users also want important and sensitive information to be secure, stable and reliable. Maximizing our value of quick and low cost minimizes our ability to provide secure and high quality information and the reverse is true also. Thus the designers of information technologies are constantly faced with making uncomfortable compromises. The early web pioneer Stewart Brand sums this up well in his famous quote:

In fall 1984, at the first Hackers' Conference, I said in one discussion session: "On the one hand information wants to be expensive, because it's so valuable. The right information in the right place just changes your life. On the other hand, information wants to be free, because the cost of getting it out is getting lower and lower all the time. So you have these two fighting against each other" (Clarke 2000—see Other Internet Resources)<sup>[1]</sup>

Since these competing moral values are essentially impossible to reconcile, they are likely to continue to be at the heart of moral debates in the use and design of information technologies for the foreseeable future.

## 3. Specific Moral Challenges at the Cultural Level

In the section above, the focus was on the moral impacts of information technologies on the individual user. In this section, the focus will be on how these technologies shape the moral landscape at the societal level. At the turn of the twentieth century the term "web 2.0" began to surface and it referred to the new way that the world wide web was being used as a medium for information sharing and collaboration as well as a change in the mindset of web designers to include more interoperability and user-centered experiences on their websites. This term has also become associated with "social media" and "social networking." While the original design of the World Wide Web in 1989 by its creator Tim Berners-Lee was always one that included notions of meeting others and collaborating with them online, users were finally ready to fully exploit those capabilities by 2004 when the first Web 2.0 conference was held by O'Reilly Media (O'Reilly 2007 [2005]). This change has meant that a growing number of people have begun to spend significant portions of their lives online with other users experiencing a new unprecedented lifestyle. Social networking is an important part of many people's lives worldwide. Vast numbers of people congregate on sites like Facebook and interact with friends old and new, real and virtual. The Internet offers the immersive experience of interacting with others in virtual worlds where environments are constructed entirely out of information. Just now, emerging onto the scene are technologies that will allow us to merge the real and the virtual. This new form of "augmented reality" is facilitated by the fact that many people now carry GPS enabled smart phones and other portable computers with them upon which they can run applications that let them interact with their surroundings and their computers at the same time, perhaps looking at an item through the camera in their device and the "app" calling up information about that entity and displaying it in a bubble

above the item. Each of these technologies comes with their own suite of new moral challenges some of which will be discussed below.

### 3.1 Social Media and Networking

Social networking is a term given to sites and applications which facilitate online social interactions that typically focus on sharing information with other users referred to as “friends.” The most famous of these sites today is Facebook but there are many others, such as Instagram, Twitter, Snapchat, to name just a few. There are a number of moral values that these sites call into question. Shannon Vallor (2011, 2016) has reflected on how sites like Facebook change or even challenge our notion of friendship. Her analysis is based on the Aristotelian theory of friendship (see entry on Aristotle’s ethics). Aristotle argued that humans realize a good and true life through virtuous friendships. Vallor notes that four key dimensions of Aristotle’s ‘virtuous friendship,’ namely: reciprocity, empathy, self-knowledge and the shared life, and that the first three are found in online social media in ways that can sometimes strengthen friendship (Vallor 2011, 2016). Yet she argues that social media is not yet up to the task of facilitating what Aristotle calls ‘the shared life.’ Meaning that social media can give us shared activities but not the close intimate friendship that shared daily lives can give. (Here is a more complete discussion of Aristotelian friendship). Thus these media cannot fully support the Aristotelian notion of complete and virtuous friendship by themselves (Vallor 2011). Vallor also has a similar analysis of other Aristotelian virtues such as patience, honesty, and empathy and their problematic application in social media (Vallor 2010). Vallor has gone on to argue that both the users and designers of information technologies need to develop a new virtue that she terms “technomoral wisdom” which can help us foster better online communities and friendships (Vallor, 2016).

Johnny Hartz Søraker (2012) argues for a nuanced understanding of online friendship rather than a rush to normative judgement on the virtues of virtual friends.

Privacy issues abound in the use of social media. James Parrish following Mason (1986) recommends four policies that a user of social media should follow to ensure proper ethical concern for other’s privacy:

1. When sharing information on SNS (social network sites), it is not only necessary to consider the privacy of one’s personal information, but the privacy of the information of others who may be tied to the information being shared.
2. When sharing information on SNS, it is the responsibility of the one desiring to share information to verify the accuracy of the information before sharing it.
3. A user of SNS should not post information about themselves that they feel they may want to retract at some future date. Furthermore, users of SNS should not post information that is the product of the mind of another individual unless they are given consent by that individual. In both cases, once the information is shared, it may be impossible to retract.
4. It is the responsibility of the SNS user to determine the authenticity of a person or program before allowing the person or program access to the shared information. (Parrish 2010)

These systems are not normally designed to explicitly infringe on individual privacy, but since these services are typically free there is a strong economic drive for the service providers to harvest at least some information about their user’s activities on the site in order to sell that information to advertisers for directed marketing. This marketing can be done with the provider just selling access to users’ data that has been made anonymous, so that the advertiser knows that the user may be likely to buy

a pair of jeans but they do not be given the exact identity of that person. In this way a social network provider can try to maintain the moral value of privacy for its users while still profiting off of linking them with advertisers.

### 3.1.1 Online Games and Worlds

The first moral impact one encounters when contemplating online games is the tendency for these games to portray violence, sexism, and sexual violence. There are many news stories that claim a cause and effect relationship between violence in computer games and real violence. The claim that violence in video games has a causal connection to actual violence has been strongly critiqued by the social scientist Christopher J. Ferguson (Ferguson 2007). However, Mark Coeckelbergh argues that since this relationship is tenuous at best and that the real issue at hand is the effect these games have on one's moral character (Coeckelbergh 2007). But Coeckelbergh goes on to claim that computer games could be designed to facilitate virtues like empathy and cosmopolitan moral development, thus he is not arguing against all games just those where the violence inhibits moral growth (Coeckelbergh 2007). A good example of this might be the virtual reality experience that was designed by Planned Parenthood in 2017, "...which focuses on the experience of accessing abortion in America, positively influences the way viewers feel about the harassment that many patients, providers, and health center staff experience from opponents of safe, legal abortion" (Planned Parenthood, 2017).

Marcus Schulzke (2010) defends the depiction of violence in video games. Schulzke's main claim is that actions in a virtual world are very different from actions in the real world. Although a player may "kill" another player in a virtual world, the offended player is instantly back in the game

and the two will almost certainly remain friends in the real world. Thus virtual violence is very different from real violence, a distinction that gamers are comfortable with (Schulzke 2010). While virtual violence may seem palatable to some, Morgan Luck (2009) seeks a moral theory that might be able to allow the acceptance of virtual murder but that will not extend to other immoral acts such as pedophilia. Christopher Bartel (2011) is less worried about the distinction Luck attempts to draw; Bartel argues that virtual pedophilia is real child pornography, which is already morally reprehensible and illegal across the globe.

While violence is easy to see in online games, there is a much more substantial moral value at play and that is the politics of virtual worlds. Peter Ludlow and Mark Wallace describe the initial moves to online political culture in their book, *The Second Life Herald: The Virtual Tabloid that Witnessed the Dawn of the Metaverse* (2007). Ludlow and Wallace chronicle how the players in massive online worlds have begun to form groups and guilds that often confound the designers of the game and are at times in conflict with those that make the game. Their contention is that designers rarely realize that they are creating a space where people intended to live large portions of their lives and engage in real economic and social activity and thus the designers have the moral duties somewhat equivalent to those who may write a political constitution (Ludlow and Wallace 2007). According to Purcell (2008), there is little commitment to democracy or egalitarianism by those who create and own online games and this needs to be discussed, if more and more of us are going to spend time living in these virtual societies.

