POST-DIGITAL CYBERETHICS

by

The Honorable John McClellan Marshall

Senior Judge, Fourteenth Judicial District of Texas
Honorary Professor of the University, UMCS, Lublin, Poland
Member, International Academy of Astronautics

"The Times They Are a-Changin'"
~ Bob Dylan (1965), Nobel Laureate

It is a tendency of human nature to reflect and reminisce on what has happened in their personal experiences. Over time, this is translated into a nostalgia for "things as they once were". This is perhaps the greatest delusion to which human beings are susceptible because it ignores the one true rule of the Universe: change. In fact, we probably see those things as we are.[1] That said, we may not even be seeing them as we ourselves were "then", depending in part on our own life experiences.

This is followed closely by the notion that time is passing by very rapidly. The reality is that, from the perspective of the viewer, time passes at the same rate that it always has. What is important about the relationship of these two concepts is that the pace of change is independent of the apparent rate at which time passes.

For the latter half of the 20th Century, the world was collectively pursuing technological innovation in fields that have focused on engineering solutions to problems as diverse as space flight and non-stick cookware. This pursuit was not limited by national boundaries or policies, but was driven in part by economics and in part by politics. At the same time, the expansion of technology impacted humanity in such matters as treatments for diseases, some of which had been around for centuries and some of which were brand new. Taken as a whole, this period represents what could be termed the Technological/Digital Revolution. It was, to some extent, a period in which the pursuit was an end in itself and did not look at long-term outcomes or perceive consequences. In some respects this could be compared to a dog that chases a truck, because the question that arises is, "What will the dog do with the truck if it catches it?"

To an extent, the "dog" has in fact caught the "truck", and the Technological/Digital Revolution has evolved into a Post-Digital Revolution. The reality of the 21st Century demonstrates this dilemma quite clearly in the collision of technological innovation with arts and the humanities.

The impact of this collision is summed up in the word "cyberethics". It is defined as *the relationship between the ethical and legal systems that have been developed to serve humanity from ancient times to the present, as expressed in our philosophical and ethical systems of thought*

[1] Anaïs Nin, *Seduction of the Minotaur*, Vol. 5 of *Cities of the Interior* (1959). By extension, a professor at a college once said, "[The college] isn't what it used to be. . ., and it never was."

and, for society, in the judicial process as contrasted with the ability of computer-driven technology to operate outside those conventions with almost no limits.[2] In essence, the *cyberethical problem* has been accelerated by the pace of technological innovation. As a result, the impact is not merely in terms of time, but would appear to be expanding societally in scope as well.

Until recently, the pace of innovation has been most visible in those fields that are capable of creating engineering solutions to human problems. Digital technology, however, has altered the thrust of such innovations in ways that spread the impact quite broadly. The chronicalling of the sweep of technology through the world was recorded first on tape, then on laser discs, then on digital hard drives. As a result, the line between mere technology and the digital reality to which it gave birth became blurred, if not nonexistent.

An example of this in the medical field was the development of Computed Axial Tomography (CAT) or CT scanning technique. This system takes very detailed photographs of the human body which it then stores in a digital form that allows for a computer to analyze them. In this way, the diagnostic skill of the physician is enhanced by the machine. The very enhancement, however, diminishes the human element in the process, which arguably reduces the physician to an extension of the machine. The digital base of the CT process, however, allows for the possiblity of a "hack" that could alter the diagnostic outcome to the detriment of the patient.

On the societal level, the expansion of the recordation of information, sometimes referred to as "Big Data", has led to a subtle change in the day-to-day employment of many occupations. The definition of "workplace" allowed by the availability of data on a wide scale has led to an increase in "work from home" employment in many fields. Further, it has fostered the creation of a "digital nomad" who does not go into an office as a routine part of his or her job, yet is able to perform the tasks "normally."[3] One result of this is an increasing dissociation of the workers from one another and, therefore, a lessening of the value of human interaction in the process of "doing the job."

The downside of this hybridization is most readily apparent in the academic environment. In addition to the potential compromise of the integrity of academic records of students, with the consequent falsification of résumés when the student enters the work world, there is the question of the quality of the education itself. While researchers often work in a highly individualized situation, the process of education historically has involved interaction between professors and students. The introduction of conferencing software that allows "remote" instruction by definition removes the student from the professor if only by the ability to "mute" the conversation or turn off the video and wander away from the class. It also allows the responses of the student to inquiries from the professor to be falsified by access to resources such as smart phones located

[2]This concept was originally articulated by the author in the paper "The Terminator Missed a Chip!: Cyberethics", presented at the International Astronautical Congress of 1995, Oslo and originally published by the American Institute of Aeronautics and Astronautics, Inc. with permission. Released to IAF/AIAA to publish in all forms. The corollary is the ability of technology to drive alterations in those conventions without regard to human input in a societal "default" to the machines.

