Preface

OUR DIGITAL NETWORKED WORLD: ISSUES, CHALLENGES, AND OPPORTUNITIES

Information defines us. It defines the age we live in, the societies we inhibit, the ways we conduct our lives, and ultimately, who we are as humans. Information is the output of our human intellectual endeavors. Since there are no limits to human intellectual capabilities, none can exist for information either. It is unmistakable that we are in the midst of a "digital revolution" with profound implications on the way we conduct our lives. This revolution is characterized by digital network pervasiveness and the resulting transformation of our daily lives in ways unimaginable less than a decade ago. New technologies make possible what was not possible before. We are more interconnected now than we have ever been in our history. The dizzying pace of advances in information technology that characterize this revolution and the extent to which these technologies have become "information appliances" have transformed our lives even more drastically than what we had envisioned. The digital ubiquity and the resulting interconnectedness have fundamentally redefined who we are and how we relate to one another and to the technology. Our world has been altered so drastically that we are no longer able to conduct our lives without the use of communication technologies such as our smartphones, social media, instant messaging, and chats. These technologies allow us to communicate and stay in touch more freely and effortlessly with our families and friends, to stay informed about current events that impact our lives and even shape these events, and to make more informed decisions, be it medical, financial, educational, or even emotional, but open us to underserved scrutiny and possible demonetization and retribution.

Perhaps the most sweeping aspect of this revolution can be found in the ways in which we relate, interact, and communicate not just with one another, including with those in businesses we transact with and government agencies representing us and also in the way we interact with the technology itself. Ultimately, it will redefine the way we perceive and identify ourselves as individuals and members of human society. By making available new options, technologies have led to a restructuring of the hierarchy of values by which we measure and assess the value of these interactions. The impact of this new and fluid value structure will be the driving force in our societal discourse for a long time to come. Technology has also redefined our relationships with businesses we interact with and governmental agencies representing us. We understand and hope that the governments are there to protect and fight for our rights while criminal hackers lurching in the myriad of technologies we use are intended to harm us. However, we also understand the issues and hiding in the shadows are not as clear-cut as we were once led to believe and are changing all the time. Although we are still clearly able to perceive and sometimes identify

and thwart the bad guys intended on robbing us by stealing our personal identifies and other valuable information assets by means of hacking and other malicious intrusive and illegal intents whether they are hackers or spammers, or other criminal wrong doers, we are not so sure about who the good guys are and how to identify and deploy methods to thwart and punish the destructive and criminal behaviors of such groups. The government agencies created to protect us were once viewed and regarded as beacons of justice and proctor of our security and privacy. The extent of reach by the NSA in accessing, storing, eavesdropping, and mining our electronic communications have seriously eroded its "good guy" perception. The government is a prime example of this disambiguation of the perception we assign to it. Is the government a friend or a foe when it comes to protecting our privacy? The perception of the righteousness of our government's intentions in accessing, storing, mining, and analyzing our interactions with them or others has irrevocability changed negatively after Snowden's revelations. Given the complexities of the issues in understanding our relationships, including those between the people, their representative government and business entities, we are only at the threshold of what is promised to be by many experts. We are on the verge of the biggest societal transformation in the history of mankind traced directly to advances in the information technology. This transformation will most likely create new opportunities and many challenges we have yet to fathom.

On June 6, 2013, *The Guardian* and *Washington Post* simultaneously released PowerPoint slides revealing the existence of a top-secret mass-surveillance program called the PRISM. The revelations were made by the 29-year-old American whistleblower Edward Snowden. Although prior to Snowden's leak, it was widely believed that intelligence agencies were able to spy on communication systems, the extents of such capabilities revealed by Snowden were shocking. The 41-slide PowerPoint presentation provided by Snowden was classified by the National Security Agency (NSA) as "top secret with no distribution to foreign allies" (The Guardian, 2014) and was developed as part of a training program for intelligence operatives on the capabilities of PRISM. According to Snowden, the NSA and its British counterpart, the Government Communications Headquarters (GCHQ), were (are) using PRISM program to gain direct access to the servers of some of the world's biggest tech companies including tech giants like Apple, Google, Facebook, and Microsoft. Among the details that the PowerPoint presentation provided was the revelation that large tech companies had cooperated closely with these intelligence agencies to help them circumvent encryption and other privacy controls. *The Guardian* reported that using PRISM, "… these agencies are able to access information stored by major US technology companies, often without individual warrants, as well as mass-intercepting data from the fibre-optic cables which make up the backbone of global phone and Internet networks. The agencies have also worked to undermine the security standards upon which the Internet, commerce, and banking rely" (The Guardian, 2014). Snowden later revealed the existence of Boundless Informant, an NSA tool that provides the intelligence agency with "near real-time" spying statistical capabilities and Stellar Wind program to collect Internet metadata. It is expected that many more shocking revelations are yet to come. It is estimated that the NSA collected almost 3 billion pieces of intelligence on U.S. citizens in February 2013 alone, and it is able to track over 1 billion mobile calls daily. What Snowden disclosed had an immediate and far-reaching impact on not only the ongoing debate surrounding information security and privacy, but broader issues of our relationships with each other and with our government.