### 3.1.2 The Lure of the Virtual in Game Worlds

A persistent concern about the use of computers and especially computer games is that this could result in anti-social behavior and isolation. Yet

studies might not support these hypotheses (Gibba, et al. 1983). With the advent of massively multiplayer games as well as video games designed for families the social isolation hypothesis is even harder to believe. These games do, however, raise gender equality issues. James Ivory used online reviews of games to complete a study that shows that male characters outnumber female characters in games and those female images that are in games tend to be overly sexualized (Ivory 2006). Soukup (2007) suggests that gameplay in these virtual worlds is most often based on gameplay that is oriented to masculine styles of play thus potentially alienating women players. And those women that do participate in game play at the highest level play roles in gaming culture that are very different from those the largely heterosexual white male gamers, often leveraging their sexuality to gain acceptance (Taylor et al. 2009). Additionally, Joan M. McMahon and Ronnie Cohen have studied how gender plays a role in the making of ethical decisions in the virtual online world, with women more likely to judge a questionable act as unethical than men (2009). Marcus Johansson suggests that we may be able to mitigate virtual immorality by punishing virtual crimes with virtual penalties in order to foster more ethical virtual communities (Johansson 2009).

The media has raised moral concerns about the way that childhood has been altered by the use of information technology (see for example Jones 2011). Many applications are now designed specifically for babies and toddlers with educational applications or just entertainment to help keep the children occupied while their parents are busy. This encourages children to interact with computers from as early an age as possible. Since children may be susceptible to media manipulation such as advertising we have to ask if this practice is morally acceptable or not. Depending on the particular application being used, it may encourage solitary play that may lead to isolation but others are more engaging with both the parents and the children playing (Siraj-Blatchford 2010). It should also be noted that pediatricians have advised that there are no known benefits to early media

use amongst young children but there potential risks (Christakis 2009). Studies have shown that from 1998 to 2008, sedentary lifestyles amongst children in England have resulted in the first measured decline in strength since World War Two (Cohen et al. 2011). It is not clear if this decline is directly attributable to information technology use but it may be a contributing factor. In 2018 the American Academy of Pediatrics released some simple guidelines for parents who may be trying to set realistic limits on this activity (Tips from the American Academy of Pediatrics).

### 3.1.3 The Technological Transparency Paradox

One may wonder why social media services tend to be free to use, but none the less, often make fabulous profits for the private companies that offer these services. It is no deep secret that the way these companies make profit is through the selling of information that the users are uploading to the system as they interact with it. The more users, and the more information that they provide, the greater the value that aggregating that information becomes. Mark Zuckerberg stated his philosophical commitment to the social value of this in his letter to shareholders from February 1, 2012:

At Facebook, we build tools to help people connect with the people they want and share what they want, and by doing this we are extending people's capacity to build and maintain relationships. People sharing more – even if just with their close friends or families – creates a more open culture and leads to a better understanding of the lives and perspectives of others. We believe that this creates a greater number of stronger relationships between people, and that it helps people get exposed to a greater number of diverse perspectives. By helping people form these connections, we hope to rewire the way people spread and consume

information. We think the world's information infrastructure should resemble the social graph "a network built from the bottom up or peer-to-peer, rather than the monolithic, top-down structure that has existed to date. We also believe that giving people control over what they share is a fundamental principle of this rewiring" (Facebook, Inc., 2012).

The social value of perusing this is debatable, but the economic value has been undeniable. At the time this was written, Mark Zuckerberg has been constantly listed in the top ten richest billionaires by Forbes Magazine where he is typically in the top five of that rarefied group. An achievement built on providing a free service to the world. What companies like Facebook do charge for are services, such as directed advertising, which allow third party companies to access information that users have provided to the social media applications. The result is that ads bought on an application such as Facebook are more likely to be seen as useful to viewers who are much more likely to click on these ads and buy the advertised products. The more detailed and personal the information shared, the more valuable it will be to the companies that it is shared with. This radical transparency of sharing deeply personal information with companies like Facebook is encouraged. Those who do use social networking technologies do receive value as evidenced by the rapid growth of this technology. Statista reports that in 2019 there will be 2.77 billion users of social media worldwide and it will grow to 3.02 by 2021 (Statista, 2018). The question here is, what do we give up in order to receive this "free" service? In 2011, back when there were less than a billion social media users the technology critic Andrew Keen warned that, "sharing is a trap," and that there was a kind of cult of radical transparency developing that clouded our ability to think critically about the kind of power we were giving these companies (Keen, 2011). Even before companies like Facebook were making huge profits, there were those warning of the dangers of the cult of transparency with warning such as:

...it is not surprising that public distrust has grown in the very years in which openness and transparency have been so avidly pursued. Transparency destroys secrecy: but it may not limit the deception and deliberate misinformation that undermine relations of trust. If we want to restore trust we need to reduce deception and lies, rather than secrecy. (O'Neill, 2002)

In the case of Facebook we can see that some of the warnings of the critics were prescient. In April of 2018, Mark Zuckerberg was called before congress where he apologized for the actions of his corporation in a scandal that involved divulging a treasure trove of information about his users to an independent researcher, who then sold it to Cambridge Analytica, which was a company involved in political data analysis. This data was then used to target political ads to the users of Facebook. Many of which were fake ads created by Russian intelligence to disrupt the US election in 2016 (Au-Yeung, 2018).

The philosopher Shannon Vallor critiques the cult of transparency as a version of what she calls the "Technological Transparency Paradox" (Vallor, 2016). She notes that those in favor of developing technologies to promote radically transparent societies, do so under the premise that this openness will increase accountability and democratic ideals. But the paradox is that this cult of transparency often achieves just the opposite with large unaccountable organizations that are not democratically chosen holding information that can be used to weaken democratic societies. This is due to the asymmetrical relationship between the user and the companies with whom she shares all the data of her life. The user is, indeed radically open and transparent to the company, but the algorithms used to mine the data and the 3rd parties that this data is shared with is opaque and not subject to accountability. We, the users of these technologies, are forced to be transparent but the companies profiting off our information are not required to be equally transparent.

### 3.3 Malware, Spyware and Informational Warfare

Malware and computer virus threats continue to grow at an astonishing rate. Security industry professionals report that while certain types of malware attacks such as spam are falling out of fashion, newer types of attacks such as Ransomware and other methods focused on mobile computing devices, cryptocurrency, and the hacking of cloud computing infrastructure are on the rise outstripping any small relief seen in the slowing down of older forms of attack (Cisco Systems 2018; Kaspersky Lab 2017, McAfee 2018, Symantec 2018). What is clear is that this type of activity will be with us for the foreseeable future. In addition to the largely criminal activity of malware production, we must also consider the related but more morally ambiguous activities of hacking, hacktivism, commercial spyware, and informational warfare. Each of these topics has its own suite of subtle moral ambiguities. We will now explore some of them here.

While there may be wide agreement that the conscious spreading of malware is of questionable morality there is an interesting question as to the morality of malware protection and anti-virus software. With the rise in malicious software there has been a corresponding growth in the security industry which is now a multibillion dollar market. Even with all the money spent on security software there seems to be no slowdown in virus production, in fact quite the opposite has occurred. This raises an interesting business ethics concern; what value are customers receiving for their money from the security industry? The massive proliferation of malware has been shown to be largely beyond the ability of anti-virus software to completely mitigate. There is an important lag in the time between when a new piece of malware is detected by the security community and the eventual release of the security patch and malware removal tools.

