Journal of Entrepreneurship and Business Venturing
Vol 3, Issue 1, 2023, PP. 119-146

E-Commerce and Social Media Policies in the Digital Age: Legal Analysis and Recommendations for Management

Bahaudin G. Mujtaba
College of Business and Entrepreneurship, Nova Southeastern University, Florida, USA.
Frank J. Cavico
College of Business and Entrepreneurship, Nova Southeastern University, Florida, USA
cavico@nova.edu.

Corresponding: mujtaba@nova.edu

ARTICLE INFO

Article History:
Received: 11 Jan, 2023
Revised: 10 Feb, 2023
Accepted: 22 Feb, 2023
Available Online: 27 Feb, 2023

DOI:

https://doi.org/10.56536/jebv.v3i1.37

Keywords:
E-commerce, Internet,
privacy rights, workplace privacy,
data security.

JEL Classification:
L81

ABSTRACT

Technological developments, innovations, and e-commerce complexities have made it a requirement for human resources professionals in today's digital workplace to become aware of modern laws regulating their workplace data handing procedures, while also making sure the entire organization is compliant. This paper provides a historical review of e-commerce laws, challenges, and how these are impacting the modern workplace's privacy issues related to employees and consumers. Next, the paper explores the concept of sectoral policies in the United States. Finally, the paper examines and assesses the necessity of regulations currently in place as well as future legal needs. The conclusion is that as the internet matures and private sector procedures become standardized, there will be a need for more regulations for each sector of industry to protect the privacy of employees, along with the confidentiality of consumers' data. Sound regulations will create clarity, certainty, and consistency in expectations and procedures, thereby reducing employee stress and voluntary turnover as well as avoiding legal problems.

INTRODUCTION

The widespread existence and fast growth of e-commerce and digital technologies have transformed the modern workplace and society in most developed economies where consumers now have regular access to the internet. Since we are all now experiencing the growth and development stages of the internet and e-commerce, sound legal and practical policies and norms are continuously being created, adapted, and revised as necessary. The impacts of electronic information exchange are very hard to control as private information and even misinformation can leak out. The transmission of valuable information has caused worry and even anxiety for e-commerce stakeholders. Of course, the dynamic is based on the substance of the message. On the off chance that the message does not have any believable and legitimate information, it is viewed as of no value and worth (Jamshed, 2022, p. 63). People are worried

that their private data may not be kept in a confidential manner as firms continue to use them for marketing and product promotion purposes; therefore, legal interventions are necessary

One recent headline example is the article entitled, "*FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations,"* where the agency charges that the firm's geolocation information from millions of mobile devices can be used to personally identify specific individuals and trace their movements (FTC, August 29, 2022). Apparently, the Federal Trade Commission (FTC) is suing data broker Kochava Inc. for "selling geolocation data from hundreds of millions of mobile devices that can be used to trace the movements of individuals to and from sensitive locations" (para. 1) that should remain confidential. The public exposure of such personal information could endanger a person or groups of people if they went to the reproductive health clinics, religious organizations such as temples and mosques, violence shelters, and even to addiction or healing services. Given the unfortunate political rhetoric in society, such personal information can have a disparate impact on some individuals as it can lead to the stigmatization, annoyance, discrimination, job termination, and even bodily harm of innocent individuals in the community (Muffler, Cavico, and Mujtaba, 2010). The FTC lawsuit is attempting to stop companies from selling any sensitive geolocation data and they must be required to immediately and properly delete any such vulnerable information they might have already collected. Of course, the goal of FTC has always been to protect sensitive consumer data, including geolocation and health information of all citizens, from being misused by falling in the hands of criminals (Mujtaba, 2023).

Sound regulation is necessary to encourage data protection, inclusion, and network neutrality in these times of digital diversity. One may always wonder whether the regulations should come from consumers, businesses, or governments? Since government agencies are not in the e-commerce business and they are not out to make a profit, and thus they are the best sources for the final review and approval of fair policies to protect all parties. Also, since businesses have the goal of maximizing profitability, they should not be the sole source for policies since unchecked ambition and greed can drive some unethical businesses toward monopolizing the industry to benefit their stockholders (Mujtaba, 2003). Another efficacious source of the regulations might be to allow consumers to initiate sound policies by verbalizing their demands through their "pocketbooks," which forces businesses to "keep their fingers on the pulse" of their clients and customers, while offering them exactly what they need accompanied by good quality and service. In this manner, businesses will be influenced and impacted by the demands of their customers and accordingly the "market," and thereby sound policies will be created that are accepted by all stakeholders. Finally, these policies and norms should be finalized into laws through the public sector's professional servants and enforced by relevant government

branches, while always aiming for net neutrality. All advanced countries are having to experiment with relevant policies to protect data and privacy of their citizens. It is said that,

> The massive and implausible advancements in the fields of information and communications technology, and especially the internet, have increased both the value and threats to the information privacy of individuals. The Malaysian Personal Data Protection Act 2010 (PDPA) was a governmental endeavor to protect the information privacy of the citizens. However, the Act's output and the level of compliance by the data users are in a halo of ambiguity (Alibeigi, Munir and Asemi, 2022, p. 119).

Grimmelmann (2019) explains that "network neutrality" rules require internet service providers (ISPs) not to discriminate against legal uses of their networks. In other words, Internet speeds should not be slowed down indiscriminately since everyone has the right to equal access to the modern digital diversity that exists in the online world (Ohlhausen, 2013). Some people use the term "Internet freedom" to describe "net neutrality." The debates over network neutrality are based on the beliefs of access, competition, and innovation on the Internet. The first belief, *access,* emphasizes digital diversity in that as many people as possible should be able to connect and use the internet to communicate and do business with each other. The second belief, *competition,* rationalizes that the Internet is better because different individuals, teams and companies compete to offer enhanced service, which ultimately benefits consumers. The third belief of *innovation* is based on the premise that investments in technological improvements to the Internet can benefit people and society toward efficiency, environmental responsibility, sustainability, and thus less pollution and reduced climate change. It is a reality that sometimes these beliefs and values can reinforce each other; but at other times they conflict (Grimmelmann, 2019, p. 582). All these philosophical beliefs and privacy concerns merit awareness, reflection, as well as integration into discussions regarding regulations impacting e-commerce along with the quality engagement of employees in the organization (Phomkamin, Pumpuang, Potijak, Sangngam, Ketprasit, and Mujtaba, 2021). As mentioned by Ohlhausen (2013, p. 81): "Some content providers want the government to adopt regulations to guarantee them fair access to the Internet", however "some network owners, like Verizon or Comcast, disagree and think such regulations are unnecessary and could stifle innovation on the Internet." Of course, such debates will continue to take place among consumers, businesses, and government officials because these are the times of transformational change that will determine how we access and use the Internet over the coming years, decades, and century.

In the next section, e-commerce literature is provided; and it is highlighted that e-commerce and the Internet have reduced public and personal privacy, since more and more people are online more often. Researchers continue to emphasize that unprotected technology is impacting privacy concerns of employees and consumers in a deleterious manner. Next, the paper will

explore the concept of sectoral policies which are traditionally practiced in the United States of America. Finally, the paper will examine some of the regulations currently in place as well as point out future regulatory needs.

THE DEMOLITION OF PRIVACY

Technology and the widespread use of the internet through social media platforms have reduced privacy as every transaction provides an opportunity for personal data to be stored on "cookies" or leaked to unethical users or criminals. In the modern society, we see that hackers and law enforcement officials alike can easily access anyone's computer, phone contacts, text messages, and call-history from mobile devices without the person's permission and without notice. While there are conveniences associated with technology, there certainly are negatives as well. Even now a very young, five-year child can easily get into modern smartphones, make calls, go online, and purchase products from e-commerce retailers without an adult's permission, since there is so much information already programmed into the mobile devices.

