Preface

In the 1948 issue of *Bell Systems Technical Journal*, researcher Claude Shannon published the article, "A Mathematical Theory of Communication." The arguments Shannon made were taken from his own observation of electrical relays, from which he started to develop the idea that all communication was reducible to basic logic, and from there to two basic elements, "yes" and "no," signified mathematically as "one" and "zero."[1] Shannon had no idea that the theory he was proposing would be the spark for a global information revolution, but scientists and engineers immediately saw the potential in his idea, a revolutionary system of encoding data that inspired decades of research and development.

It took half a century for digital technology to become the norm and this involved inventing new methods for encoding data that gave rise to new technological fields including personal computing, cellular communication, and Internet networking. Each of these technological fields was transformative on its own, but each was also a stepping stone in the progression inspired by Shannon's theory: the digitization of all human communication and knowledge. This process has been so encompassing that the entire period from the 1980s to the present, has been called "The Digital Age," bringing a symbolic end to the "Industrial Age" in which industrial manufacturing and consumer machines changed every aspect of society.

The Power of Knowledge

The idiom "knowledge is power," often attributed to Sir Francis Bacon's *Meditationes Sacrae* (1597), became a symbolic expression of the scientific revolution.[2] The essential meaning is that knowledge is the essential fuel for personal, social, and societal development, allowing individuals and groups to understand and address their needs, empowered by a rational understanding of the problems they face. One of the hallmarks of the digital age has been the conversion of human knowledge to digital media, which led to a subsequent decentralization and democratization of both knowledge and power.

Digitization, the conversion of data to digital "ones" and "zeroes," greatly enhanced the capacity for preserving, transmitting, and communicating information. The digital age is also therefore known as the "information age," a term attributed to Richard Leghorn, a 1960s pioneer in aerospace intelligence technology.[3] The ability to digitize information developed alongside "digital storage," from the first floppy disks to later DVDs and drives, that allowed for encoded data to be stored and transported. The first personal computers, introduced to the public in 1975, brought digital technology to the consumer market.

From the very beginning of the digital age, there have been pioneers who envisioned that digital technology would be a powerful force in the democratization of knowledge. One such pioneer was Michael S. Hart, who created Project Gutenberg in 1971, with the goal of creating a digital public library of books in the public domain, available to the public for free. By 2015, Project Gutenberg had digitized more than 49,000 books, and was still guided by Hart's belief that digital technology

could "universalize" knowledge because digital books could be cheaply produced, without the need for physical paper and ink, and could be reproduced and shared infinitely from a single copy.[4] Similar efforts to create public libraries of important information followed. For instance, in 1994, the Library of Congress began its Digital Library Program (NDLP), which resulted in the digitization of thousands of books, periodicals, manuscripts, photos, videos, and audio files for public use and research.[5] Digitization would not have been as transformative without the capability to easily transmit digital data. This is the primary innovation behind the Internet, the name now used for the networks of computers linked through utility lines that allow users to transmit information instantly across any distance. Interestingly, the pioneers that developed the first "Internet," known as the World Wide Web, also envisioned this technology as a powerful tool for democratization, sharing the "power" of knowledge with everyone around the world. The World Wide Web Consortium, established by pioneer Tim Berners-Lee, was created with these goals in mind, fostering a new, non-corporate, non-governmental mode of communication for the people that would foster the free, open, exchange of information and ideas.[6]

The democritization of knowledge *has* been a central feature of the digital age. The invention of "electronic mail" enabled individuals to instantly share documents, videos, audio files and to communicate freely across International lines, and the addition of instant online chat and video chat programs effectively eliminated the monopoly of long distance phone providers on International communication. However, as the digital age progressed a new breed of corporate giants emerged, competing to gain a monopoly over the new digital information market.

Management consultant Peter Drucker theorized in his 1960s books and articles that the economies of western nations would become "knowledge economies," in which data would become the most important resource.[7] The Internet corporations of the twenty-first century, like Google and Facebook, have made Drucker's predictions reality, essentially using customer data as currency to be traded with advertisers for revenue. Internet companies provide free services, but in return collect and analyze all data provided by their customers, and also filter the Internet experience, inundating users with a constant flow of directed advertisements based on their history of Internet browsing. Critics of this development, including Internet pioneer Tim Berners-Lee, have spoken out against corporate manipulation of the Internet, calling it a threat to the potential for democratization that the Internet represents.