The anti-virus *modus operandi* of receiving a sample, analyzing the sample, adding detection for the sample, performing quality assurance, creating an update, and finally sending the update to their users leaves a huge window of opportunity for the adversary ... even assuming that anti-virus users update regularly. (Aycock and Sullins 2010)

This lag is constantly exploited by malware producers and in this model there is an ever-present security hole that is impossible to fill. Thus it is important that security professionals do not overstate their ability to protect systems, by the time a new malicious program is discovered and patched, it has already done significant damage and there is currently no way to stop this (Aycock and Sullins 2010).

In the past most malware creation was motivated by hobbyists and amateurs, but this has changed and now much of this activity is criminal in nature (Cisco Systems 2018; Kaspersky Lab 2017, McAfee 2018, Symantec 2018). Aycock and Sullins (2010) argue that relying on a strong defense is not enough and the situation requires a counteroffensive reply as well and they propose an ethically motivated malware research and creation program. This is not an entirely new idea and it was originally suggested by the Computer Scientist George Ledin in his editorial for the *Communications of the ACM*, “Not Teaching Viruses and Worms is Harmful” (2005). This idea does run counter to the majority opinion regarding the ethics of learning and deploying malware. Many computer scientists and researchers in information ethics agree that all malware is unethical (Edgar 2003; Himma 2007a; Neumann 2004; Spafford 1992; Spinello 2001). According to Aycock and Sullins, these worries can be mitigated by open research into understanding how malware is created in order to better fight this threat (2010).



When malware and spyware is created by state actors, we enter the world of informational warfare and a new set of moral concerns. Every developed country in the world experiences daily cyber-attacks, with the major target being the United States that experiences a purported 1.8 billion attacks a month in 2010 (Lovely 2010) and 80 billion malicious scans world wide in 2017 (McAfee 2018). The majority of these attacks seem to be just probing for weaknesses but they can devastate a countries internet such as the cyber-attacks on Estonia in 2007 and those in Georgia which occurred in 2008. While the Estonian and Georgian attacks were largely designed to obfuscate communication within the target countries more recently informational warfare has been used to facilitate remote sabotage. The famous Stuxnet virus used to attack Iranian nuclear centrifuges is perhaps the first example of weaponized software capable of creating remotely damaging physical facilities (Cisco Systems 2018). The coming decades will likely see many more cyber weapons deployed by state actors along well-known political fault lines such as those between Israel-America-western Europe vs Iran, and America-Western Europe vs China (Kaspersky Lab 2018). The moral challenge here is to determine when these attacks are considered a severe enough challenge to the sovereignty of a nation to justify military reactions and to react in a justified and ethical manner to them (Arquilla 2010; Denning 2008, Kaspersky Lab 2018).

The primary moral challenge of informational warfare is determining how to use weaponized information technologies in a way that honors our commitments to just and legal warfare. Since warfare is already a morally questionable endeavor it would be preferable if information technologies could be leveraged to lessen violent combat. For instance, one might argue that the Stuxnet virus used undetected from 2005 to 2010 did damage to Iranian nuclear weapons programs that in generations before might have only been accomplished by an air raid or other kinetic military action that would have incurred significant civilian casualties—and that so far there

have been no reported human casualties resulting from Stuxnet. Thus malware might lessen the amount of civilian casualties in conflict. The malware known as “Flame” is an interesting case of malware that evidence suggests was designed to aid in espionage. One might argue that more accurate information given to decision makers during wartime should help them make better decisions on the battlefield. On the other hand, these new informational warfare capabilities might allow states to engage in continual low level conflict eschewing efforts for peacemaking which might require political compromise.

### 3.4 Future Concerns

As was mentioned in the introduction above, information technologies are in a constant state of change and innovation. The internet technologies that have brought about so much social change were scarcely imaginable just decades before they appeared. Even though we may not be able to foresee all possible future information technologies, it is important to try to imagine the changes we are likely to see in emerging technologies. James Moor argues that moral philosophers need to pay particular attention to emerging technologies and help influence the design of these technologies early on to encourage beneficial moral outcomes (Moor 2005). The following sections contain some potential technological concerns.

#### 3.4.1 Acceleration of Change

An information technology has an interesting growth pattern that has been observed since the founding of the industry. Intel engineer Gordon E. Moore noticed that the number of components that could be installed on an integrated circuit doubled every year for a minimal economic cost and he thought it might continue that way for another decade or so from the time he noticed it in 1965 (Moore 1965). History has shown his

predictions were rather conservative. This doubling of speed and capabilities along with a halving of costs to produce it has roughly continued every eighteen months since 1965 and is likely to continue. This phenomenon is not limited to computer chips and can also be found in many different forms of information technologies. The potential power of this accelerating change has captured the imagination of the noted inventor and futurist Ray Kurzweil. He has famously predicted that if this doubling of capabilities continues and more and more technologies become information technologies, then there will come a point in time where the change from one generation of information technology to the next will become so massive that it will change everything about what it means to be human. Kurzweil has named this potential event “the Singularity” at which time he predicts that our technology will allow us to become a new post human species (2006). If this is correct, there could be no more profound change to our moral values. There has been some support for this thesis from the technology community with institutes such as the Acceleration Studies Foundation, Future of Humanity Institute, and H+. [2] Reaction to this hypothesis from philosophers has been mixed but largely critical. For example Mary Midgley (1992) argues that the belief that science and technology will bring us immortality and bodily transcendence is based on pseudoscientific beliefs and a deep fear of death. In a similar vein Sullins (2000) argues that there is often a quasi-religious aspect to the acceptance of transhumanism that is committed to certain outcomes such as uploading of human consciousness into computers as a way to achieve immortality, and that the acceptance of the transhumanist hypothesis influences the values embedded in computer technologies, which can be dismissive or hostile to the human body.

There are other cogent critiques of this argument but none as simple as the realization that:

...there is, after all, a limit to how small things can get before they simply melt. Moore’s Law no longer holds. Just because something grows exponentially for some time, does not mean that it will continue to do so forever... (Floridi, 2016).

While many ethical systems place a primary moral value on preserving and protecting nature and the natural given world, transhumanists do not see any intrinsic value in defining what is natural and what is not and consider arguments to preserve some perceived natural state of the human body as an unjustifiable obstacle to progress. Not all philosophers are critical of transhumanism, as an example Nick Bostrom (2008) of the Future of Humanity Institute at Oxford University argues that putting aside the feasibility argument, we must conclude that there are forms of posthumanism that would lead to long and worthwhile lives and that it would be overall a very good thing for humans to become posthuman if it is at all possible (Bostrom, 2008).

### 3.4.2 Artificial Intelligence and Artificial Life

Artificial Intelligence (AI) refers to the many longstanding research projects directed at building information technologies that exhibit some or all aspects of human level intelligence and problem solving. Artificial Life (ALife) is a project that is not as old as AI and is focused on developing information technologies and or synthetic biological technologies that exhibit life functions typically found only in biological entities. A more complete description of logic and AI can be found in the entry on logic and artificial intelligence. ALife essentially sees biology as a kind of naturally occurring information technology that may be reverse engineered and synthesized in other kinds of technologies. Both AI and ALife are vast research projects that defy simple explanation. Instead the focus here is on

the moral values that these technologies impact and the way some of these technologies are programmed to affect emotion and moral concern.