In the United States and many other developed economies, the "right to privacy" is an important and necessary right of every citizen. Over a century ago in their seminal article, authors Samuel Warren and Louis Brandeis (1890) emphasized that privacy is the right "to be left alone," the right to liberty or to enjoy life and to being protected from undue outside interferences or scrutiny. With the widespread availability of trackable technology and consequently the capability of each person's moves being recorded in most public domains, it is clear to see the importance and relevancy of "being left alone" that was envisioned by these authors over 130 years ago.

Through their vision over one-century ago, Warren and Brandeis talked about the intrusion of technology and viewed it as a threat to privacy of individual freedoms afforded to all citizens, consumers, and employees. Of course, today, technology is progressing faster than ever before, thereby spreading information quickly and often instantaneously through social media platforms and organizational communication systems. Regardless of technology, there are certain privacy rights (such as "full protection" in person and in property) that each person should be entitled to in the United States and the rest of the world. For example, "the common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others" (Warren and Brandeis, 1890, p. 202). Warren and Brandeis talked about how over time, there came the "qualified protection of the individual against offensive noises and odors, against dust and smoke, and excessive vibration…." And eventually, "The law of nuisance was developed" (p. 192).

As human beings progress, move forward, take on new initiatives, and invent better or more intrusive technologies, the legal side of protecting people's rights must also keep pace with it simultaneously. As such,

> This development of the law was inevitable. The intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear to men that only a part of the pain, pleasure, and profit of life lay in physical things. Thoughts, emotions, and sensations demanded legal recognition, and the beautiful capacity for growth which characterizes the common law enabled the judges to afford the requisite protection, without the interposition of the legislature (Warren and Brandeis, 1890, p. 194).

What was envisioned by Warren and Brandeis so long ago in this *Harvard Business Review* article is very relevant for the modern workplace because data is being compiled about every move we make in any modern economy. For example, using GPS technology, any parent can now track the location of his/her child simply by looking at one's phone. While the parent can feel some comfort in knowing that the child has arrived at school or home as planned, the same technology can be also used by people with bad intentions and by hackers, perhaps with evil intentions, to track innocent children along with their whereabouts.

When private data are intentionally or unintentionally leaked, the transmission can cause "emotional harm," especially on impressionable young teenagers. On June 29, 2022, PBS News in South Florida discussed mental health and how more young people have been thinking of committing suicide because of conflicting information, lack of sufficient mental help counseling, and the additional challenges associated with Covid-19 isolation over the past three years in the United States of America. Human resources professionals can and should educate employees and warn them about privacy rights and responsibilities and social media risks regarding personal data as well as to educate them on how to protect their own privacy and that of their colleagues' and customers, particularly by not publishing any private information on public forums. Of course, we also need to remind our children of such risks and harms as they are online regularly and much more often than previous generations. It is true that maintaining a low-profile on social media may avoid some of the privacy violations and intrusions, but maintaining a low-profile will not bring a person new knowledge, connections, fame, financial stability, and/or career opportunities through networking. However, the hard truth is that shortcuts can lead to damaging results. As such, we all, younger and older online "surfers," need to balance our activities and proceed cautiously to reduce the negative risks. Eventually, rational legal regulations and sound policies will be developed to eliminate or reduce some of the risks by having reasonable privacy laws. One should recall the old maxim: "It takes time for the law to catch up to technology."

While all firms must be concerned about the data and privacy of their employees, vendors, suppliers, and customers, this awareness is especially true for e-commerce-linked firms since

trust is essential for their existence. As human resource professionals and managers, we must all be concerned about the ubiquitous nature of modern technology, the prevalence of privacy issues and concerns, and the utmost importance of keeping employees' as well as customers' data secure.

E-COMMERCE BEGINNINGS

E-commerce is the norm for most people in this Twenty-First century marketplace. However, it is not a common practice in poorer and developing nations yet. Nonetheless, modifications and shifts are coming in every corner of the globe; and accordingly these "Disparate populations, once separated by distance and time, will experience these changes as part of a global community" (Clinton and Gore, 1997, p. 1). As mentioned by the former President William J. Clinton and Vice President Albert Gore (1997, p. 1), "No single force embodies our electronic transformation more than the evolving medium known as the Internet. The Internet has emerged as an appliance of everyday life, accessible from almost every point on the planet." Any typical online user would agree that the Internet is now regularly used in developed economies, not only to reinvent government and reshape our lives, but also impacting how communities are interacting and communicating with each other. It is true that the Internet is empowering citizens of each locality to accept or reject certain regulations. In a way, the Internet and social media are democratizing diverse societies as people can more easily and instantaneously voice their common disagreements with their political leaders (Imtiaz and Nasim, 2022). As explained by Imtiaz and Nasim, "Companies typically function and flourish in the exchange of knowledge and contact with new and current customers, hoping that brand recognition and brand image are generated, eventually boosting their sales" (2022, p. 34). Through the Internet, both small and large-scale entrepreneurs can capitalize on new business opportunities more easily by accessing highly segmented customers worldwide in just a matter of days, if not hours, through email distribution or website promotions (Phomkamin et al., 2021).

There are certain common themes and principles that will continue to influence policy makers, entrepreneurs, and consumers in the e-commerce business. Initially as e-commerce growth and regulation possibilities were being envisioned by political leaders, the five principles discussed in the document entitled "*The Framework for Global Electronic Commerce*," by the Clinton and Gore Whitehouse (1997) were as follows:

1. The private sector should lead.
2. Governments should avoid undue restrictions on electronic commerce.
3. Where governmental involvement is needed, its aim should be to support and enforce a predictable, minimalist, consistent and simple legal environment for commerce.
4. Governments should recognize the unique qualities of the Internet.
5. Electronic Commerce over the Internet should be facilitated on a global basis.

E-commerce is still a developing industry, and most transactions are handled by the private sector based on the needs, wants, and desires of their consumers. So, the private sector will continue to lead as they know their customers' demands; however, the private sector leaders must act in a socially responsible manner to keep all relevant stakeholders happy instead of being driven by the greed mentality and only focusing on "the dough." Otherwise, the "invisible hands" of the government will have to impose more restrictions. During the Covid-19 pandemic, e-commerce became the norm in most developed economies because it offered safety, flexibility, convenience, speed, and few restrictions (Mujtaba, 2022a). As such, irrelevant public sector restrictions and impositions on e-commerce should be avoided in this steadily growing and developing industry. Government involvement in e-commerce should focus on the creation of certainty, standardization, a fair legal framework in this developing industry, and the consistent enforcement of agreed-upon rules to keep consumer and employee data safe (Cavico and Mujtaba, 2020).

Most experts agree that "The genius and explosive success of the Internet can be attributed in part to its decentralized nature (sector-based laws) and to its tradition of bottom-up governance" (Clinton and Gore, 1997, p. 4). The decentralized framework enables and empowers creative entrepreneurs to capitalize on their innovations, hard work and persistence in meeting specific consumer needs locally, nationally, and globally. As such, the bottom-up form of governance needs to continue in the decades to come. Since the Internet is changing and will continue its amorphous format as it becomes the more common means of commerce around the world in all nations, the international community will have to create certain common regulatory provisions that are good for all. As such, "Regulation should be imposed only as a necessary means to achieve an important goal on which there is a broad consensus…Existing laws and regulations that may hinder electronic commerce should be reviewed and revised or eliminated to reflect the needs of the new electronic age" (Clinton and Gore, 1997, p. 4).

Today, "The Internet is emerging as a global marketplace" (Clinton and Gore, 1997, p. 4). Of course, much development has taken place over the past two decades, yet the e-commerce framework is still at its infancy and, therefore, needs further improvement, consistency, and governance of data security from hackers and the misuse of personal records. As such, this paper's analysis supports Clinton and Gore's statement that "The legal framework supporting commercial transactions on the Internet should be governed by consistent principles across state, national, and international borders that lead to predictable results regardless of the jurisdiction in which a particular buyer or seller resides" (1997, p. 4).