[3]Bryan Lufkin,"Is the great digital-nomad workforce actually coming?", June 15, 2021 (BBC), https://www.bbc.com/worklife/article/20210615-is-the-great-digital-nomad-workforce-actually-coming?ocid=ww.social.link.email

outside the range of the camera. Although detailed studies of the long-term impact of this type of instruction environment have yet to emerge, there is already some evidence that the quality of the educational product is degraded, and quality of education may take a back seat.

Unfortunately, some of the studies that have been done tend to look at "cost effectiveness" as a major factor in the decision to "go remote".[4] That said, the problem of remote education may be compounded by the lack of innovation in the format. Indeed, the technology seems simply to be used to re-create the classroom without human contact.[5] The problem is further compounded by the disconnect between the faculty and students such that the student has little "feel" [human impact] for the material being studied. Such dissociation arguably illustrates, for some, the distinction between "book learning" and "education" particularly as the student moves into "the real world."

A further example of the extent of the diminution of the human factor in an institutional context is the operation of some governmental functions. For example, in the processes associated with the judicial function, a central element is the availability of trustworthy evidence. At the outset, it needs to be remembered that the court is an inherently human institution, designed to serve society by resolving disputes for people who cannot resolve them for themselves. Recent research has revealed that it had its origins in the earliest, perhaps pre-history, phases of the human presence on the planet. Indeed, the concept of "trustworthiness" is an uniquely human construct that underlies much of modern society. In the Post-Digital world, however, trustworthiness itself may be getting redefined.

Historically, the standard for trustworthy evidence in court has been in the form of testimony of live witnesses in open court, aided by photographs, documents, and items that contribute to the presentation of the facts to a judge or jury. Such evidence reflects the sensual impressions of the witness as well. Sometimes, a witness has died before the trial, so he or she was typically brought into court in the form of a written deposition. Thanks to digital technology, this person could be resurrected and testify as a hologrammatic projection. "Photographs", as such, no longer exist. They are reproduced as "images" created digitally by what the "camera" saw. While that image may be more accurate than eyesight filtered through a human brain, it is much more vulnerable to manipulation, thus introducing at the threshold an element of distrust as to the authenticity of the image. Similar manipulation as to voice recordings or documents potentially dilutes the trustworthiness of the evidence and, therefore, of the process itself. For the lawyer, characteristically educated in the humanities, the need for some education as to the digital capabilities is necessary to prepare adequate examination of the evidence or "witnesses" in a trial context.

Perhaps an even more disquieting example of the ability of digital manipulation of the facts occurred several years ago during a lawsuit. This was in relation to the transfer of funds from a bank in the United States to an overseas account in defiance of a temporary injunction. The attorneys for the plaintiff which had sought the injunction were not "digital savvy", so they sought advice on how to recover the funds. They were advised that if they

[4]See U.S. Department of Education, Office of Educational Technology, "Understanding the Implications of Online Learning for Educational Productivity" January 2012.

[5]See Justin Reich, *Failure to Disrupt: Why Technology Alone Can't Transform Education* (Harvard University Press, 2020).

obtained the numerical code by which the funds had been sent and simply reversed them, there would be one set of "ones and zeros" left over. With any luck, all that would be necessary would be to reverse those final digits to retrieve the money from overseas to the American bank account. Despite skepticism on the part of the attorneys, the instructions were followed, and the money was recovered within 24 hours of the initial discovery of the transaction. The fact that this created a small diplomatic incident was beside the point. What is significant about this example is the fact that the course of justice was in fact controlled by the digital technology of the times. There can be little question that this creates a concern about the trustworthiness of the facts that are then presented to a jury in the full trial.

In a particular area of the law, the intersection between technology and the humanities is quite clear: the arts. The term "arts" would embrace not just the plastic arts, but intellectual property itself in the broadest sense.[6] Further, the very concept/definition of "intellectual property" (IP) may have already undergone a change in the Post-Digital Revolution. For example, few would deny that a book or a painting would qualify as "IP". The question is presented, however, as to whether a digital copy of a book or a painting or either one that is initially created digitally is IP that is subject to protection as the author's creation through copyright or trademark. An item as prosaic as a piece of jewelry might seem at first to be IP, regardless of how many copies were made. If, on the other hand, the designer of the jewelry were to include some extra "signature" in the original design, such as a stone of a different color in a particular location, the question becomes whether copies of the design without that stone would be a violation of the IP rights of the original creator.[7] Put another way, would the presence or absence of the "signature" determine the right to protection under the law?