#### 3.4.2.1 Artificial Intelligence

Alan Turing is credited with defining the research project that would come to be known as Artificial Intelligence in his seminal 1950 paper “Computing Machinery and Intelligence.” He described the “imitation game,” where a computer attempts to fool a human interlocutor that it is not a computer but another human (Turing 1948, 1950). In 1950, he made the now famous claim that

I believe that in about fifty years’ time.... one will be able to speak of machines thinking without expecting to be contradicted.

A description of the test and its implications to philosophy outside of moral values can be found here (see entry on the Turing test). Turing’s prediction may have been overly ambitious and in fact some have argued that we are nowhere near the completion of Turing’s dream. For example, Luciano Floridi (2011a) argues that while AI has been very successful as a means of augmenting our own intelligence, but as a branch of cognitive science interested in intelligence production, AI has been a dismal disappointment. The opposite opinion has also been argued and some claim that the Turing Test has already been passed or at least that programmers are on the verge of doing so. For instance it was reported by the BBC in 2014 that the Turing Test had been passed by a program that could convince the judges that it was a 13 year old Ukrainian boy, but even so, many experts remain skeptical (BBC 2014).

For argument’s sake, assume Turing is correct even if he is off in his estimation of when AI will succeed in creating a machine that can converse with you. Yale professor David Gelernter worries that that there would be certain uncomfortable moral issues raised. “You would have no

grounds for treating it as a being toward which you have moral duties rather than as a tool to be used as you like” (Gelernter 2007). Gelernter suggests that consciousness is a requirement for moral agency and that we may treat anything without it in any way that we want without moral regard. Sullins (2006) counters this argument by noting that consciousness is not required for moral agency. For instance, nonhuman animals and the other living and nonliving things in our environment must be accorded certain moral rights, and indeed, any Turing capable AI would also have moral duties as well as rights, regardless of its status as a conscious being (Sullins 2006).

AI is certainly capable of creating machines that can converse effectively in simple ways with human beings as evidenced by Apple Siri, Amazon Alexa, OK Google, etc. along with the many systems that businesses use to automate customer service, but these are still a ways away from having the natural kinds of unscripted conversations humans have with one another. But that may not matter when it comes to assessing the moral impact of these technologies. In addition, there are still many other applications that use AI technology. Nearly all of the information technologies we discussed above such as, search, computer games, data mining, malware filtering, robotics, etc., all utilize AI programming techniques. Thus AI will grow to be a primary location for the moral impacts of information technologies. Many governments and professional associations are now developing ethical guidelines and standards to help shape this important technology, on a good example is the Global Initiative on the Ethics of Intelligent and Autonomous Systems (IEEE 2018).

### 3.4.2.2 Artificial Life

Artificial Life (ALife) is an outgrowth of AI and refers to the use of information technology to simulate or synthesize life functions. The problem of defining life has been an interest in philosophy since its founding. See the entry on life for a look at the concept of life and its philosophical ramifications. If scientists and technologists were to succeed in discovering the necessary and sufficient conditions for life and then successfully synthesize it in a machine or through synthetic biology, then we would be treading on territory that has significant moral impact. Mark Bedau has been tracing the philosophical implications of ALife for some time now and argues that there are two distinct forms of ALife and each would thus have different moral effects if and when we succeed in realizing these separate research agendas (Bedau 2004; Bedau and Parke 2009). One form of ALife is completely computational and is in fact the earliest form of ALife studied. ALife is inspired by the work of the mathematician John von Neumann on self-replicating cellular automata, which von Neumann believed would lead to a computational understanding of biology and the life sciences (1966). The computer scientist Christopher Langton simplified von Neumann's model greatly and produced a simple cellular automata called "Loops" in the early eighties and helped get the field off the ground by organizing the first few conferences on Artificial Life (1989). Artificial Life programs are quite different from AI programs. Where AI is intent on creating or enhancing intelligence, ALife is content with very simple minded programs that display life functions rather than intelligence. The primary moral concern here is that these programs are designed to self-reproduce and in that way resemble computer viruses and indeed successful ALife programs could become as malware vectors. The second form of ALife is much more morally charged. This form of ALife is based on manipulating actual biological and biochemical processes in such a way as to produce novel life forms not seen in nature.

Scientists at the J. Craig Venter institute were able to synthesize an artificial bacterium called JCVI-syn1.0 in May of 2010. While media paid attention to this breakthrough, they tended to focus on the potential ethical and social impacts of the creation of artificial bacteria. Craig Venter himself launched a public relations campaign trying to steer the conversation about issues relating to creating life. This first episode in the synthesis of life gives us a taste of the excitement and controversy that will be generated when more viable and robust artificial protocells are synthesized. The ethical concerns raised by Wet ALife, as this kind of research is called, are more properly the jurisdiction of bioethics (see entry on theory and bioethics). But it does have some concern for us here in that Wet ALife is part of the process of turning theories from the life sciences into information technologies. This will tend to blur the boundaries between bioethics and information ethics. Just as software ALife might lead to dangerous malware, so too might Wet ALife lead to dangerous bacteria or other disease agents. Critics suggest that there are strong moral arguments against pursuing this technology and that we should apply the precautionary principle here which states that if there is any chance at a technology causing catastrophic harm, and there is no scientific consensus suggesting that the harm will not occur, then those who wish to develop that technology or pursue that research must prove it to be harmless first (see Epstein 1980). Mark Bedau and Mark Taint argue against a too strong adherence to the precautionary principle by suggesting that instead we should opt for moral courage in pursuing such an important step in human understanding of life (2009). They appeal to the Aristotelian notion of courage, not a headlong and foolhardy rush into the unknown, but a resolute and careful step forward into the possibilities offered by this research.

### 3.4.3 Robotics and Moral Values

Information technologies have not been content to remain confined to virtual worlds and software implementations. These technologies are also interacting directly with us through robotics applications. Robotics is an emerging technology but it has already produced a number of applications that have important moral implications. Technologies such as military robotics, medical robotics, personal robotics and the world of sex robots are just some of the already existent uses of robotics that impact on and express our moral commitments (see, Anderson and Anderson 2011; Capurro and Nagenborg 2009; Lin et al. 2012, 2017).

There have already been a number of valuable contributions to the growing fields of machine morality and robot ethics (roboethics). For example, in Wallach and Allen's book *Moral Machines: Teaching Robots Right from Wrong* (2010), the authors present ideas for the design and programming of machines that can functionally reason on moral questions as well as examples from the field of robotics where engineers are trying to create machines that can behave in a morally defensible way. The introduction of semi and fully autonomous machines, (meaning machines that make decisions with little or no human intervention), into public life will not be simple. Towards this end, Wallach (2011) has also contributed to the discussion on the role of philosophy in helping to design public policy on the use and regulation of robotics.

Military robotics has proven to be one of the most ethically charged robotics applications (Lin et al. 2008, 2013, Lin 2010; Strawser, 2013). Today these machines are largely remotely operated (telerobots) or semi-autonomous, but over time these machines are likely to become more and more autonomous due to the necessities of modern warfare (Singer 2009). In the first decades of war in the 21<sup>st</sup> century robotic weaponry has been involved in numerous killings of both soldiers and noncombatants (Plaw

2013), and this fact alone is of deep moral concern. Gerhard Dabringer has conducted numerous interviews with ethicists and technologists regarding the implications of automated warfare (Dabringer 2010). Many ethicists are cautious in their acceptance of automated warfare with the provision that the technology is used to enhance ethical conduct in war, for instance by reducing civilian and military casualties or helping warfighters follow International Humanitarian Law and other legal and ethical codes of conduct in war (see Lin et al. 2008, 2013; Sullins 2009b), but others have been highly skeptical of the prospects of an ethical autonomous war due to issues like the risk to civilians and the ease in which wars might be declared given that robots will be taking most of the risk (Asaro 2008; Sharkey 2011).