It is true that Internet technologies are having a profound effect on global trade in its various forms and services being offered to businesses and consumers. Nonetheless, "Many businesses and consumers are still wary of conducting extensive business over the Internet because of the

lack of a predictable legal environment governing transactions…This is particularly true for international commercial activity where concerns about enforcement of contracts, liability, intellectual property protection, privacy, security and other matters have caused businesses and consumers to be cautious" (Clinton and Gore, 1997, p. 2). As such, more work needs to be done in the decades to come to develop trust and provide certainty and security for e-commerce businesses and consumers. Since the Internet landscape is still adjusting to what works, what sells, and what keeps customers' confidence high to buy and sell online, we can recommend that the industry leaders, while "keeping their fingers on the pulse" of their customers, must keep developing consistent and reliable e-commerce rules for the global marketplace to benefit all current and prospective online consumers. Government officials must work to enforce these agreed-upon norms and policies to make sure there are no fraudulent activities, such as data hacking, identity theft, or privacy violations, in the workplace or society.

DEPLETION OF TRUST

Research shows that about 85% of consumers believe that modern businesses need to do more and be active in protecting personal data that they collect from customers and online users (IBM, 2018). A survey conducted by IBM Cybersecurity in March 2018 provided evidence that most of the respondents, 78%, believe that a company's ability to keep their data private is 'extremely important'. This should be a wake-up call for all managers and entrepreneurs since only about 20% of respondents 'completely trust' organizations to maintain the privacy of their data (IBM, 2018, para. 4). Companies have a moral and legal responsibility to protect personal data provided by consumers. To make sure firms are protecting data, the government has stepped up by creating agreed-upon common sense laws. As a matter of fact, the Consumer Privacy Bill of Rights, in the United States, "applies to *personal data*, which means any data, including aggregations of data, which is linkable to a specific individual…Personal data may include data that is linked to a specific computer or other device" (Consumer Data Privacy, 2012).

It should be clear to all managers and organizations that consumers must be able to exercise "individual control" over all the personal data companies collect from them and how that data is being used. More specifically, the U.S. government has mandated that,

> Companies should provide consumers appropriate control over the personal data that consumers share with others and over how companies collect, use, or disclose personal data. Companies should enable these choices by providing consumers with easily used and accessible mechanisms that reflect the scale, scope, and sensitivity of the personal data that they collect, use, or disclose, as well as the sensitivity of the uses they make of personal data. Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection,

> use, and disclosure. Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place (Consumer Data Privacy, 2012, p. 47).

Furthermore, besides allowing individual control to consumers over the collection and usage of their personal data, there should also be transparency, respect for context, security, fair access, accuracy, focused collection, and full accountability to enforcement authorities, consumers and clients for alignment and adherence to all the stated legal and ethical principles. Human resource professionals and all managers must be aware of another old maxim: "Once your reputation for integrity is lost, it is very difficult to get it back." Recall the Wells Fargo bank fake account and hacking scandal (Cavico and Mujtaba, 2017).

The Federal Trade Commission provides relevant guidance for all firms on data privacy as they work "for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them" (Children's Online Privacy Protection Rule, 2000, p. 15). FTC's guidelines and recommendations can be used for learning, assessment, and policy development at the organizational levels. The expectation is that organizations must train their managers and workers on how to properly handle personal data while regularly assessing their performance to make sure there are no violations of privacy rights. Furthermore, companies should conduct regular or annual audits to evaluate the performance of their managers and employees regarding the protection of personal data from their consumers. Also, any disclosure of personal data to third parties must guarantee that the beneficiaries "are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise (Consumer Data Privacy, 2012, p. 48).

There are many practical and specific rules provided by the FTC for online privacy protection, including "*How to Comply with Children's Online Privacy Protection Rule*" which is of interest to parents since teenage children often share personal data online. Of course, individuals, companies and government policies must all work together toward the same goal of keeping children safe simultaneously. Since most citizens are not likely to be able to change government policies on their own, then individual control and company responsibility should be emphasized regularly to create awareness and immediate protection for data security. However, each citizen should, and must, exercise his/her right during the election process by voting for those candidates who will represent their collective views at the government level so certain data, especially pertaining to young children can, remain private.

At a minimum, all managers and human resource professionals must know and adhere to the Children's Online Privacy Protection Act, which became effective April 21, 2000, because it applies to the online collection of adolescence's personal and identifiable information if they

are under 13 years of age. In general, everyone must remember that "It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed" by the Federal Trade Commission (Children's Online Privacy Protection Rule, 2000, p. 7). Ultimately, it is the consumers who are in the best position to secure and safeguard their own personal data, while also demanding protection by firms.

Sectoral Laws and Data Security

Data protection is important to all nations, industries, and consumers; yet the Europeans tend to have a slightly different approach to regulating data privacy compared to our system in the United States. The European Union (E.U.) nations have a centralized federal legislation process to protect data privacy, where all decisions are regulated from the top of the court system using one major law, such as the "*Data Protection Directive*." In the U.S., since the Constitution does not provide any specific or explicit right of privacy to people, we thus have a more decentralized process for data protection, where organizations and industries are largely left alone and thereby empowered to take responsibility for protecting data belonging to their employees and consumers. So, in the U.S., we use a decentralized process known as the "sectoral approach" to regulation.

The term "sectoral approach" refers to the combination of various laws, policies, and regulations which are developed to properly deal with a specific, area-by area (or sector-by-sector) need within an industry or to tackle an existing problem unique to each sector. The sectoral approach is used in the U.S. where a law or precedent might become the norm; and then eventually another sector's regulations might also become applicable to a firm since industries change, develop, and even merge at times. However, the European nations tend to use the centralized "omnibus approach," where there is "one overarching law that regulates privacy consistently across all industries" (Solove, 2015, para. 1). One thing that is indisputable is that the EU community certainly has fewer cases to litigate compared to the number of lawsuits, lawyers, and judges currently in the United States.

Solove concludes that the American approach is an outlier from the way most other nations regulate the concept of privacy. In the sectoral approach or system, people can become a bit confused as they see similar regulations being imposed on them from multiple industries with some commonalities. Industries or sectors are not static and might change or even get involved in businesses of other sectors. When a technology firm enters the healthcare profession or the financial industry, they would be regulated by multiple privacy laws which are not always similar. So, a company might have to make sure that their privacy policies are aligned with multiple regulators and different laws such as GLBA, HIPPA, FERPA, and ECPA guidelines as well as specific collective bargaining agreements from unions all at the same time. Moreover,

since the U.S. is a federal system, with a national government and constituent government entities, called "states," which also encompass counties and municipalities, all of them are empowered to make law legislatively or by means of the administrative law process within their jurisdictional domains, and there is, consequently, a LOT of law in the United States. One resulting problem is that "the law in the US is a cacophony of so many different laws and cases that it often lacks consistency or definitive answers" (Solove, 2015, para. 14). Therefore, it might be "easy" for some managers to become confused and confounded with all these complex laws, regulations, rules, and policies.

Growing modern companies accumulate demographic data from their employees and customers which often include names, home addresses, personal phone numbers, and other such information. Additionally, they have access to the collection of bank and credit card account numbers, salaries earned by specific professions and in certain regions, the credit history of customers, and their social security numbers. Of course, different regulations impose unique laws on different forms of data. One example is the Gramm-Leach-Bliley Act (GLBA), which necessitates and mandates that "financial institution" companies ensure both the security as well as complete confidentiality of sensitive and personal information. While GLBA requires security and confidentiality of data, a recruiter doing reference check on a candidate will not get the right information from a bank about this applicant which can lead to negligent hiring as data regarding a criminal's history cannot always be shared without written consent of relevant parties. In some cases, there can be economic or social considerations, market competition regulations by federal laws, parental rights issues, or other such factors that limit the amount of content which can be shared with third parties or outside entities. Additionally, the Federal Trade Commission issued the Safeguards Rule, which demands that the organizations under its jurisdiction have procedures in place to keep all such data and personal information secure. Of course, safeguarding such sensitive data about customers goes beyond the legal requirements since it is the responsibility of any legal and ethical business in any market-driven nation to develop integrity, trust, and confidence.