Corporate manipulation aside, many nations around the world censor or limit Internet communication in an effort to protect traditional institutions of power. The so called "Arab Spring" of 2011, in which a wave of protests, many organized through digital communication, spread from Tunisia into Egypt and throughout the Middle East, has been seen as the prime example of how digital communication is transforming politics.[8] Fearful of this new capacity for social/political organization many nations have enacted laws and policies that prohibit certain Internet sites and services and effectively limit free speech and expression in digital domains.

Even in nations that have attempted to protect free speech and expression on the Internet, digital technology poses a host of new national security issues, including

the potential for terrorists to use social media for organization and recruitment and the growing fields of cyberterrorism and cyberwarfare in which digital weapons are used to disrupt or destroy computer systems in enemy nations. In attempting to address these concerns, the United States and many other governments, have engaged in controversial digital surveillance programs, and these programs are part of a growing field of concern regarding "digital rights" and "digital privacy," one of the central legal/human rights issues of the twenty-first century.

As the digital exchange has become more important, there is also increasing concern that access to the latest in digital technology is creating new socio-economic classes around the world. This phenomenon, often called the "digital divide" by social scientists, is a growing problem as access to technology and careers in emerging digital fields is unevenly distributed across gender and socio-economic lines. The problem is especially acute in the field of education, where digital tools and Internet access are increasingly important in preparing students for professional careers. The digital divide is one of the most essential and pressing humanitarian issues of the twenty-first century, drawing together issues in education, public and social policy, and the social sciences.[9]

The Cyber Cipher

In his 1982 story *Burning Chrome,* science fiction author William Gibson invented the term "cyberspace," which he envisioned as a virtual world contained within computer networks where "hackers" could interact with computers linked to financial, governmental, and corporate security systems. Gibson, whose books helped create the "cyberpunk" genre, envisioned a dystopian future in which nation-sized corporations dominated the economic and social landscape and technological rebels fought for political freedom.[10]

Today, "cyberspace" is an often-used slang expression for the virtual "world" of the Internet. While the darkest predictions of cyberpunk have not come to fruition, Internet media and communication *have* created a "virtual level" of existence that has become increasingly essential to modern lives and livelihoods. Commerce, education, and recreation take place through virtual platforms and social networks accessible from any location, and this has rapidly become the new norm of social interaction. The importance of this new digital mode of existence is so prevalent that educational expert Mark Prensky coined the term "digital natives" in 2001, as a way to refer to the first generation of young people who "grow up" as "native speakers" of a new language based on digital communication and technology.[11]

As individuals communicate, shop, play, and conduct business online, they create an "online identity" or "online presence," formed from their browsing history, social media activity, and both intentional and unintentional communication. This online identity is one of the most important tools in the digital age, and some analysts of the digital age have theorized that a person's online persona may one day be more important professionally than traditional professional references. In the 2010s, there has been increasing interest in "personal branding," by controlling one's online identity to present a more positive professional image.

However, online identities have also become targets for exploitation. Cybercriminals, for instance, can use malicious codes and programs to conduct identity theft, using information found online to make purchases or to apply for loans and credit. Likewise, the phenomenon of cyberbullying, in which an individual torments, insults, or harasses another individual through social media and digital channels, is another example of how a person's online identity presents a target for abuse. Sexual predators and violent criminals have used online tracking to locate victims and an increasing study of online misogyny and racism indicates that the freedom of expression offered through digital media has also made the Internet a haven for those who wish to conduct abuse or issue threats of racial or misogynistic violence. As police struggle to address the prevalence of virtual crime, activists and social scientists are faced with a conundrum, making online environments safe for users without censoring or restricting free speech. Psychologists have also found that the gradual acclimation to digital trends and tools is having a profound and potentially lasting affect on the human brain, in both positive and negative ways. Educators note that individuals are more accustomed to writing and literary expression, thanks to social media, but also that "digital natives" have difficulty with long-term concentration and focus. Likewise, as the tools of communication from the previous age become obsolete, social scientists are increasingly considering whether or not humanity is losing important skills and techniques in the process.

