Winter 7-21-2023

Personal Protection of Privacy in the Information Age

Rashidat Taiwo ADELEKE University Library,
Fountain University, Osogbo. Osun State., adeleker1980@gmail.com

Jesubukade Emmanuel Ajakaye
Federal Polytechnic Ayede, ajakaye.bukade@gmail.com

Personal Protection of Privacy in the Information Age

BY

ADELEKE, RASHIDAT TAIWO

Abstract

The Information Age has revolutionized society through the use of computers and digital technology, enabling improved communication, increased productivity, and versatile working. However, this period has also resulted in excessive data collection and surveillance, threatening individual privacy, freedom of expression, and civic engagement. Despite data privacy laws, the increasing use of automated technologies by both government and private entities has made it difficult to safeguard individual rights. In the digital age, personal privacy is becoming increasingly difficult to protect, with the omnipresent danger of personal data being stolen or sold. To address this, various processes have been suggested, including using a Virtual Private Network (VPN), encrypting emails, being cautious with links and attachments, looking for privacy indicators on websites, using anti-malware and anti-virus protection, and following the principle of least privilege. Libraries play a crucial role in promoting and protecting individual privacy by empowering individuals, developing procedures to protect patron privacy, advocating for privacy in the public sphere, and educating users about the importance of digital privacy. By implementing these steps, individuals and organizations can protect their personal information and prevent hackers from accessing sensitive data. As we continue to navigate the Information Age, protecting privacy and promoting digital literacy will be critical in ensuring a safe and equitable future.

Keywords: Information age, Personal Protection, Privacy

Introduction

Information is the means through which the minds expand and increases its capacity to achieve its goals, often as the result of input from another mind. Thus, information forms the intellectual capital from which human beings craft their lives and secure dignity. According to (DeCew 1997) informational *privacy* is concerned with the interest of individuals in exercising control over access to information about themselves. Informational privacy in a normative sense refers typically to a non-absolute moral right of persons to have direct or indirect control over access to: Information about oneself; Situations in which others could acquire information about oneself; Technology that can be used to generate, process or disseminate information about oneself. Human beings value their privacy and the protection of their personal sphere of life. They value some control over who knows what about them. They certainly do not want their personal information to be accessible to just anyone at any time. But recent advances in information technology threaten privacy and have reduced the amount of control over personal data and opened up the possibility of a range of negative consequences as a result of access to personal data.

Information Age

The information age also commonly known as the *Computer Age* or *Digital Age*, is a period in human history characterized by a departure from traditional industry to an economy based on the manipulation of information, i.e., an information society. This period started in the 1970s with the introduction of the personal computer with subsequent technology introduced providing the ability to transfer information freely and quickly (Manue, 1996). The onset of the Information Age is associated with the Digital Revolution, just as the Industrial Revolution marked the onset of the Industrial Age. During the information age, the phenomenon is that the digital industry creates a knowledge-based society surrounded by a high-tech global economy that spans its influence on how the manufacturing throughput and the service sector operate in an efficient and convenient way (Mathias, 1998). In a commercialized society, the information industry is able to allow individuals to explore their personalized needs, therefore simplifying the procedure of making decisions for transactions and significantly lowering costs for both the producers and buyers.

The Information Age formed by capitalizing on the computer micro miniaturization advances, with a transition spanning from the advent of the personal computer in the late 1970s, to the Internet's reaching a critical mass in the early 1990s, and the adoption of such technology by the public in the two decades after 1990. Bringing about a fast evolution of technology in daily life, as well as in educational lifestyle, the Information Age has allowed rapid global communications and networking to shape modern society (Mathias, 1998; Hibert, 2015). Most agree that the period of the information age is generally said to have begun in the latter half of the 20th century and continues through the present; although the precise date varies, because of the difficulty in pinpointing the specific dates for the global and public use of personal computers, Internet, e-mail, cell phones, personal communications devices, and social networking sites. Therefore, many dates for the important contributing factors to the spread of information within the common man's routine implementation are approximate and widely recognized as such.