The omnibus approach used in the EU can have its own unique challenges, but generally, it regulates privacy of individuals and security the same way regardless of whether data is collected by an automotive company, a restauranteur, a healthcare firm, or a financial company such as a bank. There appears to be a kind of simplicity and elegance in the omnibus approach to data protection, but it can at times fail to articulate the uneasiness just so that things can look flawless. In one of its rulings (May 13, 2014), the EU Court concluded that individuals could have the right, under certain conditions (adequacy, relevancy, and accuracy), to ask search engines to permanently delete or remove links with personal information about them. Companies operating within the EU territory and/or impacting its citizens are required to assist individuals in deleting their requested information when this data is inadequate, irrelevant, and/or inaccurate. The conditions specify that decisions might be made on a case-by-case basis

assessment so a fair balance can be sought between the legitimate interests of Internet users and the person's fundamental rights. The balance may include the nature of the information in question, its sensitivity for the person's private life and the public interest in having that information. The answer may also depend on the person asking for removal of his/her information. Overall, "The Right to be Forgotten is a right which is given to all citizens in the EU, no matter what their nationality, subject to the conditions outlined" (European Commission Factsheet, 2014). European Union's 2014 "*General Data Protection Regulation*" or GDPR is designed to govern and specify how private data of individuals should be collected, treated, managed, and/or deleted. In today's hyper-connected world, a person's "right to be forgotten" is a reality, but certainly it can be very complicated when it comes to deleting one's private or personal data from the online community's plethora of webservers. Nonetheless, organizations that are present in the European Union or those that deal with the collection of its citizens' data must create and make available a right for people to be forgotten as per the GDPR compliance requirement (GDPR, 2014).

Many experts would agree with the EU Court's findings which allow individuals to be in control of their data and records, especially when it comes to information that is inadequate, irrelevant, and/or inaccurate. Of course, individuals might have different reasons for not wanting certain information to be publicly available; and sometimes one's current employer might not want the professional to be affiliated with previously employed organizations. For example, when a person leaves an organization and is no longer working with its personnel, then his/her online affiliations with that organization should reflect that new status. If a professor works as an Associate Professor for a university in California, and he or she takes a job with another institution in Florida, then the professor's affiliation with the university in California must no longer appear as presently teaching with them, since this duality can create accreditation problems for the institution in Florida. As such, it is extremely important that adequate, relevant, and accurate information is provided about individuals on all private and public online forums. Overall, therefore, the American approach to privacy is sector-based, with a big mix of legislation and regulation which provide legal rules and encourages self-regulation and ethical behavior. This approach focuses on protecting personal information in each industry or sector. The disadvantage of the American approach is that it can be time-consuming and complicated and perhaps even contradictory. Also, diverse juries and judges might make different judgments due to situational and legal differences and perhaps even pressures from political parties' ideologies. The advantage is that the regulations will be more relevant to the unique and specific needs of each industry and profession. In the United States, the Gramm-Leach-Bliley Act and the Federal Trade Commission's Safeguards Rule appear to be effective laws as they have many similarities and consistencies in forcing companies to properly secure customers' private data. Ultimately, a combination of the two systems might be the best approach. At the beginning of an industry, the EU method is best to protect everyone by providing a level playing field. Once the industry is mature, then a sector-based or decentralized regulation process is more relevant.

Consumer Protection

The Consumer Financial Protection Bureau (CFPB) is public sector agency in the United States dedicated to making sure Americans are treated fairly by entities such as banks, lenders, and other such institutions. Their aim is to "protect consumers from unfair, deceptive, or abusive practices and take action against companies that break the law" (CFPB, 2022, para. 3). CFPB equips consumers that deal with banks and financial institutions with the most relevant information, knowledge, steps, recommendations, and tools needed for smart monetary decisions.

CFPB's vision is to have all companies play by the same consumer protection rules as these businesses compete fairly while providing the best quality and service. To achieve this vision of consistent protection for all consumers along with standardized rules for all companies, CFPB (2022, para. 3 - 4) promises to empower consumers, enforce the federal laws, and educate organizations to conduct business in a socially responsible manner.

- *Empower*. CFPB creates tools, answers common questions, and provides tips that help consumers navigate their financial choices and shop for the deal that works best for them.
- *Enforce*. CFPB acts against predatory companies and practices that violate the law and have already returned billions of dollars to harmed consumers.
- *Educate*. CFPB encourages financial education and capability from childhood through retirement, publish research, and educate financial companies about their responsibilities.

CFPB's role in protecting consumers is a very important and significant one to deter wrongdoing on the part of powerful institutions and to enforce existing laws when unfair practices are reported. More specifically, the CFPB was created to provide:

1. Rooting out unfair, deceptive, or abusive acts or practices by writing rules, supervising companies, and enforcing the law.
2. Enforcing laws that outlaw discrimination in consumer finance.
3. Taking consumer complaints.
4. Enhancing financial education.
5. Researching the consumer experience of using financial products.
6. Monitoring financial markets for new risks to consumers (CFPB, 2022, para. 6).

CFPB is always on the lookout for any problems and risks, especially those associated with online payment systems. Any online payment system could face a myriad of problems and challenges from hackers and improperly protected systems. At a minimum, personal experience with online retailers shows that to process an online sales transaction effectively, at least three

things are needed for security, protection, trust development, and efficiency: 1) Shopping Cart, 2) Secure Server, and 3) Payment Processing.

The main *shopping cart software* keeps track of what the user selects to buy from the website before proceeding to the "checkout". The company and financial institutions need to make purchasing as easy and stress-free as possible for the customer, which should help to avoid "*shopping cart abandonment*," which describes customers who select items to buy, but then decide not to purchase. To reduce shopping cart abandonment, Authorize.net (2012) suggestions the following:

1. Show customers that you are a reputable business.
2. Consider using third-party endorsements.
3. Clearly show how you will protect the customer's personal information. Let them know about transaction security features and services used by your e-commerce website.
4. Make sure visitors know where they are in the checkout process.
5. Have *progress indicators* on screen to let visitors know where they are in the checkout process.
6. Keep the checkout process streamlined. If the checkout process is too long and there are too many steps, you will lose customers.
7. Provide clear instructions for how to proceed through the product selection and checkout process. Make sure the shopping cart buttons clearly indicate the next steps (e.g., Continue with Checkout, Finalize Purchase, etc.). Make sure that an "add to cart" button is clearly visible on the product page.
8. Provide warranties or guarantees for your product. Make sure warranties or guarantees are clearly visible, particularly during the last steps of the checkout process (Authorize.Net, 2012).

CFPB seems to be offering various ways to protect consumers' and businesses which appear sufficient for most prospective complaints and disputes. As a matter of fact, CFPB processes about 10,000 complaints on a weekly basis regarding online payments and other such financial products and services so that companies can provide a response. Since Internet laws are still being developed, adapted, and adjusted, it is a positive factor that they are open to improving their own services as there is the CFPB Ombudsman to deal with any process issues. Their CFPB Ombudsman's Office is expected to act as an independent, impartial, and confidential resource to help consumers and businesses resolve any process-related problems in an informal manner. Any consumer or entity can contact the CFPB Ombudsman about a process issue from interacting with the CFPB if the issue could not be resolved by first contacting their staff and management, or when one simply wants to share the concern with the Ombudsman in confidence.