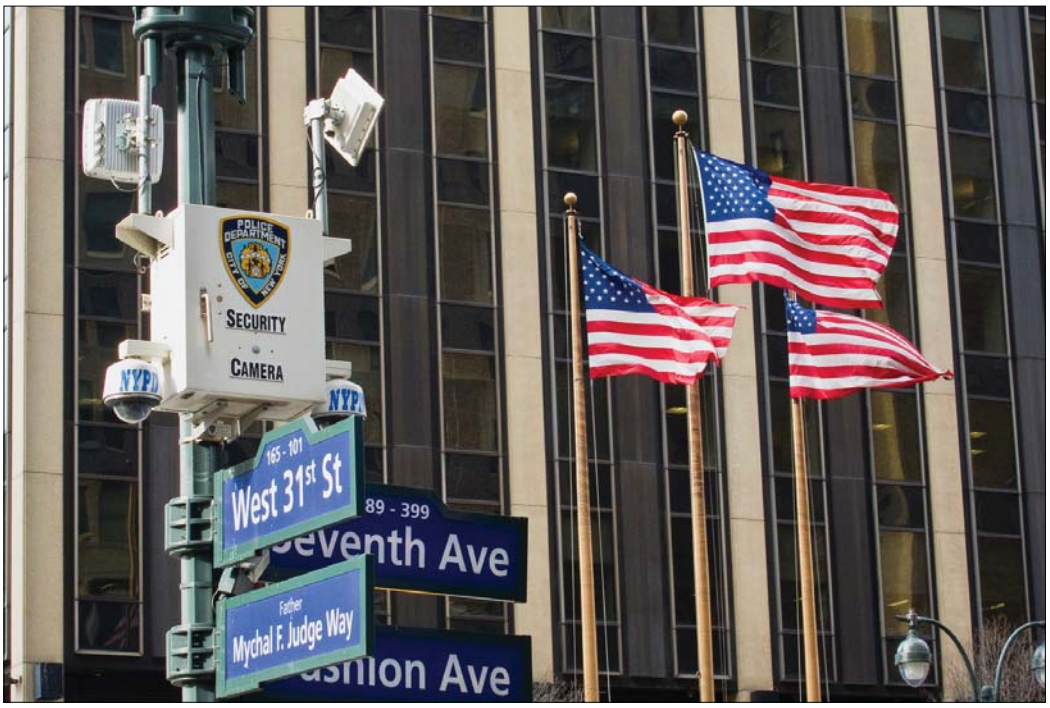
It is important to remember that the digital age is in its infancy. Though digitization began in the 1960s, the broader, social transition began far more recently and the social institutions and structures of society are only now beginning to adjust. The digital age offers tremendous benefits, but these benefits come with a cost, in the form of industries, livelihoods, and cultural institutions made obsolete by new norms of communication, commerce, and recreation. Moving forward, global societies have difficult decisions and negotiations that will determine how digital technology shapes evolution, what aspects of the past will be preserved, and how growth and change can be accommodated without sacrificing

Micah L. Issit

Notes

1. Waldrop, "Claude Shannon."
2. Berend, *An Economic History of Nineteenth-Century Europe*, 47.
3. Gleick, "The Information Palace."
4. Tucker, "The Inventor of the Digital Age."
5. "About Digital Collections & Services."
6. Jeffries, "How the Web Lost its Way—And its Founding Principles."
7. Wartzman, "What Peter Drucker Knew About 2020."
8. "The Arab Spring: A Year of Revolution."
9. "Digital Divide."
10. Thill, "March 17, 1948: William Gibson, Father of Cyberspace."
11. Prensky, "Digital Natives, Digital Immigrants."

1
Individual Rights



Credit: © Viviane Moos/Corbis

American flags fly at full mast in front of Penn Station in NYC near a street sign for Father Mychal Judge Way. Father Judge is one of the most famous victims of the World Trade Center attack and known as the beloved New York Fire Department chaplain. New York City's police department is using tens of thousands of closed circuit security cameras set up on the streets as surveillance (like in this photo), part of a Homeland Security and Defense program to track terror suspects and solve crimes. Civil-rights activists worry about the impact of the new cameras and the people's right to privacy.

Toward a Digital Bill of Rights

In many ways, cyberspace is the new frontier of human exploration. Like the colonies founded by oceanic explorers in antiquity, cyberspace offers previously unimagined resources and the ability to explore new domains of thought and expression. However, the digital world is also unregulated, in many ways lawless, and fraught with new and unexpected dangers. With the growing importance of digital technology and Internet connectivity, many around the world now believe that digital access is a basic right that should be afforded to all people. However, protecting and maintaining this utility requires addressing fundamental questions about the rights of digital citizens. Many of these issues, including the protection of free speech and the limits of a person's right to privacy, mirror the revolutionary struggles that gave rise to the United States Constitution and its amendments. These issues and a host of new digital-specific concerns are shaping digital rights in the modern era and into the future.