The Information Age was embraced and accepted by the masses since the late 1980s and into the 21st century, although the intellectual concepts and original inventions were developed somewhat earlier in the 20th century. Another important matter that arose from the emergence of the Information Age was the overarching need to define the construct of information. Just what is information? And how does it apply to this context? Raw data is not information. Data is not information until it is collected, saved, stored, organized, transmitted, received, and understood. Data certainly must have meaning, hopefully, the same meaning to both the sender and the receiver (Downing, 2016).

Characteristics of the information age

- It is characterized by the departure from the traditional age to an economy based on the manipulation of information
- It brings about a fast evolution of technology in daily life, as well as in educational lifestyle
- Information Age allows rapid global communications and networking to shape modern society
- It enables decentralization among workers. Workers need to be close to the workplace, work can now be done wherever they may be. An example is the freelancer workers
- The emergence of the information age brings about a more comfortable living.

Advantages of Information Age in the Society

Digital technology has transformed modern life, bringing with it many advantages. We carry more computing and storage power in our mobile phones than was used to launch and land the first lunar module. Digital technology has transformed nearly every aspect of modern life. Travel, work, shopping, entertainment, and communications are just some of the areas that have been revolutionized in recent decades. It's now rare to find an electronic device or piece of machinery that doesn't incorporate digital technology in some way. The evolution of technology is beneficial to humans for several reasons, some of which are explained below.

Communication: The invention of the computer was a very important point. Communication is thus enhanced, and companies can communicate more easily with foreign countries. Research is also simplified. Digital technology makes it easy to stay in touch with friends, family, and work remotely, even if you are in another part of the world. You can communicate by words, video, audio, and exchange other media. Websites, apps, and software have all been created to help users to socialize. With social media, messaging, texting, laptops, tablets, and mobile phones, nobody needs to feel isolated in the digital world. News and local events update users regularly. Internet speeds have increased exponentially since the early days of dial-up. Ever faster broadband enables the transfer of large amounts of information across the web almost instantaneously, making it possible to stream video and audio in real-time, send large data files, and access data from virtually anywhere in the world. Traditional media generally takes much longer.

Productivity: In the modern industrial world, machines carry out most of the agricultural and industrial work and as a result, workers produce much more goods than a century ago and work less. They have more time to exercise and work in safer environments. For companies, progress is saving time and therefore money. Exchanges are faster especially with the Internet. Sales and purchases are now facilitated and possible worldwide. This allows businesses to buy raw materials with discounts or at reduced prices. Similarly, global tourism has grown. Technology has also increased the productivity of almost every industry in the world (Nick Ismail, 2017).

Versatile working: The nature of work has been transformed by digital technology. Increased connectivity options mean that many people now have far more opportunities for working from

home, as remote working becomes increasingly common. Many jobs can now be done from hundreds, or even thousands of miles away without difficulty. Without the need for all workers to be present in the same building, many other flexible working practices are now possible (John Goodman, 2019)

Learning Opportunities: Anybody with access to the internet now has access to a huge proportion of the world's knowledge over the web. Lessons and courses can now be delivered virtually online. Communication advances mean that you can now easily communicate with most of the world's population and learn directly from sources, for example if you are trying to understand foreign events, or learning a new language. Digital technology can also be easier to use for people with disabilities and often give them equal access.

Information storage: Technology improves daily lives; allowing moving physical storage units to virtual storage banks and more. Digital technology enables the storage of massive amounts of information in relatively small spaces. Large amounts of media, such as photos, music, videos, contact information, and other documents can be carried around on small devices like mobile phones. As well as physical locations, data can also be stored online, enabling it to be safe and accessed from any device which has internet access

Banking and Finance: There's no doubt that digitalization has led to a revolution in financial matters. Online banking done either through a laptop, tablet, or phone app is now the norm. Bank users can now check their incoming and outgoing payments remotely, as well as arrange money transfers and bill payments. Outside of banking, other financial matters, such as buying and selling currency and shares can be dealt with online. Transferring money between accounts both nationally and internationally has also seen a great deal of innovation in recent years. Thanks to technology, we can even pay with bitcoins instead of using banks. The digital coin has been such a game-changing factor, that many realised that this is the right time to open a Bitcoin demo account.