Since the events of September 11, 2001, the government has become more aggressively involved and open about the use of data mining and other profiling and data collection techniques, which are being deployed as a matter of national security. Although the government's use of these techniques is not

new, as Snowden's revelations proved, they have become more prolific and invasive. These actions are fueling a heated debate on privacy. Security and Privacy of data has gained increased importance in this new age of information and terrorism. Because of the advances in technology and the lag of the legal/judicial system to amend laws, many organizations as well as the government have been able to collect and use personally identifiable data on individuals to their advantage. Some of this usage is known to the individual but much is collected unknown to the individual. The perceived use of this information is what has sparked many individuals to protest its very collection and use. The tragic events of September 11, 2001 have accelerated the governmental agencies' need for and use of personally identifiable information. These needs and uses are being justified in the name of protecting and promoting national, public, or individual security. For example, organizations and local, state, or federal agencies need to identify individuals faster and to make assessments and judgments about people more accurately and more reliably, in real or near-real time. They also need to authenticate the identities of individuals, check backgrounds and histories, and to verify their credentials and authorizations. In order to do this in a timely fashion, they need to access and sift through massive amounts of personal data quickly from many sources, both public and private, and across numerous jurisdictions, intercept communications and monitor electronic activities. Government agencies and organizations also need to share data and intelligence across different jurisdictions and domains. Data sharing, in particular, magnifies privacy violation risks and underlines the need for reliable Privacy-Preserving Data Mining techniques.

There is a pervasive belief in the American culture that individuals are entitled to a particular level of privacy. According to Justice Brandeis of the U.S. Supreme Court, the right to privacy is "the right to be left alone – the most comprehensive of rights, and the right most valued by civilized men" (Olmstead v. U.S., 1928). Westin (1967, p. 11) defined the right to privacy as "the right of the individuals… to determine for themselves when, how, and to what extent information about them is communicated to others." The level and the application may be debatable; however, individuals have a certain expectation of privacy, which they are reluctant to relinquish. "Privacy encompasses our right to self-determination and to define who we are. Although we live in a world of noisy self-confession, privacy allows us to keep certain facts to ourselves if we so choose. The right to privacy, it seems, is what makes us civilized" (Alderman & Kennedy, 1997, p. xiii).

Although this digital revolution has brought us closer and has made our lives easier and more productive, paradoxically, it has also made us more capable of harming one another and more vulnerable to be harmed by others. Our new vulnerabilities are the consequence of the evolving nature of our interconnectedness. Mason (1986) claims that unique challenges facing our modern societies are the result of the evolving nature of information itself. This evolving nature of information requires us to rethink the way we interact with one another. Mason argues that in this age of information, a new form of social contract is needed in order to deal with the potential threats to the information that defines us. Mason (1986) states, "Our moral imperative is clear. We must ensure that information technology, and the information it handles, are used to enhance the dignity of mankind. To achieve these goals, we must formulate a new social contract, one that insures everyone the right to fulfill his or her own human potential" (Mason, 1986, p. 26). This new social contract has profound implications for the way our society views information and the technologies that support them. For technology to enhance the "human dignity," it should assist humans in exercising and asserting their rights as individuals. Governments play an important role in not only setting the standards of what is acceptable but making sure that our society is protected from "wrong doers." What makes it hard for these agencies to regain the trust of those they are charged

to protect is the prevailing notion that given this current climate of unbridled and unprecedented powers given to the governmental agencies like NSA, the agencies' powers can easily morph into a "big brother," watching you, creating the perception that the government is the "wrong doer" when it comes to protecting its citizens' freedom of expression and self-determination made possible by our constitution. This perception of the people that their governmental representatives are there to protect them can be easily eroded. This can prove very detrimental to these agencies, whose stated goal is protecting the citizens, since it is ultimately impossible to achieve this goal without the support of the citizens. Once this perception takes hold, which it has recently, it will be very difficult if not impossible to change. However, Americans are resilient and reasonable and understand the threats facing them may require new ways of fighting the adversary. What they are asking for are guaranties from these agencies that they understand and discriminate between what is right, ethical, legal, and permissible with what is necessary and vital to protecting our national security. The debate must go on.