When an artist creates a painting, there is undeniably a certain IP character to the original item as produced. If the painting should have a copyright symbol on it, then undoubtedly it would have some protection under the law. On the other hand, if the painting were sold or donated to a museum without such a notice, would the common law copyright, and therefore, the ability to protect the IP pass to the new "owner", or is some vestige of it remaining with the artist? The answer to this question is made even more complex by the notion that even after a purchase of a work of art, the "owner" is merely a steward of it, because no one really "owns" art. That said, in the Post-Digital world, a painting in a museum could be copied an infinite number of times and distributed throughout the world without the knowledge of (or compensation to) the artist. In such a situation, the legal concept of IP and its protection simply cease to exist.

At its foundation, the Post-Digital Revolution has a potentially fatal, yet systemic, flaw. . .the digital base itself. The creation of digital code as a mechanism for the creation of and support of technological innovation is certainly an act of creativity on the part of the writer. Is it a book in the same sense as *The Decameron*, or is it

[6]"Intellectual property" can be characterized as non-physical property that is the product of original thought. Typically, some rights do not surround the abstract non-physical entity; rather, intellectual property rights define the parameters of the control of physical manifestations or expressions of ideas. See Moore, Adam and Ken Himma, "Intellectual Property" in Zalta, Edward N., ed., *The Stanford Encyclopedia of Philosophy* (Winter 2018 Edition), https://plato.stanford.edu/archives/win2018/entries/intellectual-property.

[7]Such a "signature" is, in fact, a characteristic of the jewelry designs of an Italian designer, Roberto Coin.

merely an intangible tool used to create other "books"? As an item of IP, a computer program, whether an operating system or an app, becomes available to be read when introduced into a computer or placed for sale on the internet. In a pristine form, it probably can be protected by copyright or trademark conventions with little problem. The question is whether the software used in a digital creation of an item or a modification of it by a subsequent user provides the creator of the software with an entrée into the "rights" arising from the final product.

That said, however, a clever code writer can take that code, add or change a few parts of it, and, in effect create a "new" code that is in fact in part "stolen" from someone else. Does the original writer have any rights? The answer, of course, is "yes" and "no". A recent lawsuit involving the rights to a particular portion of a piece of music illustrates the problem. At its heart was the question of "plagiarism".[8] Based on the legal standard in this case, under a test of "substantial similarity", whether or not a modification of a computer program would be deemed an infringement is problematical. Again, the question of the trustworthiness of the evidentiary presentation is central not just to the legal outcome, but as a general proposition.

The question that needs to be asked, in modern times, is whether close monitoring of the citizenry is consistent with the "right of the people to be secure in their persons, houses, papers, and effects."[9] While the existence of the "digital footprint", including facial recognition software, of the citizen is now beyond question, from a philosophical perspective it clearly endangers the notion that individual rights are God-given in the Jeffersonian world and not state-given as posited by Frederick the Great. As a consequence, it falls to government to protect the individual against the diminution of his or her "space" from digital willy-nilly erosion.

Of course, in the criminal law, the Post-Digital Revolution has been very much a part of the judicial process for more than twenty years. The simple attachment of individuals to their smart phones in the modern day provides law enforcement with an ongoing monitoring system over movement and activity. Such evidence, including location and phone records, thus adduced pursuant to proper warrants is routinely introduced in court as trustworthy for the jury to consider. That the mere non-governmental suveillance capability exists outside of the realm of the need for a search or arrest warrant, as required by the Fourth Amendment to the Constitution, is disquieting.

In addition to the legal community, there are other institutions the trustworthiness of which is questionable in the Post-Digital environment. One of the most prominent, and yet pedestrian, is the automobile industry as a whole, without regard to fossil fuel or electric propulsion. According to Alfred Katzenbach, the director of information technology management at Daimler, the radio and navigation systems of the 2009 S-class Mercedes-Benz alone require over 20 million lines of code alone and nearly as many ECUs as the Airbus A380 (excluding the plane's in-flight entertainment system). In 2009, the business research firm Frost & Sullivan estimated that cars may require 200

[8]See *Skidmore v. Led Zeppelin, 952 F.3d 1051 (9th Cir. 2020).* The issue before the court was "substantial similarity", not extending copyright protection beyond the provisions of the original deposit copy.

[9]Amendment IV, Constitution of The United States.

million to 300 million lines of software code in the near future.[10]

Similarly, modern aircraft are characterized by extensive electronic avionics systems. The avionics system in the F-35 Joint Strike Fighter, which became operational in 2010, requires about 5.7 million lines of code to operate its onboard systems. Boeing's 787 Dreamliner, in service since 2010, requires about 6.5 million lines of software code to operate its avionics and onboard support systems.[11] The very quantity of the combination of lines of coding and the circuitry necessary to implement them may be in fact the Achilles heel of the Post-Digital Revolution.