Issues in the information age

The building of intellectual capital is vulnerable in many ways. For example, people's intellectual capital is impaired whenever they lose their personal information without being compensated for it when they are precluded access to information which is of value to them, when they have

revealed information, they hold intimate, or when they find out that the information upon which their living depends is in error. The social contract among people in the information age must deal with these threats to human dignity. Hence, this brings about various issues in the information age. The ethical and social issues involved are many and varied. However, it is helpful to focus on just four. These may be summarized into:

Privacy: According to Yusuf, Folorunso, and Akinwale (2011), the rapid increase in computing and communications power has raised considerable concern about privacy both in the public and private sectors. Decreases in the cost of data storage and information processing make it likely that it will become practicable for both government and private data-mining enterprises to collect detailed dossiers on all citizens. Nobody knows who currently collects data about individuals, how this data is used and shared or how this data might be misused. These concerns lower the consumers' trust in online institutions and communication and, thus, inhibit the development of electronic commerce. What information about one's self or one's associations must a person reveal to others, under what conditions and with what safeguards? What things can people keep to themselves and not be forced to reveal to others? A technological approach to protecting privacy might be by cryptography although it might be claimed that cryptography presents a serious barrier to criminal investigations.

Accuracy: It is popular wisdom that people today suffer from information overload. A lot of the information available on the Internet is incomplete and even incorrect. People spend more and more of their time absorbing irrelevant information just because it is available and they think they should know about it. Therefore, how people assign credibility to the information they collect in order to invent and develop new credibility systems to help consumers, to manage the information overload must be studied. Who is responsible for the authenticity, fidelity and accuracy of information? Similarly, who is to be held accountable for errors in information and how is the injured party to be made whole?

Property: Increasing representation of a wide variety of content in digital form results in easier and cheaper duplication and distribution of information. This has a mixed effect on the provision of content. Content can be distributed at a lower unit cost, and distribution of content outside of channels that respect intellectual property rights can reduce the incentives of creators and distributors to produce and make content available in the first place. Information technology raises a host of questions about intellectual property protection, who owns information? What are

the just and fair prices for its exchange? Who owns the channels, especially the airways, through which information is transmitted? How should access to this scarce resource be allocated? New tools and regulations have to be developed in order to solve this problem.

Accessibility: This has to do with what information a person or an organization has a right or a privilege to obtain, under what conditions and with what safeguards.

Individual Privacy and Privacy Protection

Individual privacy

Individual privacy is the right of the individual to decide with whom and when to share information regarding his/her own life and thoughts and feeling he/she has. You may also have, by extension of the previous concept, couple privacy, family privacy, corporate privacy and so on and so forth. Individual privacy is the ability of an individual to seclude themselves or information about themselves and thereby express themselves selectively. One's personal information is more than name, address, and phone number. It also includes your shopping habits, work history, credit score etc. Having control over this personal information is referred to as the *right to privacy*. It is the ability to limit who has this information, how this information is kept and what can be done with it.

Unfortunately, an individual's privacy is lost, unknowingly forfeited, purchased or stolen every day, through the daily activities that we perform such as paying the mortgage, surfing the internet, performing online transactions, registrations etc. A lot of personal information of people is compromised through data breaches and online information brokers are also readily available to package and sell the information to anyone interested. People as a result become victims of identity theft, credit theft, job loss and so on, hence the need to protect individuals' privacy in today's information age is a crucial matter which needs urgent attention.