Digital Privacy

As of 2015, all information transmitted through the Internet or digital data carriers by United States citizens is subject to joint ownership. Facebook's policy on data collection, for instance, states clearly that Facebook claims partial ownership over any data provided on a user's Facebook page, including photos, text, and information in the user's personal profile.[1] Essentially then, whatever information users share on sites like Facebook, YouTube, and Twitter, is also being given to and shared with the company and its advertisers.

Ownership of digital data became controversial in the 2000s, as journalists revealed that digital data providers and web-service companies were sharing personal consumer data with the National Security Agency (NSA) and Federal Bureau of Investigation (FBI). These organizations, under the Bush administration, were collecting data as part of a broader effort to prevent foreign and domestic terrorism. The 1978 Foreign Intelligence Surveillance Act (FISA), requires that government agencies obtain special warrants before they can conduct surveillance on American citizens.[2] However, after 9/11 Congress passed measures that allowed security agencies to collect "digital data" without court orders.

Widespread concern about digital surveillance developed only after former NSA analyst Edward Snowden leaked government documents to the press in 2013 that revealed the scope of ongoing surveillance operations. Among other revelations, the leaked documents indicated that the NSA collected more than 250 million emails and contact lists from Facebook, Gmail, and Yahoo[3] and collected millions of facial images from posted photos and web cams that were used to develop software that would allow government agencies to identify individuals by matching facial features

with digital images.[4] In addition, security agencies had been able to obtain access to cell phone records and digital voice data with the cooperation of cell phone carriers like AT&T and Sprint.

There is no explicit right to privacy in the United States Constitution. However, the Fourth Amendment of the Bill of Rights, which guarantees freedom from "unreasonable searches and seizures," has been used to justify protecting the privacy of individuals within their homes and in private communications.[5] In the December 2013 case of *Klayman v. Obama*, Federal District Judge Richard J. Leon ruled that NSA surveillance programs violate Fourth Amendment protections.[6] That same month, however, District Judge William Pauley ruled, in the case of *American Civil Liberties Union v. Clapper*, that the metadata collected by the NSA has already been "shared" with the phone company. Pauley therefore ruled that the consumer has no "expectation of privacy," and that the companies, like Google, Facebook, and Sprint, have the right to share customer data with federal agencies.

A number of important court rulings have extended Fourth Amendment protections to cover digital data and devices. For instance, in 2010, a Federal Appeals Court ruled that government agencies needed a court order to search an individual's email. Similarly, in the 2014 case of *Riley v. California*, the Supreme Court held that government agencies needed a specific warrant to search a cellular phone, even if the owner had already been arrested for a crime.[7] These protections, however, are still subject to interpretation and debate and protecting digital data is complicated by joint corporate/user ownership. Digital rights organizations like the Electronic Frontier Foundation (EFF) are also concerned about corporate invasion of privacy. The EFF has been one of the strongest critics of corporations like Facebook and Google, which collect and analyze communications from users in an effort to create better advertising. The question remains whether regulations should be put into place to clarify the rights of users in terms of *both* government and corporate surveillance.

Corporate Censorship

In 2014 and 2015, the terrorist organization ISIS captured and executed a number of American and European journalists working in the Middle East and distributed videos of the executions (by beheading) to the international media. A number of news agencies worldwide refused to allow videos or photos of the executions to be shared, published, or posted. Social media sites in the United States, like the Google owned site YouTube and the social media giant Twitter, also refused to allow users to post or share ISIS videos claiming justification under "community guidelines" and a corporate designation between "free expression" and "terrorist propaganda."[8] Other media outlets, however, published or allowed users to publish both the full videos and still photos on the basis that the public had a right to uncensored communication and information.

Though most are not as graphic as the infamous ISIS videos, there are a variety of videos and photos published through mainstream media that depict violent events. Military operations and police shootouts with suspects provide examples of

when the media have accepted videos or photos of real-life violence as legitimate journalism. Any content that depicts real-life events in which an individual is killed or physically abused might be considered inappropriate or immoral for distribution, especially by the family, friends, or individuals depicted. Given that moral value is a highly subjective issue, it remains unclear whether or not there is a reliable way to determine when it is appropriate to censor content.