The Federal Trade Commission

The Federal Trade Commission (FTC) is an independent bureau or organization in the United States to enforce the civil U.S. antitrust laws and to protect consumers from fraudulent business transactions. More specifically, the agency's role in any form of commerce is critically significant and very important as "The Federal Trade Commission works to prevent fraudulent, deceptive, and unfair business practices. They also provide information to help consumers spot, stop, and avoid scams and fraud" (FTC, 2022, para. 1).

There are millions of identity theft victims each year in the United State of America. As such, one of the main goals of the Federal Trade Commission is to prevent identity theft which hurts consumers' confidence in doing business face-to-face and especially online, where data and information can be collected using "cookies" on each website. When this data is not kept private and not protected well, a person can fall victim to identity theft. Of course, identity theft is a crime. The Identity Theft Act (ITA) sees identification of a person by such elements as a name, social security number, date of birth, government-issued driver's license, and biometric data such as fingerprints, etc.

Most time-impoverished online users tend to quickly agree with any disclosures made by various entities as they are in a hurry to make their purchase and receive their products. Nonetheless, it is the duty and responsibility of advertisers to make sure consumers fully understand what they are agreeing to when purchasing products online. Advertisers should make their disclosures transparent, clear, and readily available to consumers to ensure that their personal data (i.e., personal phone numbers) will not be made available publicly for others to use. The Dot Com disclosures laws require that advertisers should provide clear and conspicuous content while they "draw attention to" disclosures, which should be "as close as possible" to the relevant products or purchases. Furthermore, advertisers should "avoid using hyperlinks for disclosures that involve product cost or certain health and safety issues" (Dot Com Disclosure, 2022, para. 5). All these regulations and suggested approaches are designed to protect consumers from becoming victims of identity theft. As such, entrepreneurs, employers, human resource professionals, and managers must follow the laws and recommendations provided by the Federal Trade Commission and other government entities.

The FTC's Fair Information Practice Principles (FIPP) serve as a framework to protect the privacy of everyone regarding personally identifiable information (PII) at the Department of Homeland Security (DHS). FIPP are recommended guidelines regarding fair and ethical information practices in today's world of electronic commerce or e-marketplace. Many of these principles, if not all, are very relevant for application in any organization today since all firms

and individuals are likely to be connected to the internet in getting their work done. There are eight specific principles to FIPP:

1. Transparency
2. Individual participation
3. Purpose specification
4. Data minimization
5. Use limitation
6. Data quality and integrity
7. Security
8. Accountability and auditing

The security principle of FIPP states that the technology used within the department must be of sufficient quality to ensure private contents or personally identifiable information (PII) are kept secure. FIPP's purpose is "to ensure that security controls are put in place in IT systems that are commensurate with the sensitivity of the information they hold." The security principle should be practiced by all firms because privacy mandates are supposed to be proactively built into the systems to safeguard employees and consumers' data "from inappropriate, unauthorized, or unlawful access, use, disclosure, or destruction." Furthermore, the employed professionals working with PII are required to be certified with relevant qualifications and security standards.

The data minimization principle is there to encourage the collection of only the most relevant information from everyone. For example, the Department of Health Services (DHS) employees can only collect a person's Social Security number when it is truly necessary and aligned with the authority granted to them. The data minimization principle is very appropriate for companies so they can focus on only collecting what is truly relevant and necessary information and to use it for the specific purpose when it was obtained. The data minimization principle should be practiced by all organizations; and when such data is no longer necessary, it must be safely and securely destroyed to prevent it from being used by unauthorized individuals or hackers.

The individual choice principle should allow "users" to consent for the collection, use, dissemination, and maintenance of their personally identifiable information. This principle should be practiced by all organizations, including government organizations, and the later must allow and enable individuals to correct any errors through the Freedom of Information Act (FOIA).

While the world of Internet of Things (IoT) is constantly changing everything we do, and consequently more data will continue to be collected for the benefit of consumers and society,

the specific principles to keep data secure will need to be adjusted and expanded on in accordance with prevailing legal, ethical, and business norms. In the current times, the utilization of these FIPP guidelines can afford the minimum security needed to keep consumers' data secure in today's cyberspace or Internet of Things world where everything appears to be connected and communicating to something else in real time with the aim of network neutrality or equal access to all. Overall, as one expert summarizes,

> The Internet has evolved in one generation from a network of electronically interlinked research facilities in the United States to one of the most dynamic forces in the global economy, in the process reshaping entire industries and even changing the way we interact on a personal level. The FCC's efforts to create network neutrality rules notwithstanding, the federal government has largely stood back and allowed this phenomenon to occur without imposing much regulation. And, as we have seen over the years with AOL, Microsoft, Google, Facebook, Apple, and many, many, others, the industry left largely to its own devices has experimented with countless business and technological models, many to great effect. Google for example follows an open model, while Apple almost religiously adheres to a closed system. Each is successful. And, in its own way, each is valuable to the Internet business ecosystem and to consumers (Ohlhausen, 2013, p. 85).

RECOMMENDATION

Internet and the social media technologies and applications have advanced faster than the laws about their ethical and legal use. Social media is vast, and can include social or professional networking, blogs and micro-blogs, digital media video and image sharing, and other online applications which may include location-sharing, consumer reviews, virtual worlds, and social bookmarking (Imtiaz and Nasim, 2022; social media, 2018). Businesses and government officials must do everything possible to protect employees and consumers. Moreover, employees and customers must also be educated to take personal responsibility in cautiously posting and sharing their personal data (Wilkinson & Reinhardt, 2015). Research shows that while more people are sharing photos online now (76.7% in 2020 versus 69.8% in 2016), "the majority of internet users take online privacy seriously" (Alibeigi, Munir and Asemi, 2022, p. 120). Consequently, there is a need for more guidelines and clarity on what data is being collected through website cookies and how privacy is being protected. "The guidelines may include the type of data that they will collect through cookies, the type of cookies, and the duration of use, the deletion of data and the purpose of collection" (Alibeigi, Munir and Asemi, 2022, p. 133).

Most technically savvy organizations are putting social media into good use by promoting their firms' brand awareness and by regularly engaging their customers; in this way, this constant social media engagement allows firms to "keep their finger on the pulse" of their existing and

prospective clients and customers. Some of the most common social media usages and practices can include (Social Media Risks, 2019) correcting rumors and false information that are hurtful to one's image and brand. In addition, proper social media use is often used for employment practices, such as the staffing, attraction, and retention of workers.

Firms can monitor social media platforms to make sure there are no false information about their brand, products, and/or services. The company should implement a formal monitoring program for potentially damaging comments about the company or its products and services by hiring a third-party monitoring vendor or using their own internal employees. It is important that firms do not ignore defamatory comments or misleading information about their brand and range of products. In some cases, the company can take legal action or send a formal "cease and desist" letter. It is very important for companies to regularly enforce their policies on a consistent basis (Social Media Risks, 2019). However, as an important legal and ethical perquisite it is critical that employers notify employees that their social media use will be monitored, which notification should also obviate invasion of privacy lawsuits. That is, an invasion of privacy lawsuit requires a "reasonable" expectation of privacy in a protected and private sphere; and thus how can one have a "reasonable" expectation of privacy for social media use when one is being informed by one's employer that such use will be monitored. (Cavico and Mujtaba, 2020).

Employee misuse of social media can be devastating to a company, as it can lead to harassment and discrimination cases. Ultimately, when workers are constantly griping on social media about their departments, managers, or the general work environment in the organization, it can negatively impact the employer's reputation, thereby thwarting future candidates from applying as well as consumers from wanting to do business with the firm. There are other forms of risks associated with employee use of social media, which can include (Social Media Risks, 2019):

1. Decrease in productivity.
2. Inappropriate conduct among employees.
3. Disclosure of confidential or proprietary information.
4. Unlawful disciplinary action for certain non-working time and off-duty conducts or otherwise protected social media use.
5. Liability for employee content.

Considering the relevant risks associated with employees' use of social media, it is important for companies to create rational policies and send a "loud and clear" message about the organization's expectations for employees' use of online forums to make sure there are no violations of anyone's privacy rights. Without sound policies in the workplace, employees will be more confused, stressed, less productive, and more likely to leave employment.