Privacy in the Information Age

Privacy is the "right to be free from unwarranted intrusion and to keep certain matters from public view" (Law 2015; IFLA, 2018). As such, "privacy is an important element in the autonomy of the individual. Much of what makes us human comes from our interactions with others within a private sphere where we assume no one is observing. A private space enhances autonomy. If we feel we may not be completely autonomous in our thoughts and actions, we may

hold back crucial elements of ourselves. Privacy, therefore, "protects our subjectivity from the pervasive efforts of commercial and government actors to render individuals and communities fixed, transparent and predictable. Privacy is an indispensable feature of a democracy where an individual maintains his identity while contributing to their civic duty" (Cohen 2016).

As set out in IFLA's own Statement on Privacy in the Library Environment, 'excessive data collection and use threatens individual users' privacy and has other social and legal consequences. When Internet users are aware of large-scale data collection and surveillance, they may self-censor their behaviour due to the fear of unexpected consequences. Excessive data collection can then have a chilling effect on society, narrowing an individual's right to freedom of speech and freedom of expression because of this perceived threat. Limiting freedom of speech and expression has the potential to compromise democracy and greatly limit civil engagement by making us "predictable" in our actions and thoughts (Cohen, 2016).

Surveillance and communications interception the right to privacy in the digital age is threatened aggressively by data automation. In 1985 Spiros Simitis, Germany's leading privacy scholar recognized the risks data automation would cause to privacy, individuals and the democratic process. 'Privacy is not an end in itself, Simitis suggested, but an important tool to achieve a self-critical democracy where citizens are not unwitting suppliers of information to an all-seeing, and all-optimizing technocrats" (Morozov 2013). If privacy is at risk or threatened, we might miss the chance for a personal assessment of the political process, one based on critical evaluation and self-reflection of our choices and preferences. Data collection, through hacking or simple data harvesting, allows governments and commercial entities to amass huge banks of information about common citizens and their online behaviour (IFLA, 2018)

Privacy incursions occur frequently, affecting our search and digital behaviour patterns. These incursions are not only about a person or in this case a user – they can also affect a group, a family, or a community. Automated data gathering is carried out by government and private actors. Government surveillance includes communications interception, bulk data collection and 2 processing, targeted intrusions in ICT systems and issues relating to cross-border surveillance and access to personal data. As one of the many examples of governmental privacy infringement, the Pegasus software allowed the Mexican Government to spy on human rights defenders, journalists and anti-corruption activists. In this specific case of government-sponsored

cyberattacks, the WhatsApp feed of the son of a prominent lawyer and civil rights journalist was the target of intrusion and privacy infringement (New York Times 2017; IFLA, 2018).

Businesses can also contribute to surveillance activities based on data automation and collection and so encroach on our privacy. The latest scandal involves Facebook users and Cambridge Analytica researchers mishandling the data of over 40 million users. The dubious data gathering tactic included the use of Facebook Graphs API (application program interface) "that makes possible all the interconnectivity and the data delivery Facebook boasts when claiming that the platform was building a web where the default option is sharing" (Albright 2018). What is worrisome is that FB claims that its interface is based on the presence that users are in control of what is shared. In actuality, Facebook users have next to no control over what is covertly shared about them – meaning the information and metadata others can extract.

Whether the threat comes from governments or private entities, these occurrences pose a significant question as to the right to live without arbitrary attacks on privacy (Article 12 of the Universal Declaration on Human Rights) and how our right to safeguard privacy can be defended. Laws Are Not Enough While data protection legislation has the potential to cut back on speculative data collection by companies, data privacy laws are not well placed to protect individuals' rights vis-a-vis automated technologies and privacy can all too often be undermined by laws elsewhere. Currently, as a response to terrorist attacks in Europe, increased surveillance powers have been implemented at the national level, with much data shared across borders. Security has too often been cited as a reason for limiting the use of encryption technologies, or for creating 'back-doors', which are likely to facilitate incursions on privacy by both government and other actors. There are already voices against blanket surveillance (IFLA, 2018).

Roles of the library in promoting and protecting individual privacy

Librarians agree that data privacy is a vital part of broader digital literacy – the ability to get the best out of the opportunities that digital technologies offer. As reviewed by The International Federation of Library Association and Institutions (IFLA, 2018), Libraries can play a powerful role in the promotion and protection of privacy given their long experience in working with information and helping users. Some of these roles are discussed.