## 4. Information Technologies of Morality

A key development in the realm of information technologies is that they are not only the object of moral deliberations but they are also beginning to be used as a tool in moral deliberation itself. Since artificial intelligence technologies and applications are a kind of automated problem solvers, and moral deliberations are a kind of problem, it was only a matter of time before automated moral reasoning technologies would emerge. This is still only an emerging technology but it has a number of very interesting moral implications which will be outlined below. The coming decades are likely to see a number of advances in this area and ethicists need to pay close attention to these developments as they happen. Susan and Michael Anderson have collected a number of articles regarding this topic in their book, *Machine Ethics* (2011), and Rocci Luppigini has a section of his anthology devoted to this topic in the *Handbook of Research on Technoethics* (2009).

#### 4.1 Information Technology as a Model for Moral Discovery

Patrick Grim has been a longtime proponent of the idea that philosophy should utilize information technologies to automate and illustrate philosophical thought experiments (Grim et al. 1998; Grim 2004). Peter Danielson (1998) has also written extensively on this subject beginning with his book *Modeling Rationality, Morality, and Evolution* with much of the early research in the computational theory of morality centered on using computer models to elucidate the emergence of cooperation between simple software AI or ALife agents (Sullins 2005).

Luciano Floridi and J. W. Sanders argue that information as it is used in the theory of computation can serve as a powerful idea that can help resolve some of the famous moral conundrums in philosophy such as the nature of evil (1999, 2001). They propose that along with moral evil and natural evil, both concepts familiar to philosophy (see entry on the problem of evil); we add a third concept they call artificial evil (2001). Floridi and Sanders contend that if we do this then we can see that the actions of artificial agents

...to be morally good or evil can be determined even in the absence of biologically sentient participants and thus allows artificial agents not only to perpetrate evil (and for that matter good) but conversely to 'receive' or 'suffer from' it. (Floridi and Sanders 2001)

Evil can then be equated with something like information dissolution, where the irretrievable loss of information is bad and the preservation of information is good (Floridi and Sanders 2001). This idea can move us closer to a way of measuring the moral impacts of any given action in an information environment.

#### 4.2 Information Technology as a Moral System

Early in the twentieth century the American philosopher John Dewey (see entry on John Dewey) proposed a theory of inquiry based on the instrumental uses of technology. Dewey had an expansive definition of technology which included not only common tools and machines but information systems such as logic, laws and even language as well (Hickman 1990). Dewey argued that we are in a 'transactional' relationship with all of these technologies within which we discover and construct our world (Hickman 1990). This is a helpful standpoint to take as it allows us to advance the idea that an information technology of morality and ethics is not impossible. As well as allowing us to take seriously the idea that the relations and transactions between human agents and those that exist between humans and their artifacts have important ontological similarities. While Dewey could only dimly perceive the coming revolutions in information technologies, his theory is useful to us still because he proposed that ethics was not only a theory but a practice and solving problems in ethics is like solving problems in algebra (Hickman 1990). If he is right, then an interesting possibility arises, namely the possibility that ethics and morality are computable problems and therefore it should be possible to create an information technology that can embody moral systems of thought.

In 1974 the philosopher Mario Bunge proposed that we take the notion of a 'technoethics' seriously arguing that moral philosophers should emulate the way engineers approach a problem. Engineers do not argue in terms of reasoning by categorical imperatives but instead they use:

... the forms If  $A$  produces  $B$ , and you value  $B$ , chose to do  $A$ , and If  $A$  produces  $B$  and  $C$  produces  $D$ , and you prefer  $B$  to  $D$ , choose  $A$  rather than  $C$ . In short, the rules he comes up with are based on fact and value, I submit that this is the way moral rules ought to be

fashioned, namely as rules of conduct deriving from scientific statements and value judgments. In short ethics could be conceived as a branch of technology. (Bunge 1977, 103)

Taking this view seriously implies that the very act of building information technologies is also the act of creating specific moral systems within which human and artificial agents will, at least occasionally, interact through moral transactions. Information technologists may therefore be in the business of creating moral systems whether they know it or not and whether or not they want that responsibility.

### 4.3 Informational Organisms as Moral Agents

The most comprehensive literature that argues in favor of the prospect of using information technology to create artificial moral agents is that of Luciano Floridi (1999, 2002, 2003, 2010b, 2011b), and Floridi with Jeff W. Sanders (1999, 2001, 2004). Floridi (1999) recognizes that issues raised by the ethical impacts of information technologies strain our traditional moral theories. To relieve this friction he argues that what is needed is a broader philosophy of information (2002). After making this move, Floridi (2003) claims that information is a legitimate environment of its own and that has its own intrinsic value that is in some ways similar to the natural environment and in other ways radically foreign but either way the result is that information is on its own a thing that is worthy of ethical concern. Floridi (2003) uses these ideas to create a theoretical model of moral action using the logic of object oriented programming.

His model has seven components; 1) the moral agent *a*, 2) the moral patient *p* (or more appropriately, reagent), 3) the interactions of these agents, 4) the agent's frame of information, 5) the factual information available to the agent concerning the situation that agent is attempting to navigate, 6) the environment the interaction is occurring in, and 7) the

situation in which the interaction occurs (Floridi 2003, 3). Note that there is no assumption of the ontology of the agents concerned in the moral relationship modeled and these agents can be any mixture or artificial or natural in origin (Sullins 2009a).

There is additional literature which critiques arguments such as Floridi's with the hope of expanding the idea of automated moral reasoning so that one can speak of many different types of automated moral technologies from simple applications all the way to full moral agents with rights and responsibilities similar to humans (Adam 2008; Anderson and Anderson 2011; Johnson and Powers 2008; Schmidt 2007; Wallach and Allen 2010).

While scholars recognize that we are still some time from creating information technology that would be unequivocally recognized as an artificial moral agent, there are strong theoretical arguments in suggesting that automated moral reasoning is an eventual possibility and therefore it is an appropriate area of study for those interested in the moral impacts of information technologies.

## Bibliography

- Adam, A., 2002, "Cyberstalking and Internet pornography: Gender and the gaze," *Ethics and Information Technology*, 4(2): 133–142.
- , 2008, "Ethics for things," *Ethics and Information technology*, 10(2–3): 149–154.
- American Academy of Pediatrics, 2018, "Tips from the American Academy of Pediatrics to Help Families Manage the Ever Changing Digital Landscape," May 1, available online.
- Anderson, M. and S. L. Anderson (eds.), 2011, *Machine Ethics*, Cambridge: Cambridge University Press.
- Arkin, R., 2009, *Governing Lethal Behavior in Autonomous Robots*, New York: Chapman and Hall/CRC.