LAYOUT OF THE BOOK

The authors present a new approach to Algorithm-Based Fault Tolerance (ABFT) for high performance computing systems. The Algorithm-Based Fault Tolerance approach transforms a system that does not tolerate a specific type of faults, called the fault-intolerant system, to a system that provides a specific level of fault tolerance, namely recovery. The ABFT techniques to detect errors rely on the comparison of parity values computed in two ways; the parallel processing of input parity values produce output parity values comparable with parity values regenerated from the original processed outputs can apply convolutional codes for the redundancy. This method is a new approach to concurrent error correction in fault-tolerant computing systems. Chapter 1 proposes a novel computing paradigm to provide fault tolerance for numerical algorithms. The authors also present, implement, and evaluate early detection in ABFT.

Investing in Information Technology (IT) security is a critical decision in the digital age. In most organizations, it is wise to allocate a significant amount of resources to IT infrastructure. However, it is difficult to determine how much to invest in IT as well as to quantify the maximum threshold, where the rate of return of this investment begins to diminish. The main research question is: How much and what financial resources should be allocated to IT security? Chapter 2 analyzes different practices and techniques used to determine the degree of investment in IT security and recommends some suitable methods for deciding how much should be invested in IT security.

Models transform the managerial inputs into useful information for managerial decision. The Project Evaluation and Review Technique (PERT) is the most widely used model for project management. However, it requires three estimates for the duration of each activity as its input. This uncertainty in the input requirement makes the Critical Path (CP) unstable, causing major difficulties for the manager. A linear programming formulation of the project network is proposed in chapter 3 for determining a CP, based on making one estimate for the duration of each activity. Upon finding the CP, Sensitivity Analysis (SA) of Data Perturbation (DP) is performed using the constraints of the dual problem. This largest DP set of uncertainties provides the manager with a tool to deal with the simultaneous, independent, or dependent changes of the input estimates that preserves the current CP. The application of DP results to enhance

the traditional approach to PERT are presented. The proposed procedure is easy to understand, easy to implement, and provides useful information for the manager. A numerical example illustrates the process.

Authenticity means that the closeness of observation matters for acceptance of new knowledge. The social norm of authenticity can have positive effects of colleagues to appreciate "better" knowledge within opportunity structures for knowledge sharing. However, how ICT influences authenticity in knowledge sharing needs more attention in research on knowledge sharing through online networks. Chapter 4 reports and discusses recent finding of how ICT (here the interactive tool GoToMeeting™) facilitates authenticity.

Information privacy concerns are a dominant concern of the information age, a concern that results from tension between the correct use of personal information and the individual's desire for their information to be private. That tension has extended to the computer-mediated work environment as employees' awareness of the ways in which management can employ technologies to monitor their email and Internet interactions has increased. These concerns have the potential to negatively impact organisational productivity and employee morale. The aim of chapter 5 is to outline some of the key issues relating to workplace surveillance and provide a balanced perspective that identifies the emerging issues and subsequent privacy concerns from the employees' perspective as well as the rationale underlying managements' decision to employ monitoring technologies in the workplace. In doing so, it attempts to progress academic understanding of this issue and enhance practitioners' understanding of the factors that influence employees' technology-related privacy concerns.

Chapter 6 discusses information security challenges encountered during the wearIT@work project and selected legal aspects of wearable computing. Wearable computing will offer interesting opportunities to improve and reengineer work processes in organizations, but can introduce alignment problems as users in organizations may adopt the new technology before organizations are prepared. Further, alignment problems posed by the emerging trend "Bring Your Own Device" (BYOD) are discussed. In addition, needed supportive legal frameworks have not yet fully addressed the new wearable computing technology. Different alignment concepts for how such challenges can be managed are discussed in the chapter.