Empowering individuals: Teaching the meaning of digital privacy undoubtedly enhances security practices. When there is a deep, systemic problem such as the current attacks to our

privacy, the solution does not come from ad hoc deletion of problematic software or applications, but it comes from education, digital literacy, global cooperation and tirelessly advocating on best practices (IFLA, 2018)

Privacy in the library environment: Libraries can develop procedures to protect user privacy. The International Federation of Library Association and Institutions (IFLA) statement on Privacy in the Library Environment (2015), emphasized the role of library crypto parties. They have taken place in the UK, France, the Netherlands, Australia, Sweden, the US, Canada, and Germany, to name just a few. These explore everything from specific tools, such as ToR browsers or anti-tracking software, to simpler behavioural changes which can reduce or manage risks. While much of the discourse around crypto parties focus on government surveillance, good data hygiene is just as applicable in dealing with unwanted attention from businesses, hackers, or even members of personal networks.

Limiting personal data collection: Libraries can push partners (commercial or otherwise) to limit personal data collection. In addition, to minimize the number of data libraries' computers collect, libraries also promote best practices by determining what user data they collect to limit information held about their users.

Enhance security practices: Many libraries instituted a set of practices where "Web browsers have temporary Internet files set to 2 MB, history retention set to 0 days, form-filling memory turned off, password memory turned off, and downloads turned off. In some libraries, all computers have special products installed to restore them to a standard template when rebooted. Computers will be set up to reboot after a set time of inactivity. This will clear any individual who forgot to log off and delete his activities from the computer" (Coombs 2005).

Importance of individual privacy protection

The following types are moral reasons for the protection of personal data and for providing direct or indirect control over access to those data by others can be distinguished (van den Hoven 2008). These formulations all provide good moral reasons for limiting and constraining access to personal data and providing individuals with control over their data.

Prevention of harm: Unrestricted access by others to one's passwords, characteristics, and whereabouts can be used to harm the data subject in a variety of ways.

Informational inequality: Personal data have become commodities. Individuals are usually not in a good position to negotiate contracts about the use of their data and do not have the means to

check whether partners live up to the terms of the contract. Data protection laws, regulation and governance aim at establishing fair conditions for drafting contracts about personal data transmission and exchange and providing data subjects with checks and balances, guarantees for redress.

Informational injustice and discrimination: Personal information provided in one sphere or context (for example, health care) may change its meaning when used in another sphere or context (such as commercial transactions) and may lead to discrimination and disadvantages for the individual.

Encroachment on moral autonomy: Lack of privacy may expose individuals to outside forces that influence their choices.

Protecting Individuals' Privacy in the Information Age

It's become much harder to have personal privacy in the digital world and that's on top of the dangers of your personal data being stolen or sold. For instance, everybody has the ability to take photos and video footage on their mobile phone, and then post it online. Employers can search for people online and maybe find unflattering photographs, or see those expressing controversial opinions on social media or blogs. Digital cameras watch and record our movements in public places. Minor indiscretions can now haunt an individual for life when they're posted on the internet. Controlling your personal information is very difficult and sometimes impossible. The privacy of individuals and organizations can be protected in the information age through the processes enumerated by Bill (2018).

Use a VPN: A virtual private network (VPN) is the most secure way to protect your privacy in the digital age. Think of it as a tunnel between your device and the internet. This tunnel is shrouded in armour like SSL security and other privacy protection features so that no one can track your online activities. "VPNs are a way for users to win back some control," explains a *Mashable* article. "Remember: All of your information and activity is known to your ISP because of your IP address. By changing your IP address, you can sidestep your ISP and mask your internet activity. A VPN lets you do that by routing your activity through its own servers." VPN services are available for anyone, not just those in the commercial sector. Find a great individual VPN to meet your daily browsing needs, and enjoy unlimited security.