- Arquilla, J., 2010, "Conflict, Security and Computer Ethics," in Floridi 2010a.
- Asaro, P., 2008. "How Just Could a Robot War Be?" in Philip Brey, Adam Briggie and Katinka Waelbers (eds.), *Current Issues in Computing And Philosophy*, Amsterdam, The Netherlands: IOS Press, pp. 50–64.
- , 2009. "Modeling the Moral User: Designing Ethical Interfaces for Tele-Operation," *IEEE Technology & Society*, 28(1): 20–24.
- Au-Yeung A., 2018. "Why Investors Remain Bullish On Facebook in Day Two Of Zuckerberg's Congressional Hearnings," *Forbes*, April 11, available online.
- Aycock, J. and J. Sullins, 2010, "Ethical Proactive Threat Research," *Workshop on Ethics in Computer Security Research (LNCS 6054)*, New York: Springer, pp. 231–239.
- Bartell, C., 2011, "Resolving the gamer's dilemma," *Ethics and Information Technology*, 14(1):11–16.
- Baase, S., 2008, *A Gift of Fire: Social, Legal, and Ethical Issues for Computing and the Internet*, Englewood Cliffs, NJ: Prentice Hall.
- BBC, 2014, "Computer AI passes Turing test in 'world first'," *BBC Technology* [available online]
- Bedau, M., 2004, "Artificial Life," in Floridi 2004.
- Bedau, M. and E. Parke (eds.), 2009, *The Ethics of Protocells: Moral and Social Implications of Creating Life in the Laboratory*, Cambridge: MIT Press.
- Bedau, M. and M. Taint, 2009, "Social and Ethical Implications of Creating Artificial Cells," in Bedau and Parke 2009.
- Bostrom, N., 2008, "Why I Want to be a Posthuman When I Grow Up," in *Medical Enhancement and Posthumanity*, G. Gordijn and R. Chadwick (eds), Berlin: Springer, pp. 107–137.
- Brey, P., 2008, "Virtual Reality and Computer Simulation," in Himma and Tavanni 2008
- , 2010, "Values in Technology and Disclosive Computer Ethics," in Floridi 2010a.
- Bunge, M. 1977, "Towards a Technoethics," *The Monist*, 60(1): 96–107.
- Bynum, T., 2000, "Ethics and the Information Revolution," *Ethics in the Age of Information Technology*, pp. 32–55, Linköping, Sweden: Center for Applied Ethics at Linköping University.
- , 2008, "Norbert Wiener and the Rise of Information Ethics," in van den Hoven and Weckert 2008.
- Capurro, R., Nagenborg, M., 2009, *Ethics and Robotics*, [CITY]: IOS Press
- Christakis, D. A., 2009, "The effects of infant media usage: what do we know and what should we learn?" *Acta Paediatrica*, 98 (1): 8–16.
- Cisco Systems, Inc., 2018, *Cisco 2018 Annual Security Report: Small and Mighty: How Small and Midmarket Businesses Can Fortify Their Defenses Against Today's Threats*, San Jose, CA: Cisco Systems Inc. [available online]
- Coeckelbergh, M., 2007, "Violent Computer Games, Empathy, and Cosmopolitanism," *Ethics and Information Technology*, 9(3): 219–231
- Cohen, D. D., C. Voss, M. J. D. Taylor, A. Delextrat, A. A. Ogunleye, and G. R. H. Sandercock, 2011, "Ten-year secular changes in muscular fitness in English children," *Acta Paediatrica*, 100(10): e175–e177.
- Danielson, P., 1998, *Modeling Rationality, Morality, and Evolution*, Oxford: Oxford University Press.
- Dabringer, G., (ed.) 2010, *Ethica Themen: Ethical and Legal Aspects of Unmanned Systems, Interviews*, Vienna, Austria: Austrian Ministry of Defence and Sports. [available online]
- Denning, D., 2008, "The Ethics of Cyber Conflict," In Himma and Tavanni 2008.
- Dodig-Crnkovic, G., Hofkirchner, W., 2011, "Floridi's 'Open Problems in Philosophy of Information', Ten Years Later," *Information*, (2): 327–359. [available online]



- Edgar, S.L., 2003, *Morality and Machines*, Sudbury Massachusetts: Jones and Bartlett.
- Epstein, R., 2007, "The Impact of Computer Security Concerns on Software Development," in Himma 2007a, pp. 171–202.
- Epstein, L.S. 1980. "Decision-making and the temporal resolution of uncertainty". *International Economic Review* 21 (2): 269–283.
- Ess, C., 2009, *Digital Media Ethics*, Massachusetts: Polity Press.
- Facebook, Inc., 2012, *Form S-1: Registration Statement*, filed with the United States Securities and Exchange Commission, Washington, DC, available online.
- Floridi, L., 1999, "Information Ethics: On the Theoretical Foundations of Computer Ethics", *Ethics and Information Technology*, 1(1): 37–56.
- , 2002, "What is the Philosophy of Information?" in *Metaphilosophy*, 33(1/2): 123–145.
- , 2003, "On the Intrinsic Value of Information Objects and the Infosphere," *Ethics and Information Technology*, 4(4): 287–304.
- , 2004, *The Blackwell Guide to the Philosophy of Computing and Information*, Blackwell Publishing.
- (ed.), 2010a, *The Cambridge Handbook of Information and Computer Ethics*, Cambridge: Cambridge University Press.
- , 2010b, *Information: A Very Short Introduction*, Oxford: Oxford University Press.
- , 2011a, "Enveloping the World for AI," *The Philosopher's Magazine*, 54: 20–21
- , 2011b, *The Philosophy of Information*, Oxford: Oxford University Press.
- , 2016, "Should We be Afraid of AI?", Neigel Warburton (ed.), *Aeon*, 09 May 2016, available online.
- Floridi, L. and J. W. Sanders, 1999, "Entropy as Evil in Information Ethics," *Etica & Politica*, special issue on Computer Ethics, I(2). [available online]
- , 2001, "Artificial evil and the foundation of computer ethics," in *Ethics and Information Technology*, 3(1): 55–66. [available online]
- , 2004, "On the Morality of Artificial Agents," in *Minds and Machines*, 14(3): 349–379 [available online]
- Ferguson, C. J., 2007, "The Good The Bad and the Ugly: A Meta-analytic Review of Positive and Negative Effects of Violent Video Games," *Psychiatric Quarterly*, 78(4): 309–316.
- Gelernter, D., 2007, "Artificial Intelligence Is Lost in the Woods," *Technology Review*, July/August, pp. 62–70. [available online]
- Gibba, G. D., J. R. Bailey, T. T. Lambirth, and W. Wilson, 1983, "Personality Differences Between High and Low Electronic Video Game Users," *The Journal of Psychology*, 114(2): 159–165.
- Grim, P., 2004, "Computational Modeling as a Philosophical Methodology," In Floridi 2004.
- Grim, P., G. Mar, and P. St. Denis, 1998, *The Philosophical Computer: Exploratory Essays in Philosophical Computer Modeling*, MIT Press.
- Grodzinsky, F. S. and H. T. Tavani, 2002, "Ethical Reflections on Cyberstalking," *Computers and Society*, 32(1): 22–32.
- Hansen, R. and J. Grossman, 2008, "Clickjacking," *SecTheory: Internet Security*. [available online]
- Hickman, L. A. 1990, *John Dewey's Pragmatic Technology*, Bloomington, Indiana: Indiana University Press.
- Himma, K. E. (ed.), 2007a, *Internet Security, Hacking, Counterhacking, and Society*, Sudbury Massachusetts: Jones and Bartlett Publishers.
- Himma, K. E., 2007b, "Hacking as Politically Motivated Digital Civil Disobedience: Is Hacktivism Morally Justified?" In Himma 2007a, pp. 73–98.
- Himma, K. E., and H. T. Tavanni (eds.), 2008, *The Handbook of Information and Computer Ethics*, Wiley-Interscience; 1<sup>st</sup> edition
- Hongladarom, S., 2008, "Privacy, Contingency, Identity and the Group," *Handbook of Research on Technoethics. Vol. II*, R. Luppici