Writing in the *Guardian*, journalist James Ball called Twitter's decision to block ISIS videos a form of corporate censorship. Ball argues that Twitter claims to be a "platform" for public expression and not a news organization. While news organizations can decide what constitutes appropriate content based on internal policies on morality and ethics, Twitter's censorship essentially means that the company is claiming responsibility for what is posted on their site, rather than serving as a legitimate open platform for expression.[9]

Should corporations be permitted to determine when content is morally out of bounds for expression or consumption, or should this decision belong Internet users? In past eras, books, television programs, films, and many other types of media have been censored for moral reasons. United States court rulings have determined that government censorship is permissible only when the speech or expression poses an imminent, demonstrable threat to public safety or directly violates the rights of others. In the digital age, the question is one of corporate censorship. Those interested in the rights of expression must now determine whether social media constitute a legitimate forum for free speech or whether they are corporate publishing platforms that can be justifiably policed and controlled by a corporation's own policies on morality and ethics. As of 2015, social media fall into the latter category and remain a forum for free speech only in so far as that speech meets with corporate guidelines.

New Concerns and the Bill of Rights

In the 2014 book *So You've Been Publicly Shamed* author Jon Ronson discusses a new rights issue that has emerged from the sharing and transmission of digital data: the phenomenon of digital public humiliation. The concept is simple: an individual digitally stores or more often shares a photo, video, or text that portrays the original poster in an unfavorable light, and the content inadvertently becomes public. In the many examples shared by Ronson are examples in which inappropriate or distasteful photos or jokes have led to individuals being fired from their jobs, publically insulted through social media, and turned into media pariahs.[10]

Incidents like this raise a new question, should Internet users have a "right to be forgotten," meaning the right to have information about themselves removed from the Internet. The right to be forgotten is an important part of the evolving concept of digital ethics. The European Union has passed laws giving individuals the right to request that information about them be removed from Internet search engines in cases where the information is "abusive, excessive, or inaccurate" for data processing.[11] As of 2015, the United States had not adopted similar legislation, but privacy

advocacy groups are currently lobbying for a similar United States law to protect digital privacy.

In his book, Ronson quotes digital privacy expert Michael Fertik as saying, "The biggest lie, is *The Internet is about you*."[12] Ferkit argues that, despite the claims of Internet service companies, the Internet isn't about expression and creativity, but rather it is a landscape generated by companies in the process of selling products and content. Public shaming is good for Internet providers, driving traffic to websites and advertisers. Digital privacy, censorship, and new issues like public shaming are all essentially rooted in the same issue: that the digital sphere of human activity is, as it currently exists, a public space that creates the illusion of a private venue for expression. One might know, logically and rationally, that Twitter posts are potentially transferrable to the Internet at large, but few imagine that their Tweets will reach beyond their select group of followers.

Tim Berners-Lee, often considered the person who most directly "invented" the Internet, has argued in the media for the adoption of a "Digital Bill of Rights" that would explicitly guarantee the rights of users and place limitations on the corporate and governmental rights of organizations that want to manipulate, intercept, and use digital data.[13] Until such a measure is passed and reliably enforced, Internet users in the United States must accept that the Internet belongs to the companies that facilitate it, and to the extent that digital expression belongs to the people, it belongs to all people and therefore to no one in particular.

Micah L. Issit

Notes

1. "Data Policy," *Facebook*, Jan 30, 2015.
2. "About the Foreign Intelligence Surveillance Court."
3. Gellman, "NSA Collects Millions of E-mail Address Books Globally."
4. Risen and Poitras, "N.S.A. Collecting Millions of Faces from Web Images."
5. Linder, "The Right to Privacy."
6. Savage, "Judge Questions Legality of N.S.A. Phone Records."
7. "Riley v. California," 2.
8. Bercovici, "YouTube's Policies Are Clear."
9. Ball, "Twitter: From Free Speech Champion to Selective Censor?"
10. Ronson, *So You've Been Publically Shamed*, 70-74, 206-214.
11. "Factsheet on the 'Right to be Forgotten' Ruling."
12. Ronson, 276.
13. Finley, "Inventor of the Web is Right: We Need an Internet Bill of Rights."