Preface

Cyber education continues to expand globally and includes K-12, higher education, corporate training, and government programs. The topography of conventional teaching and learning is changing rapidly as educational budgets are decreasing. In the meantime, the demand for more digitally mediated forms of education is on the rise and is forever altering the silhouette of the average student and of the traditional instructor. Once confined to physical classrooms, today’s learner connects globally for communication, entertainment, education, and information thus placing the individual in a new position that allows for the creation of an expanded identity (New Media Consortium, 2007). Part of the new online learner identity is influenced by the anonymity inherent in technology. Likewise, the identity of the instructor has changed, transforming the cyber educator’s role from a facilitator to a member of the learning community who is part of the reciprocal exchange of knowledge. Both the medium for delivery and the pedagogy for learning are changed by technologies in the digital age. Cyber education includes all online, mobile, and digitally mediated means of communication used to connect learners and engage them in the learning process.

The increased demand for cyber education calls for a heightened sense of awareness among all stakeholders of online learning programs because digitally mediated communications afford benefits as well as constraints, especially as they relate to learning. Current literature generally discusses the benefits of such communications, yet the potential tradeoffs for learners and cyber educators are seldom explored. In this manuscript, such benefits and potential tradeoffs are discussed using the terms online learning, cyber education, and digitally mediated learning interchangeably.

Technologies for mobile learning, virtual worlds, and social software among others, are providing new opportunities and increasing the options available to instructional designers, cyber educators, and learners. New approaches to education mean that concerns of anonymity, authenticity, identity, and trust will also be on the rise. In the report Learning on Demand: Online Education in the United States, 2009 Allen and Seaman (2009) concluded that at least one in every four higher education students is taking one or more online courses. Over 4.6 million students
took at least one online course during the fall 2008 term, which represents a 17 percent increase over the previous year. These numbers, however, are even higher when taking into account the increased population of K-12 online learners and the staggering increase in corporate training offered online today.

The anonymity inherent in digitally mediated communications also impacts the way learners interact in the online environment and supports the emergence of new identities. The definition of identity is no longer one-dimensional. Digitally mediated communications influence how anonymity may aid individuals to develop their online identity, and how this identity may lead to either authenticity and trust or deceit. While the sense of anonymity may free individuals to express or create a new self, the digital technologies used to enable this communication may conversely restrict free interactions and facilitate new methods of capturing, tracking, and scrutinizing data. There are legal ramifications and concerns behind this game of alter egos and emerging social mores. A close examination of the implications of anonymity in cyber education reveals how the issues of anonymity, authenticity, identity, and trust are at the center of online learning.

**CHALLENGES AND THEIR IMPACT IN CYBER EDUCATION**

The challenges and benefits of using digitally mediated communications for learning are explored in this manuscript through several theoretical lenses. This book focuses on the interactive and social nature of communications. While there are many other theoretical approaches and schools of thought that could be utilized to explore these issues, the authors chose those that they found to be most applicable to the discussion. Constructivism, connectivism, cognitivism, stakeholder theory, deindividuation theory, social presence theory, situated learning, situated cognitive theories, and activity theories are the key theoretical lenses used throughout the manuscript.

The “other side” to digitally mediated learning is the less discussed part of online learning that is challenged by cheating, authenticity, identity, and privacy issues. There is also a struggle with the reliability of sources, deception, and trust. Anonymity and issues of trust are interrelated. The secrecy and obscurity of faceless digitally mediated communications provides a sense of mystery and ambiguity. Anonymity is directly tied to privacy and identity. Learner authenticity, assessment reliability, and data security are issues most online establishments need to address more feverishly. But concerns are not limited to verifying the identity of the student, or making sure data is safe. Digitally mediated communications envelop dichotomies that suggest the safety of privacy and anonymity, yet capture and record each interaction.

The impact of anonymity and how it influences privacy is of global concern. Different countries have chosen contrasting approaches to regulating an individual.
learner’s right to privacy. Regardless, Internet users leave behind a traceable trail of
digital footprints and fingerprints that can be easily exploited, even in educational
settings. What once was said in casual conversation is now recorded via instant
messaging, blogs, wikis, and online course rooms. Data mining is a regular practice
on public servers and on the data streams connecting the Internet. Spyware is com-
monly used, hindering privacy by invading computer or mobile devices to collect
data for marketing and profiling purposes. Enormous amounts of data are mined
and sorted by companies, educational organizations, and governments alike. The
problem is that the individual may never know for what purpose or whose purpose
this information is collected.