- and Rebecca Adell Eds. Hershey, PA: IGI Global, pp. 496–511.
- IEEE 2018, “Ethically Aligned Design: The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems”, *IEEE* [available online ]
- Ivory, J. D., 2006, “Still a Man’s Game: Gender Representation in Online Reviews of Video Games,” *Mass Communication and Society*, 9(1): 103–114.
- Johansson, M., 2009, “Why unreal punishments in response to unreal crimes might actually be a really good thing,” *Ethics and Information Technology*, 11(1): 71–79
- Johnson, D.G., 1985, *Computer Ethics*, Englewood Cliffs, New Jersey: Prentice Hall. (2<sup>nd</sup> ed., 1994; 3<sup>rd</sup> ed., 2001; 4<sup>th</sup> ed., 2009).
- Johnson D. G., and T. Powers, 2008, “Computers and Surrogate Agents,” In van den Hoven and Weckert 2008.
- Jones, T., 2011, “Techno-toddlers: A is for Apple,” *The Guardian*, Friday November 18. [available online ]
- Kaspersky Lab, 2017, *Kaspersky Security Bulletin: KASPERSKY LAB THREAT PREDICTIONS FOR 2018*, Moscow, Russia: Kaspersky Lab ZAO. [available online]
- Keen, A., 2011, “Your Life Torn Open, Essay 1: Sharing is a trap,” *Wired*, 03 Feb 2011, available online.
- Kurzweil, R., 2006, *The Singularity is Near*, New York: Penguin Press.
- Langton, C. G., (ed.), 1989, *Artificial Life: the Proceedings of an Interdisciplinary Workshop on the Synthesis and Simulation of Living Systems*, Redwood City: Addison-Wesley.
- Ledin G., 2005, “Not Teaching Viruses and Worms is Harmful” *Communications of the ACM* , 48(1): 144.
- Lessig, L., 1999, *Code and Other Values of Cyberspace*, New York: Basic Books.
- Levy, S., 1984, *Hackers: Heroes of the Computer Revolution*, New York: Anchor Press.
- Lin P., 2010, “Ethical Blowback from Emerging Technologies”, *Journal of Military Ethics*, 9(4): 313–331.
- Lin, P., K. Abney, and R. Jenkins, 2017, *Robot Ethics 2.0: From Autonomous Cars to Artificial Intelligence*, Oxford: Oxford University Press.
- Lin, P., K. Abney, and G. Bekey, 2012, *Robot Ethics: The Ethical and Social Implications of Robotics*, Cambridge, MA: MIT Press.
- 2013, “Ethics, War, and Robots”, *Ethics and Emerging Technologies*, London: Palgrave–Macmillan.
- Lin, P., G. Bekey, and K. Abney, 2008, *Autonomous Military Robotics: Risk, Ethics, and Design*, Washington, DC: U.S. Department of the Navy, Office of Naval Research. [available online]
- Lovely, E., 2010, “Cyberattacks explode in Congress,” *Politico*, March 5, 2010. [available online]
- Lü, Yao-Hui, 2005, “Privacy and Data Privacy Issues in Contemporary China,” *Ethics and Information Technology*, 7(1): 7–15
- Ludlow, P. and M. Wallace, 2007, *The Second Life Herald: The Virtual Tabloid that Witnessed the Dawn of the Metaverse*, Cambridge, MA: MIT Press.
- Luck, M., 2009, “The gamer’s dilemma: An analysis of the arguments for the moral distinction between virtual murder and virtual paedophilia,” *Ethics and Information Technology*, 11(1): 31–36.
- Luppigini, R. and R. Adell (eds.), 2009, *Handbook of Research on Technoethics*, Idea Group Inc. (IGI).
- Magnani, L., 2007, *Morality in a Technological World: Knowledge as Duty*, Cambridge, Cambridge University Press.
- Mason, R. O., 1986, Four ethical issues of the information age. *MIS Quarterly*, 10(1): 5–12.
- Markoff, J., 2005, *What the Dormouse Said: How the 60s Counterculture Shaped the Personal Computer Industry*, New York: Penguin.
- Manion, M. and A. Goodrum, 2007, “Terrorism or Civil Disobedience:





- Toward a Hacktivist Ethic,” in Himma 2007a, pp. 49–59.
- McAfee, 2018, *Economic Impact of Cybercrime: No Slowing Down, Report* [available online]
- McMahon, J. M. and R. Cohen, 2009, “Lost in cyberspace: ethical decision making in the online environment,” *Ethics and Information Technology*, 11(1): 1–17.
- Midgley, M., 1992, *Science as Salvation: a modern myth and its meaning*, London: Routledge.
- Moor, J. H., 1985, “What is Computer Ethics?” *Metaphilosophy*, 16(4): 266–275.
- , 2005, “Why We Need Better Ethics for Emerging Technologies,” *Ethics and Information Technology*, 7(3): 111–119. Reprinted in van den Hoven and Weckert 2008, pp. 26–39.
- Moore, Gordon E. 1965. “Cramming more components onto integrated circuits”. *Electronics*, 38(8): 114–117. [available online]
- Neumann, P. G., 2004, “Computer security and human values,” *Computer Ethics and Professional Responsibility*, Malden, MA: Blackwell
- Nissenbaum, H., 1997. “Toward an Approach to Privacy in Public: Challenges of Information Technology,” *Ethics and Behavior*, 7(3): 207–219. [available online]
- , 1998. “Values in the Design of Computer Systems,” *Computers and Society*, March: pp. 38–39. [available online]
- , 1999, “The Meaning of Anonymity in an Information Age,” *The Information Society*, 15: 141–144.
- , 2009, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford Law Books: Stanford University Press.
- Northcutt, S. and C. Madden, 2004, *IT Ethics Handbook: Right and Wrong for IT Professionals*, Syngress.
- O’Neil, O., 2002, “Trust is the first casualty of the cult of transparency,” *The Telegraph*, 24 April, available online.
- O’Reilly, T., 2007 [2005], “What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software,” *Communications & Strategies*, 65(1): 17–37; available online. [The earlier, 2005 version, is linked into the Other Internet Resources section below.]
- Parrish, J., 2010, “PAPA knows best: Principles for the ethical sharing of information on social networking sites,” *Ethics and Information Technology*, 12(2): 187–193.
- Pettit, P., 2009, “Trust, Reliance, and the Internet,” In van den Hoven and Weckert 2008.
- Plaw, A. 2013, “Counting the Dead: The Proportionality of Predation in Pakistan,” In Strawser 2013.
- Planned Parenthood, 2017, “New Study Shows Virtual Reality Can Move People’s Views on Abortion and Clinic Harassment,” [available online]
- Plato, “Phaedrus,” in *Plato: The Collected Dialogues*, E. Hamilton and H. Cairns (eds.), Princeton: Princeton University Press, pp. 475–525.
- Poushter J., 2016, “Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies: But advanced economies still have higher rates of technology use,” *Pew Research Center*, 22 February 2018 [available online]
- Powers, T., 2011, “Prospects for a Kantian Machine,” in Anderson and Anderson 2011.
- Purcell, M., 2008, “Pernicious virtual communities: Identity, polarisation and the Web 2.0,” *Ethics and Information Technology*, 10(1): 41–56.
- Reynolds, G., 2009, *Ethics in Information Technology*, (3<sup>rd</sup> ed.), Course Technology.
- Russell, S. and P. Norvig, 2010, *Artificial Intelligence: A Modern Approach*, (3<sup>rd</sup> ed.), Massachusetts: Prentice Hall.
- Schmidt, C. T. A., 2007, “Children, Robots and... the Parental Role,” 17(3): 273–286.
- Schulzke, M., 2010, “Defending the Morality of Violent Video Games,”