Encrypt your email: Email encryption is most often used by businesses that often transmit sensitive information; however, an increasing number of individuals are using it to protect their privacy. When encryption is enabled, it scrambles the information for anyone except the authorized sender and recipient, so even if a hacker accessed your data, they couldn't read it.

Email encryption can be integrated into your existing email address affordably and is best used when you're sending highly sensitive information like credit cards or social security numbers.

Be careful with links and attachments in emails: Phishing is one of the more common attempts to access an individual's private information. Fraudsters send emails posing as reputable companies or even people you know to steal personal information. They often use malware, ransomware, and other viruses for the same purpose. Whenever you receive an email, even from someone you recognize, be careful when clicking on links or downloading attachments. If something seems fishy about the email, simply delete it without clicking further.

Look for privacy indicators on websites: Whenever you're asked to input sensitive information, such as phone numbers, addresses, or credit card information, check for indicators that the website is secure. If it's not, you might as well hand your information to a hacker with a bright red bow on it. Northeastern University in Boston recommends double-checking that the web address starts with "https://" first. "Look for a closed padlock in your web browser," the site also warns. "When you click on the padlock you should see a message that states the name of the company and that 'the connection to the server is encrypted."

Use anti-malware and anti-virus protection: Hackers often use malware, malicious software that enables them to steal or delete information from your computer, often damaging the device in the process. Viruses may do the same thing. Never operate an internet-enabled computer without installing anti-malware and anti-virus software. It's free or affordable for your computer. To secure mobile devices, use apps designed for the same purpose.

Use strong passwords and change them often: The average internet user fails in the department of strong passwords that can protect your privacy. According to research, 86 per cent of internet account passwords are considered to be "terrible," because they're easy to guess. The most common passwords include a variation of 1234567, qwerty, password, abc123, and repeated numbers. A strong password is your best protection against brute-force hacking attempts. Every time you add a complex component, such as a special character or capital letter, it adds another layer of protection to your online accounts. Additionally, change your passwords

often. Many organizations require that their employees change their passwords monthly to avoid unauthorized access to sensitive information. Although a monthly password change may not be necessary for your personal information, consider a change at least once per year.

Automate software updates: Contrary to popular belief, software developers don't wait until they have a perfect product before releasing it to consumers. Rather, they get it as close as they can with the intention of continually working on plugging privacy and security holes and fixing glitches after it's been launched. They present these fixes in the form of patches and updates. This makes updating your software regularly imperative to protecting your information and accounts. Using automatic updating is something you won't even have to think about. "Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option," suggests an article from a cyber security organization.

Follow the principle of least privilege (POLP): In other words, limit the number of people who have access to your accounts. Too many administrators increase your risk for human error and leave your devices vulnerable to hackers monitoring the web for such an opportunity. "Do not log into a computer with administrator rights unless you must do so to perform specific tasks," Indiana University researchers wrote in a Twitter post. "Running your computer as an administrator (or as a Power User in Windows) leaves your computer vulnerable to security risks and exploits…When you do need to perform tasks as an administrator, always follow security procedures."

Beware of public Wi-Fi: Public Wi-Fi is convenient, but it's a huge privacy challenge. About 60 percent of people report using public Wi-Fi on a regular basis, whether they're connecting to a hotel network or a coffee shop. Hacking on public Wi-Fi is super easy. Anyone can learn to do it by watching YouTube videos, many of which have millions of views. They might try a "man in the middle" or "evil twin" attack to access information as it travels from your device to the server. Be very careful when connecting to public Wi-Fi unless you have a VPN. A VPN will protect you from amateur hackers, so you can use free Wi-Fi without security risks.

Turn off location data: Every device has location data that can pinpoint your location. Although the idea is hard to stomach, governments, organizations, or hackers may be watching, and you can prevent their inquiries at a basic level by turning off location services on any device that connects with the internet.