Judge Ethically

Companies need to educate their employees about ethical decisions that are good for employees, consumers, and society in general (Cavico and Mujtaba, 2016). Otherwise, regulations will be imposed by the government sector to legally punish perceived enethical violators.

Meta corporation, the parent company of Facebook, had been on the news about privacy (Johnson, Egelman & Bellovin, 2020) as they allegedly shared customer data and did not follow their own policy mandates (Liu et al., 2011). Supposedly, Meta obtained information without permission and used customers' health data from hospital websites for commercial purposes. It has been reported that, "the Meta Pixel, a portion of JavaScript code that allows websites to track visitor activity, was being used on hundreds of hospital websites…. allegedly sent packets of data to Facebook whenever someone clicked a button to schedule a doctor's appointment" (McKeon, 2022, para. 3). The claim is that Meta had been using automated technology to receive consumer data without obtaining permission from the hospitals *or* the consumers. As such, any use of this data would be in violation of existing privacy policy laws and the company's own policy.

Sadly, technology is at times used in violation of existing laws to collect consumers' data and to lock people into subscription agreements. The unethical practice of "dark patterns" has become more common among some industries and firms. For example, some firms (i.e., Noom) have been engaging in unlawful auto-renewal subscription business models as they lure customers in with the opportunity to "try" its programs. Once they are signed in to "try" the program, then these companies impose significant complex barriers to the cancellation process, such as by only allowing customers to cancel their subscriptions through their virtual coach. Such practices often result in customers paying a nonrefundable advance lump-sum payment for many months. This practice of auto renewal which often forces consumers to stay "opt-in" is known as "dark patterns," which are techniques to trick consumers into trying a service or product by agreeing to a contract with the assumption that they can easily discontinue or cancel. They often appear in the context of negative option marketing, which refers to transactions containing terms or conditions under which the seller may interpret a consumer's silence or failure to affirmatively reject or cancel a product as acceptance (such as automatic renewal subscriptions, free trial programs, etc.). Companies should avoid such unethical and illegal practices by proactively monitoring and auditing themselves annually to ensure compliance with all local, state, and federal laws as well as ethical norms.

Technical errors and personal data of employees or consumers being stolen can take place at the most secured facilities via network vulnerabilities. For example, during August 3, 2022,

Equifax admitted that some consumer credit scores were changed mistakenly because of their computer problems. Apparently, according to the company, a server "coding issue" was the cause of the inaccurate scores. Earlier, it had been reported that Equifax gave inaccurate credit scores for millions of American consumers that were securing loans. Incorrect scores were sent about these consumers around March-April until they became aware of it or revealed this problem in May of 2022. Prior to this, there was a cyberattack at Equifax, and hackers had accessed Social Security numbers, driver's license numbers, and home addresses of their consumers (Saharan, 2022). If the disclosure of consumers' identifiable information become widespread and the norm for some firms, then even the company's officials can be fined by the government for not properly securing private data. Moreover, the company will be sued civilly for invasion of privacy for negligence and perhaps even gross negligence, thus risking punitive damages for the latter culpability.

Retain the Top Talent

Modern technologies and regulations should all be balanced to help companies successfully serve their constituencies. If the public sector laws are too strict, it will stifle creativity in any capitalistic marketplace and create distress for employers, workers, and customers. If there are no laws, then some "greedy" and overly ambitious managers will focus on maximizing their profits at the cost of undue risks to personal data of their employees and customers. Again, reference must be made to the famous (infamous, rather) Wells Fargo fake account and hacking scandal (Cavico and Mujtaba, 2017). Therefore, there should be a balance of sound legal regulations and organizational ethical policies to have a high level of trust and confidence among clients, customers, employees, managers, organizations, government regulators, and the legal profession.

Attracting and retaining employees in this changing time of post-Covid-19 pandemic recovery times is one challenging and complicated task, but certainly a necessity always for great managers and firms that want to make a positive difference for their employees, community, stockholders, and other stakeholders, including society. One expert's view clearly communicates the responsibility of HR professionals as follows:

> I believe that Human Resources has a larger role than ever before. We are tasked with assisting the company and its employees as they come out of a pandemic and enter recessionary times. There are many avenues to look at and there is not one solution. Employees want flexibility, work life balance and they want to live their best lives. Human Resources can help by enhancing current benefit programs in place and see what works and what no longer does. Employees want programs for parental leave, tuition reimbursement, unlimited time off, remote work and more. This lies on the shoulders of HR. It's time to get crafty with our trade. Robust onboarding, career development, and access to unlimited training are

> other wants. Programs mentioned above were once considered perks are now a demand by the current workforce, regardless of their generation. Yes, HR bares the responsibility of creating the new programs, however, we must have the buy in from the business leaders. All programs are investments that the organization will be burdened with. In 2009, while in a recession, it was an employer's market. Now, in 2022, the tables have turned, and the employees and the candidates are calling the shots. The question is, are we up for the challenge? I am (Personal Communication with Christina Palmer, Human Resources Director, August 26, 2022).

HR professionals must be innovative and creative in meeting the demands of their employees in this digital era of e-commerce. Flexibility of using technology for work from any place is a great way to retain talented people (Mujtaba, 2014). By offering a model with a higher degree of autonomy — for example, the freedom to work where and when one wants, but with access to a physical office — may be an effective way to buffer salary increase expectations during inflation and recessionary times, while still providing employees with something they desire (Tansey, 2022). Of course, "Anything you can do to increase flexibility and the ways employees can exercise that flexibility, from extending deadlines to offering schedule-sharing or remote work, can be powerful ways to compensate without raising pay" (Tansey, 2022, para. 5). Employers should invest in the training of employees in the latest technologies and career planning of workers, perhaps through effective succession planning and development (SP&D) programs. Also, employers need to provide timely bonuses, which can be an efficacious way to appreciate employees' hard work and commitment amid stressful times and complex regulations. While employees can feel valued by monetary compensation, it should be noted that higher wages are not the only strategy for rewarding workers, since efforts like continuous education, timely coaching, and even informal mentorship programs are incentives that may not be pay-related but can be very meaningful to the attraction and retention of top talent in the modern workplace (Lopez, Marquez, Martinez, Marretta, Briana, Lozovnoy, and Mujtaba, 2022).

Human resources departments can and must help their enterprises retain talented and productive workers by listening to all voices of workers and developing sound open-door policies (Mujtaba, 2022b). For most firms, after the hiring process, some employees rarely ever have any meaningful connection with the human resources department professionals. Modern organizations should continue to track each employee's progress throughout his or her employment with the firm by "keeping their finger on the pulse" of each employee's feelings, progress, and future goals. HR personnel should also document relevant outside hobbies or activities that each employee is doing outside of the job. For example, an employee furthering his/her education in the profession or other fields, such as online security, employment laws,

etc., could be useful information for lateral career movements and even internal promotions, especially when new laws and regulations are being imposed in a specific sector of the industry. Auditing compensation and benefits practices is another important area for human resources professionals to make sure the firm is compliant with the latest laws and to adjust salaries as per the marketplace norms. Companies should periodically review similar positions at other companies and examine what those salaries look like in order to be fair and to remain competitive. This review and analysis will reduce jealously, anger, and "quiet quitting," which latter practice seems to be a trend during low unemployment periods where workers can telecommunicate or complete their tasks from home without having to move outside of the city or state. Learning more about employees' work-life balance, and how managers can offer flexibility to ensure that workers are experiencing a positive balance, could be a significant influence in people deciding to stay or look around for other opportunities. The Covid-19 pandemic changed many companies' work "ecosystems" in which the Internet was used extensively to complete tasks without physically going into the office; and accordingly, it is more important than ever for each organization to remain flexible and adjust to the needs of their employees in this age of "internet of things" and digitally diverse trade era.