The key to understanding this problem is focused on two major components of most of the modern electronic/digital control systems: the Controller Area Network (CAN) bus, and the Telematic Control Unit (TCU). At its most basic, CAN was originally developed by Bosch in 1985 to facilitate connection between various functions in automobiles. It was refined and is now considered the standard in its field. [ISO 11898]. In essence, the CAN bus is what allows modern vehicles, including some aircraft, to function at all. The TCU is an adjunct to the CAN and connects it to external inputs such as radio and GPS.

In 2009, the Center for Automotive Embedded Systems Security, a consortium of professors from the University of Washington and University of California San Diego, embarked on a project to subvert the functioning of the CAN bus in modern automobiles. They attached a laptop to the on-board diagnostics port and introduced a protocol that was designed to detect flaws in the CAN bus. These flaws were then attacked so as to immobilize or even restructure the vehicle's functions.[12] It does not require a major imaginative leap to add the TCU to this construct and enable hacking into the CAN bus of one's automobile from halfway around the world. Certainly this should be considered as a safety issue in the design of "self-driving" cars that depend upon GPS to get from one place to another. The legal liability in the event of an accident would likely extend beyond the manufacturer of the vehicle to the creator of the chip and the code the failure of which contributed to any injury to human beings. Statutes of limitations would undoubtedly complicate the matter considerably.

From a broader perspective the implications of such a technological/cyberattack are enormous. Indeed, such a concept could very well alter the shape of the battlefield, or even corporate management, in the future. With the creation of the Space Command in the armed forces of the United States, there is the growing political capability of extending the reach of such digital technology. This could reach out and immobilize an opponent's power grid, aircraft or ships, or even redirect so-called "smart" bombs to return to their point of origin. As was recently discussed by the Vice Chief of Space Operations of the Space Command, there are various techniques, including lasers, that would be available to disrupt an opponent's satellite operations.[13]

[10]Robert N. Charette, "This Car Runs on Code", *IEEE Spectrum* (February 2009).
[11]*Id.*

[12]Paul Ridden, "Automobile computer systems successfully hacked", New Atlas (May 2010), https://newatlas.com/vehicle-computer-systems-hacks/15156.
[13]Ryan, Morgan. "China, Russia Attacking US Satellites 'every single day' Space Force general says", *American Military News* (December 1, 2021).

An alternative technique could be the transmission of viral code through the TCU (or its equivalent) into an opponent's software system. Though it is true that military computerized defense systems have strong firewall protection, none is invulnerable in the Post-Digital age. Within the foreseeable future, it may be that a soldier "in the field" will only need a smart phone instead of a rifle and a degree in computer science in order to accomplish the mission of disabling an opponent's cyberdefenses.

What is at stake in this the modern environment is nothing less than a potential for the societal loss of confidence in those institutions that have defaulted a significant portion of their functions to machines. Indeed, the self-confidence of humanity at large would likely be impacted, resulting in a sort of "if it's in the computer, it is beyond my control" attitude. It is not relevant that this default may be well-intentioned or done in the name of "efficiency". The reality is that human society is not inherently "efficient". An apocalyptic view of this ultimate spiritual bankruptcy was presented in the visionary 1927 motion picture *Metropolis*, in its presentation something of a horror story, yet a fable for the modern time.[14]

To be certain, there will be changes in how society and its institutions function. After all, if society cannot trust the machines that it is creating to be secure in carrying out their functions, then how can the results of that functioning be measured against such values as "truth", "accuracy", "beneficial", or "false", "harmful"? Further, the answers to those questions must be considered as to whether they are to apply on an individual level or to society as a whole. Indeed, after several millennia of a value system that has fostered material, intellectual and spiritual growth, the question is to what extent should society discard that system in favor of "Post-Digital efficiency", knowing at the threshold that it is so deeply flawed?

Moving forward in the 21st Century, there is little doubt that the technology-driven Post-Digital Revolution will continue, probably at an increasing speed. More inventions will be created that require new coding to function, and that coding will require new forms of technology to store it and to implement its objectives. In effect, this trend, which drives with it the gradual diminution of the human element in day-to-day activities and occupations, brings the cyberethical problem into clear and disturbing focus.

The author gratefully acknowledges the thoughtful contributions of Dr. Roger Malina, Dr. Mihai Nadin, Professor Nishiki Sugawara-Beda, and Gilbert M. Swift, Esq. to the development of this article.

[14] A German expressionist science-fiction drama film directed by Fritz Lang. It was written by Thea von Harbou in collaboration with Lang and is based on von Harbou's 1925 novel of the same name. It is considered one of the most influential movies ever made.