Conclusion

Information technology is typically seen as the *cause* of privacy problems, there are also several ways in which information technology can help to solve these problems. There are rules, guidelines or best practices that can be used for designing privacy-preserving systems. Such possibilities range from ethically-informed design methodologies to using encryption to protect personal information from unauthorized use. Finally, it is appropriate to note that not all social effects of information technology concern privacy. Examples include the effects of social network sites on friendship, and the verifiability of results of electronic elections. Therefore, value-sensitive design approaches and impact assessments of information technology should not focus on privacy only, since information technology affects many other values as well. The digital age is constantly evolving, and hacker attempts are growing more complex. Only those who take security threats seriously and work to prevent them will survive with all their personal information intact.

Reference

Akinwale, L.A., Folorunsho, O., Akinwale A. T (2011). Computer in information. *International Journal of Research and reviews in computer science* ***2*** (2):1 – 6

Albright, J. (2018). The graph API: key points in the Facebook and Cambridge Analytical Debacle. Retrieved 4 April 2019 from https://medium.com/tow-centre/the-graph-api-key-points-in-the-facebook-and-cambridge-analytica-debacle-b69fe692d747

Bill, G (2018). Protection of privacy in information age. Retrieved 2 April 2019 from https://www.business2community.com/cybersecurity/10-ways-to-keep-your-informaton-safe-in-the-digital-age-02130163

Cohen, J. E. (2013). What is privacy for? *Harvard law review 126.* Retrieved 2 April 2019 from IFLA_2016_right_to_privacy_and_freedom_of_expression_in_public_libraries.pdf

Collins Dictionary (2019). Accessed 2 April 2019 on https://www.collinsdictionary.com/dictionary/english/information-age.

Coombs, K. A. (2005). Protecting USER PRIVACY in the Age of DIGITAL LIBRARIES. *Computers in libraries* **25** (6): 16 – 20.

Downing, C. E (2016). Privacy and the information age: A longitudinal view. *Journal of International Technology and Information Management* **25** (2): 33 – 46

Fundamental rights report (2017). Accessed 7 April, 2019 on http://fra.europa.cu/en/publications-and-resources/publications/annualreports/fundametal rights-2017//data-protection

Hilbert, M. (2015). Digital technology and social change [open online course at the University of California]. Retrieved on 7 April 2019 from https://canvas.instructure.com/courses/949415

IFLA (2018). The right to privacy in the digital age. Retrieved 2 April 2019 from https://www.ifla.org/files/assets/faife/ochr_privacy_ifla.pdf

Jeroen van den Hoven, Martijn Blaauw, Wolter Pieters, Martijn Warnier (2014). Privacy and Information Technology. *Stanford Encyclopedia of Philosophy*. Retrieved 22 April, 2019 from https://Privacy-and-Information-Technology (Stanford Encyclopedia of Philosophy).htm

Kapadia, R., Stanley, G., and Walker, M. (2006). "Real World Model-based Fault Management", Proceedings of the 18th International Workshop on the Principles of Diagnosis (DX 07), Nashville, TN.

Keith Goldstein, Ohad Shem Tov, Dan Prazeres (2018). The right to privacy in the digital age. Presented on behalf of Pirate Parties international headquarters a UNECOSOC Consultative member, for the report of the high commissioner for human rights

Manuel, C., (1996). The information age: economy, society and culture. Oxford Blackwell. ISBN 078-0631215943. OCLC 43092627

Mathias, H. (1998). ''Technology and Workforce: Comparison between the information revolution and the Industrial Revolution"

Moore, R., Rosenof, H., and Stanley, G. (1990). Process control using a real time expert system. *Proc. International Federation of Automatic Control (IFAC), Estonia, USSR*, 1-6

Morozov, E., (2013). The Real Privacy Problem. MIT *Technology Review*.

Newell, A., Simon, H. A. (1976). Computer science as empirical inquiry: symbols and search. *Comm. Of the ACM, 19*, 113 – 126

Poerch, M. J (2015). A new paradigm for learning language. *Connectionist artificial intelligence, Linguagem & Ensino,* **8** (1), 161-183