Ultimately, while government regulations, new technologies, and inflation might all impact firms and organizations, it is important that these costs are not passed on to employees who are also consumers. We know that employees shop at the community stores and are immediately impacted by any rise in products they consume. If workers are not receiving a concomitant or fair increase in their salaries, then the rising costs will hurt them even more, which can cause them to seek employment elsewhere. Moreover, we know that employees place great stock in learning and development (L&D) opportunities, since they gain valuable skills, knowledge, and experience in their current professions and future opportunities. So, offering these types of relevant employment development initiatives and programs can signal the willingness of a company to invest in its people, thereby retaining more top talent while attracting great prospective candidates.

Therefore, it is very important to take the time necessary to clearly communicate these policies and programs, particularly the privacy and social media policies, with all workers through the company's ethics code, manual or handbook, training programs, blogs, website, and other platforms, and especially before these policies are implemented and enforced. As always, it is essential to note that change can be difficult for employees; so, the ethical as well as "smart" firm should remain open-minded, listen to any concerns, and professionally and proactively discuss any potential issues, especially on data privacy. Of course, if used properly, the use of modern technologies can be a very powerful tool to boost productivity, safety, security, and collegiality in the workplace.

SUMMARY

With the integration of modern technology in this hyperlocal, yet global, and hyperconnected and complex work environment, employers must do everything they legally, ethically, and practically can do to protect their employees, customers, and business operations. As can be seen from the plethora of diverse sectoral regulations in the United States, firms have some freedom in monitoring and protecting their employees' offices, computers, emails, phone calls, and electronic communications. Ultimately, workplace data protection is at the discretion of companies; and if performed in a responsible manner by employers, the organization will be kept legal and competitive, and thereby safely moving forward economically, the employees, clients, and consumers will be protected. Employers, therefore, can, should, and must protect their employees, clients, and customers' data. Such protection is the legal, ethical, practical answer and thus the "right" thing to do for the just as well as egoistic firm.

Human resources professional also must educate employees and warn them about all applicable government regulations and social media to protect their own privacy as well as those of their colleagues and clients and customers by not publishing their personal information on social media since everything has the possibility of becoming public in today's age of internet. We all need to balance posting, sharing, and transmitting data with data protection by proceeding intelligently yet cautiously to reduce hacking and identity theft. Eventually, rational legal regulations, particularly regarding privacy, will catch up to technology and thus eliminate or at least reduce some of the risks created by social media and the Internet. Accordingly, the private sector should create policies that make sense in protecting their employees and customers' private data. The private sector is in the best position to do this properly as they have the egoistic financial incentive of keeping their clients and customers while attracting new ones as well as obtaining and keeping good employees. If the private sector does not create good and fair rules and policies, their clients and customers will abandon them and so will their talented employees. Of course, ultimately, it is the legal responsibility of the public sector officials and government agencies to organize and codify all the agreed-upon fair and ethical practices into sound legal rules and regulations to protect all personal data provided by clients, customers, and employees.

As a summary, to prevent identity theft and data breaches, there are many "best practices" to guide and monitor employees' social media behaviors, while respecting their rights to privacy and freedom of expression (Mujtaba 2003). At a minimum, the following should be considered:

1. Create a social media policy. A firm should create a comprehensive and updated policy that addresses data privacy and information sharing.

2. Comply fully with all relevant federal and state laws.
3. Document and communicate the social media policy through the employee handbook, intranet, and various orientation programs.
4. Prevent and block irrelevant outside content from being accessed through the company computers and internet connections.
5. Practice ethical enforcement of the policy for legitimate business needs.
6. Respect employees' privacy and rights.
7. Institute proper protection apps and software to keep all personal data private.

Therefore, managers and human resources professionals need to make sure the firm's confidentiality, privacy, Internet, and social media policies and practices are legal and moral and are respectful to all stakeholders. Moreover, such policies and practices must not be unduly intrusive or invasive on the day-to-day personal and private activities and interactions of employees. Thus, it is very important to avoid infringing on the privacy interests of employees as well as clients and customers by making sure that the company's policies and practices regarding confidentiality and privacy are legal, ethical, practically efficacious, and most importantly transparent in all circumstances and to all stakeholders. The authors submit, and firmly believe, that premised on a foundation of "good" business decision-making and concomitantly adhering to the values of legality and morality, a company or organization will do well and be successful and also will be able to sustain that success in the long-term, and thereby be a "good" firm in all respects and thereby act in a beneficial and socially responsible manner - for the firm itself and its shareholders, and also its employees, their families, the local community, and other stakeholders, including society as a whole.

REFERENCES

Alibeigi, A. Munir, A. B., and Asemi, A. (2022). A decade after the Personal Data Protection Act 2010 (PDPA): Compliance of communications companies with the notice and choice principle. *Journal of Data Protection & Privacy*, 5(2), 119-137. Website: https://www.henrystewartpublications.com/jdpp

Authorize.Net (2012). *E-commerce: Getting Started Guide*. Authorize.Net: San Francisco. Available at: www.authorize.net

Cavico, F. J. and Mujtaba, B. G. (2020). *Business Law for the Entrepreneur and Manager (4th edition)*. ILEAD Academy: Florida.

Cavico, F. J. and Mujtaba, B. G. (2017). Wells Fargo's Fake Accounts Scandal and its Legal and Ethical Implications for Management. *Advanced Management Journal*, 82(2), 4-19.

Cavico, F. J. and Mujtaba, B. G. (2016). *Developing a Legal, Ethical, and Socially Responsible Mindset for Sustainable Leadership*. ILEAD Academy: Florida.

CFPB (n.d.). *Consumer Financial Protection Bureau: The Bureau.* Accessed on August 27, 2022 at: https://www.consumerfinance.gov/ / https://www.consumerfinance.gov/about-us/the-bureau/

Children's Online Privacy Protection Rule (2000) How to Comply with The Children's Online Privacy Protection Rule: A Guide from the Federal Trade Commission the Direct Marketing Association and the Internet Alliance. Accessed on August 26, 2022, from: https://www.ftc.gov/sites/default/files/documents/cases/2008/12/081211appb0823071.pdf

Clinton, W. J. and Gore, A. (July 1, 1997). *The Framework for Global Electronic Commerce*. Clinton Whitehouse: Washington, D.C. Source: https://clintonwhitehouse4.archives.gov/WH/New/Commerce/

Consumer Data Privacy (February 2012). Consumer Data Privacy in A Networked World: A Framework for Protecting Privacy and Promoting Innovation in The Global Digital Economy. *The White House: Washington*. Link: file:///C:/Users/mujtaba/Downloads/The%20Consumer%20Privacy%20Bill%20of%20Rights.pdf

Department of Homeland Security (DHS). Link: www.dhs.gov/privacy

Dot Com Disclosure (2022). *FTC Staff Revises Online Advertising Disclosure Guidelines*. Link: https://www.ftc.gov/news-events/news/press-releases/2013/03/ftc-staff-revises-online-advertising-disclosure-guidelines

Fair Information Practice Principles (FIPP) (December 29, 2008). *FIPP Fact Sheet*. Department of Homeland Security (DHS). Link: https://www.dhs.gov/publication/privacy-policy-guidance-memorandum-2008-01-fair-information-practice-principles

FTC (August 29, 2022). FTC *Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations*. Federal Trade Commission: Protecting America's Consumers. Link: https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other

FTC (2022). Link: https://www.usa.gov/federal-agencies/federal-trade-commission

FTC (2017). Privacy & Data Security. Federal Trade Commission: United States of America. Link: file:///C:/Users/mujtaba/Downloads/privacy_and_data_security_update_2017.pdf

Ekran Systems (March 31, 202). *How to Monitor Employees at Work: 7 Best Practices*. Category: Security. Link: https://www.ekransystem.com/en/blog/best-practices-how-monitor-employees-work

European Commission Factsheet (2014). *Factsheet on the "Right to be Forgotten" Ruling*. C-131/12. Link: https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2014/06/factsheet_data_protection_en.pdf

Garon, Jon M. (2020). *A Short & Happy Guide to Privacy and Cybersecurity Law*. West Academic Publishing.