There are many collection and application sources of identity theft. The Internet is one of the vulnerable medias for identity theft and is used, especially, as an application source of identity theft. Chapter 7 has two objectives. As the first objective, it develops a conceptual framework to prevent/control identity theft of E-Commerce (EC) in conjunction with different sources of identity theft. From this framework and shedding light on the recent literature of sources of identity theft, the authors identify global laws, controls placed on organizations, publications to develop awareness, technical management, managerial policy, risk management tools, data management, and control over employees as potential measuring items to prevent identity theft in EC. All EC organizations are struggling to control identity theft. This chapter argues that control mechanisms of identity theft have both positive and negative impacts on EC. This chapter sets its second objective to explore the integrative effect of overall identity theft control mechanisms on consumer trust, the cost of products/services, and operational performance, all of which in turn contribute to a purchase intention using E-Commerce (EC). A case study in the banking sector through a qualitative approach was conducted to verify the proposed relations, constructs, and measuring items.

Chapter 8 tests the appropriateness of the Unified Theory of Acceptance and Use of Technology (UTAUT) model in the context of end user consumption by means of an online survey with 475 respondents (24% response rate). The chapter shows which factors have the greatest impact on the adoption process

of VoIP technology in the US market in addition to the interactions of the main variables in the model (Performance Expectancy, Effort Expectancy, Social Influence, and Behavioral Intention to Adopt) and whether Trust can improve the predictive value of the UTAUT model to explain intention to adopt. Partial Least Squares (PLS) is used to evaluate the interactions of the main variables. The model includes four moderator variables (Gender, Age, Experience, and Voluntariness of Use). The results support most of the relationships identified in the original UTAUT model. More specifically, Performance Expectancy appears to have the strongest influence on the Intention of a consumer to adopt a new technology. The chapter provides information about whether the inclusion of Trust can generate good results for industry.

Technology is important to software development projects; however, virtual projects are more dependent on technology than traditional co-located projects due to communication and collaboration needs. Two research studies in chapter 9 sought to determine whether seven technology-related risks pose a greater danger to virtual projects than traditional projects and to determine if technology-related risks have a high impact on project success. Results indicate that two technology-related risks exhibited a significantly greater impact on virtual IT projects: (1) inexperience with the company and its processes and (2) inadequate technical resources. Project managers need to be aware that traditional project risks can have a greater impact on virtual projects. Additionally, technology-related risks in the second study were found to have low levels of impact on project success. Results indicate, in cases where a majority of team members are experienced with the application, development technology, and project technology, the risk of technology-related issues seems to lessen.

Chapter 10 is built on two studies: Ishihara (2011) "A Forensic Authorship Classification in SMS Messages: A Likelihood Ratio-Based Approach Using N-Grams" and Ishihara (2012) "A Forensic Text Comparison in SMS Messages: A Likelihood Ratio Approach with Lexical Features." They are two of the first Likelihood Ratio (LR)-based forensic text comparison studies in forensic authorship analysis. The author attribution was modelled using N-grams in the former, whereas it was modelled using so-called lexical features in the latter. In the current study, the LRs obtained from these separate experiments are fused using a logistic regression fusion technique, and the authors report how much improvement in performance the fusion brings to the LR-based forensic text comparison system. The performance of the fused system is assessed based on the magnitude of the fused LRs using the log-likelihood-ratio cost (C_{llr}). The strength of the fused LRs is graphically presented in Tippett plots and compared with those of the original LRs. The chapter demonstrates that the fused system outperforms the original systems.

Hamid Nemati
The University of North Carolina at Greensboro, USA

REFERENCES

Alderman, E., & Kennedy, C. (1997). *The right to privacy*. New York: Random House.

Ishihara, S. (2011). A forensic authorship classification in SMS messages: A likelihood ratio based approach using n-gram. In *Proceedings of the Australasian Language Technology Workshop 2011* (pp. 47-56). Academic Press.

Ishihara, S. (2012). Probabilistic evaluation of SMS messages as forensic evidence: Likelihood ration based approach with lexical features. *International Journal of Digital Crime and Forensics*, *4*(3), 47–57. doi:10.4018/jdcf.2012070104

Mason, R. O. (1986). Four ethical issues of the information age. *Management Information Systems Quarterly*, *10*(1), 4–12. doi:10.2307/248873

The Guardian. (2014). Retrieved February 21, 2014 from http://www.theguardian.com/world/the-nsa-files

U.S. Supreme court, Olmstead v. U.S., 277 U.S. 438 (1928).

Westin, A. (1967). *Privacy and freedom*. New York: Atheneum.