- Ethics and Information Technology*, 12(2): 127–138.
- Searle, J., 1980, “Minds, Brains, and Programs,” *Behavioral and Brain Sciences*, 3: 417–57.
- Shannon, C.E., 1948, “A Mathematical Theory of Communication”, *Bell System Technical Journal*, 27(July, October): 379–423, 623–656. [available online]
- Shannon, C. E. and W. Weaver, 1949, *The Mathematical Theory of Communication*, University of Illinois Press.
- Sharkey, N.E. 2011, “The automation and proliferation of military drones and the protection of civilians,” *Journal of Law, Innovation and Technology*, 3(2): 229–240.
- Singer, P. W., 2009, *Wired for War: The Robotics Revolution and Conflict in the 21<sup>st</sup> Century*, Penguin (Non-Classics); Reprint edition.
- Siraj-Blatchford, J., 2010, “Analysis: ‘Computers Benefit Children’,” *Nursery World*, October 6. [available online]
- Soukup, C., 2007, “Mastering the Game: Gender and the Entelechial Motivational System of Video Games,” *Women’s Studies in Communication*, 30(2): 157–178.
- Søraker, Johnny Hartz, 2012, “How Shall I Compare Thee? Comparing the Prudential Value of Actual Virtual Friendship,” *Ethics and Information technology*, 14(3): 209–219. doi:10.1007/s10676-012-9294-x [available online]
- Spafford, E.H., 1992, “Are computer hacker break-ins ethical?” *Journal of Systems and Software* 17(1):41–47.
- , 2007, “Are Computer Hacker Break-ins Ethical?” in Himma 2007a, pp. 49–59.
- Spinello, R. A., 2001, *Cyberethics*, Sudbury, MA: Jones and Bartlett Publishers. (2nd ed., 2003; 3<sup>rd</sup> ed., 2006; 4<sup>th</sup> ed., 2010).
- , 2002, *Case Studies in Information Technology Ethics*, Prentice Hall. (2<sup>nd</sup> ed.).
- Sprenger P., 1999, “Sun on Privacy: ‘Get Over It’,” *Wired*, January 26, 1999. [available online]
- Statista, 2018, “Number of social media users worldwide from 2010 to 2021 (in billions)”, [available online].
- Strawser, B.J., 2013, *Killing by Remote Control: The Ethics of an Unmanned Military*, Oxford: Oxford University Press.
- Sullins, J. P., 2000, “Transcending the meat: immersive technologies and computer mediated bodies,” *Journal of Experimental and Theoretical Artificial Intelligence*, 12(1): 13–22.
- , 2005, “Ethics and Artificial life: From Modeling to Moral Agents,” *Ethics and Information technology*, 7(3): 139–148. [available online]
- , 2006, “When Is a Robot a Moral Agent?” *International Review of Information Ethics*, 6(12): 23–30. [available online]
- , 2009a, “Artificial Moral Agency in Technoethics,” in Luppigini and Adell 2009.
- , 2009b, “Telerogetic weapons systems and the ethical conduct of war,” *APA Newsletter on Philosophy and Computers*, P. Boltuc (ed.) 8(2): 21.
- , 2010, “Rights and Computer Ethics,” in Floridi 2010a.
- , forthcoming, “Deception and Virtue in Robotic and Cyber Warfare,” Presentation for the Workshop on The Ethics of Informational Warfare, at University of Hertfordshire, UK, July 1–2 2011
- Symantec, 2018, Internet Security Threat Report (ISTR), *Symantec Security Response*, [available online]
- Tavani, H. T., 2007, “The Conceptual and Moral Landscape of Computer Security,” in Himma 2007a, pp. 29–45.
- , 2010, *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing*, (3<sup>rd</sup> ed.), Wiley.
- Tavani, H. and J. Moor, 2004, “Privacy Protection, Control of Information, and Privacy-Enhancing Technologies,” in *Readings in Cyberethics, second edition*, Spinello, R. and Tavani, H. (eds.), Sudbury: Jones and Bartlett.

- Taylor, N., J. Jenson, and S. de Castell, 2009. "Cheerleaders/booth babes/ Halo hoes: pro-gaming, gender and jobs for the boys," *Digital Creativity*, 20(4): 239–252.
- Turing, A. M., 1948, "Machine Intelligence", in B. Jack Copeland, *The Essential Turing: The ideas that gave birth to the computer age*, Oxford: Oxford University Press.
- , 1950, "Computing Machinery and Intelligence", *Mind*, 59(236): 433–460. doi:10.1093/mind/LIX.236.433
- Vallor, S., 2010, "Social Networking Technology and the Virtues," *Ethics and Information Technology*, 12(2, Jan. 6): 157–170.
- , 2011, "Flourishing on Facebook: Virtue Friendship and New Social Media," *Ethics and Information Technology*, 1388–1957, pp. 1–15, Netherlands: Springer.
- , 2016, *Technology and the Virtues: A Philosophical Guide to a Future worth Wanting*, Oxford: Oxford University Press.
- Van den Hoven, J. and J. Weckert (eds), 2008, *Information Technology and Moral Philosophy*, Cambridge: Cambridge University Press.
- Von Neumann, J., 1966, *Theory of Self Reproducing Automata*, edited and completed by A. Burks, Urbana-Champaign: University of Illinois Press.
- Wallach, W., 2011. From Robots to Techno Sapiens: Ethics, Law and Public Policy in the Development of Robotics and Neurotechnologies, *Law, Innovation and Technology*, 3(2): 185–207.
- Wallach, W. and C. Allen, 2010, *Moral Machines: Teaching Robots Right from Wrong*, Oxford: Oxford University Press.
- Warschauer, M., 2003, *Technology and Social Inclusion: Rethinking the Digital Divide*, Cambridge: MIT Press.
- Weckert, John, 2007, "Giving and Taking Offence in a Global Context," *International Journal of Technology and Human Interaction*, 3(3): 25–35.
- Westin, A., 1967, *Privacy and Freedom*, New York: Atheneum.

- Wiener, N., 1950, *The Human Use of Human Beings*, Cambridge, MA: The Riverside Press (Houghton Mifflin Co.).
- , 1961, *Cybernetics: Or Control and Communication in the Animal and the Machine*, 2nd revised ed., Cambridge: MIT Press. First edition, 1948.
- Woodbury, M. C., 2010, *Computer and Information Ethics*, 2<sup>nd</sup> edition; 1<sup>st</sup> edition, 2003, Champaign, IL: Stipes Publishing LLC.

## Academic Tools

-  How to cite this entry.
-  Preview the PDF version of this entry at the Friends of the SEP Society.
-  Look up this entry topic at the Internet Philosophy Ontology Project (InPhO).
-  Enhanced bibliography for this entry at PhilPapers, with links to its database.

## Other Internet Resources

- Clarke, R., 2000, "Information wants to be Free...", unpublished manuscript.
- O'Reilly, T., 2005, "What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software".
- IEEE, 2018, "The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems".

## Related Entries

Aristotle, General Topics: ethics | artificial intelligence: logic and | computing: and moral responsibility | Dewey, John: political philosophy | ethics, biomedical: theory | evil: problem of | information technology:

phenomenological approaches to ethics and | life | pornography: and  
censorship | property: intellectual | Turing test

## Notes to Information Technology and Moral Values

1. Roger Clarke is quoting this statement from Brand; it was originally printed in a report/transcript from the conference in the May 1985 “Whole Earth Review”, p. 49.

2. See Acceleration Studies Foundation, Future of Humanity Institute, and H+.

Copyright © 2021 by the author

John Sullins