GDPR (2014). *General Data Protection Regulation*. Link: https://gdpr.eu/right-to-be-forgotten/

Goitein, Elizabeth (October 22, 2019). How the FBI Violated the Privacy Rights of Tens of Thousands of Americans. Brennan Center for Justice. Link: https://www.brennancenter.org/our-work/analysis-opinion/how-fbi-violated-privacy-rights-tens-thousands-americans

Grimmelmann, James (2019). *Internet Law: Cases and Problems*, 9th edition. Semaphore Press: Middletown: Delaware.

Habinsky, Jason and Boone, Haynes (2022). Monitoring and Protecting Employee Privacy. LexisNexis: *XpertHR Employment Law Manual, 2154.*

IBM (April 16, 2018). New Survey Finds Deep Consumer Anxiety over Data Privacy and Security. *CISION PR Newswire*. Link: https://www.prnewswire.com/news-releases/new-survey-finds-deep-consumer-anxiety-over-data-privacy-and-security-300630067.html

Identity Theft (2022). *Federal Trade Commission: Identity Theft*. Link: https://www.identitytheft.gov/#/

Imtiaz, Summan and Nasim, Irum (2022). The impact of Social Media Activities on Emotional Attachment with the Mediating role of Brand Image and Brand Commitment of retail sector. *Journal of Entrepreneurship and Business Venturing*, 2(1), 33-59. Link: https://jebv.pk/index.php/JEBV/article/view/6/8

Jamshed, Yasir (2022). A Framework for Digital Technology and Marketing Research: Examining the effects of Trust Inclination, and Information Adoption on Purchase Intentions of Commercial Business Ventures. *Journal of Entrepreneurship and Business Venturing*, 2(1), 60-78. Link: https://jebv.pk/index.php/JEBV/article/view/8/10; https://jebv.pk/index.php/JEBV/article/view/8

Johnson, M., Egelman, S., & Bellovin, S. M. (2012). Facebook and privacy: it's complicated. In *Proceedings of the eighth symposium on usable privacy and security* (pp. 1-15).

Justice Department (2020). *Overview of the Privacy Act: 2020 Edition. Criminal Penalties.* The U.S. Department of Justice. Link: https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition/criminal#:~:text=The%20Privacy%20Act%20allows%20for,if%20the%20official%20acts%20willfully

Liu, Y., Gummadi, K. P., Krishnamurthy, B., & Mislove, A. (2011). Analyzing facebook privacy settings: user expectations vs. reality. In *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 61-70).

Lopez, A., Marquez, B., Martinez, D., Marretta, G., Briana, G., Lozovnoy, N. and Mujtaba, B.G. (2022). Amazon's Gender and Racial Discrimination Impacts on Employee Performance. *Journal of Human Resources Management and Labor Studies*, 10(1), 1-10. URL: http://jhrmls.com/vol-10-no-1-june-2022-abstract-1-jhrmls; http://jhrmls.com/journals/jhrmls/Vol_10_No_1_June_2022/1.pdf

McKeon, J. (2022). Meta Faces Another Lawsuit Over Health Data Privacy Practices. *Health IT Security*. Retrieved from https://healthitsecurity.com/news/meta-faces-another-lawsuit-over-health-data-privacy-practices

Muffler, Stephen C., Cavico, Frank J., and Mujtaba, Bahaudin G. (2010). Diversity, Disparate Impact, and Ethics in Business: Implications of the New Haven Firefighters' Case and the Supreme Court's *Ricci v. DeStefano* Decision. *Advanced Management Journal*, 75(3), 11-19.

Mujtaba, B. G. (April 2023). *Digital Literacy on Privacy Rights Policies in the American Workplace.* DOI: 10.1007/978-3-031-23432-3. Book Chapter in "Multidimensional and Strategic Outlook in Digital Business Transformation" by Pelin Vardarlier (Editor). Springer International Publishing. ISBN: 9783031234316. Link: https://www.barnesandnoble.com/w/multidimensional-and-strategic-outlook-in-digital-business-transformation-pelin-vardarlier/1142680505

Mujtaba, B. G. (2014). *Managerial Skills and Practices for Global Leadership*. ILEAD Academy: Florida.

Mujtaba, B.G. (2022a). Workplace Management Lessons on Employee Recruitment Challenges, Furloughs, and Layoffs during the Covid-19 Pandemic. *Journal of Human Resource and Sustainability Studies*, 10(1), 13-29. DOI: 10.4236/jhrss.2022.101002

Mujtaba, B. G. (2022b). *Workforce Diversity Management: Inclusion and Equity Challenges, Competencies and Strategies (3rd edition).* ILEAD Academy: Florida.

Mujtaba, B. G. (2003). Ethical Implications of Employee Monitoring: What Leaders Should to Consider! *Journal of Applied Management and Entrepreneurship*, 8(3), 22-47.

Ohlhausen, Maureen K. (February 1, 2013). Net Neutrality vs. Net Reality: Why an Evidence-Based Approach to Enforcement, and Not More Regulation, Could Protect Innovation on the Web. *Engage*, 14(1), 81-87. Available at SSRN: https://ssrn.com/abstract=2670816 ; Link: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2670816

Phomkamin, J., Pumpuang, C., Potijak, P., Sangngam, S., Ketprasit, I., and Mujtaba, B.G. (December 2021). Engagement Strategies for E-commerce Businesses in the Modern Online World. *SocioEconomic Challenges, 5*(4), 24-34. Link: https://armgpublishing.sumdu.edu.ua/journals/sec/volume-5-issue-4/article-2/

Rustad, M. L. & Koenig, T. H. (2019). Towards a global data privacy standard. *Florida Law Review*, *71*, 365. Link: http://www.floridalawreview.com/2019/towards-a-global-data-privacy-standard/

Solove, Daniel (Nov. 13, 2015). The Growing Problems with the Sectoral Approach to Privacy Law. Privacy + Security Blog: Teach Privacy. Link: https://teachprivacy.com/problems-sectoral-approach-privacy-law/

Saharan, Shubham (August 2, 2022). Equifax Says Consumer Credit Scores Changed in Computer Error. *Bloomberg: US Edition.* Link: https://www.bloomberg.com/news/articles/2022-08-02/equifax-says-consumer-credit-scores-changed-by-computer-error

Social Media (2018). *Social Media in the Hiring Process*. Practical Law Practice: Note 9-535-2907. Westlaw: Thomson Reuters.

Social Media Risks (2019). *Social Media Risks and Rewards*. Practical Law Practice: Note 8-501-1933. Westlaw: Thomson Reuters.

Tansey, C. (2022, January 25). *4 ways HR teams can address inflation*. Lattice: Resources for Humans. Retrieved August 25, 2022, from: https://lattice.com/library/4-ways-hr-teams-can-address-inflation

Telecommuting (2022). *Telecommuting Policies: Key Drafting Tips*. LexisNexis. Accessed August 1, 2022 at: https://plus.lexis.com/document?crid=648749bc-a883-4dc1-bdb0-a0c93e44689f&pddocfullpath=%2Fshared%2Fdocument%2Fanalytical-materials%2Furn%3AcontentItem%3A5C67-KTK1-F1WF-M0JD-00000-00&pdsourcegroupingtype=&pdcontentcomponentid=500749&pdmfid=1530671&pdisurlapi=true

Warren, S. D. and Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220. Link: https://h2o.law.harvard.edu/text_blocks/5660 ; https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Wilkinson, T. and Reinhardt, R. (2015). Technology in Counselor Education: HIPAA and HITECH as Best Practice. *Professional Counselor, 5*(3), 407-418.