Another challenge of anonymity is intellectual property rights. These include
intangible rights that protect the creativity and ingenuity of the human intellect. While copy rights, trademarks, patent rights, publicity rights, moral rights, and
other intellectual property rights exist, these regulations are much more difficult
to enforce online. This is complicated by anonymity because digital communica-
tion has given a voice to millions of people who can share their ideas and thoughts
under cover of a pseudonym or screen name. Likewise, intellectual property such
as instructor created materials and student projects posted in a digital environment
can unscrupulously be copied, distributed, or modified, and used as someone else’s
idea. Educational institutions even quarrel over who owns the instructor created
materials used in a course.

The anonymity provided by communicating online, the advent of open source
social software, and the fact that more individuals engage in online learning, puts
academic and personal freedom in a precarious position. Questions arise regarding
who owns the data and what privacy rights exist for learner and instructor. Aca-
demic freedom and liberty to explore alternative views without fear of retribution
is a keystone of human rights. The ultimate question of anonymity and learning
online is: can this delicate balance between anonymity, authenticity, and trust be
maintained in a digitally mediated world? The definition of privacy and “time off”
has also changed. The boundaries and limitations of a physical world with time and
space constraints are being rapidly eroded. A community that operates 24/7, 365 has
little free time. Educators and learners are both faced with a day that never ends,
and where sharing details about one’s personal life via social networking sites is
an accepted norm.

Other perils that afflict the citizens of the cyber frontier are trolling and phishing.
Trolls are individuals who intentionally post controversial or contrary messages in
an on-line community with the intention of enticing users into an argumentative
response. Many Internet users also fall victims to phishing, which is an attempt
to criminally and fraudulently acquire sensitive information, such as usernames,
passwords and credit card numbers by masquerading as a trustworthy person using
digitally mediated communications. Phishing is an example of social engineering designed to manipulate the user through deceit, and is fueled by the anonymity afforded by the online environment. Cyber education is not without risks. Trolling and phishing are examples of the many cyber threats and security breaches that affect cyber education.

Digitally mediated learning also causes many institutions to struggle with evaluation and assessment, due mainly to the anonymity factor. Technology provides new ingenious methods of cheating, and the generational views on what constitutes cheating continue to evolve. Learners have easy access to a myriad of online services that provide instant answers to just about any question. Cyber educators therefore scramble to find preventative measures that safeguard academic integrity. But integrity issues do not only point to the student; integrity involves administrators and instructors. Falsifying grades and providing special favors to elite students is part of academic fraud in online learning. The prevention of plagiarism is also a subject of much attention; however, technology also makes it possible to use countermeasures that promote academic integrity. An entire industry of anti-plagiarism software now provides services to educational institutions to compare and analyze student work.

Generally there is a growing sense of awareness and frustration with the issue of academic dishonesty in online learning programs. Online assessments raise serious issues of compliance, security, and validity. Unsatisfactory methods of deterring dishonesty jeopardized the credibility in online learning. Many programs, institutions and organizations are reluctant to trust assessments other than in classroom-proctored exams because of learner anonymity. The goal is to design for authenticity, and apply newer forms of educational technologies such as avatars and virtual worlds to not only support the learning process, but to also create new forms of assessment that place the learner in a real world scenario where critical thinking skills and new concepts must be applied.

RETHINKING AND RESHAPING CYBER EDUCATION

Cyber education must be rethought and reshaped by leveraging and balancing the two sides to digitally mediated learning. Online learning programs must be grounded in trust, which in turn must be nourished and maintained in the digital environment in order for learners to be successful. It is not until a relationship is established through repeated transactions or interactions that a person will determine if the source, technological or human, is deemed reliable and trustworthy. In digitally mediated learning, it is the responsibility of cyber educators to provide a safe learning environment for students, which includes acknowledging the need for anonymity while developing trusting relationships.
Online learning is unfortunately seen by many as a way of reaching more students at a lower cost. If organizations hastily prepare the program or take financial shortcuts, quality is sacrificed. The world of cyberspace opens up a new realm of possibilities for educators; hence, a shift in perspective is needed to create a normalized set of ethical guidelines that re-focus the attention of cyber educators and other stakeholders on student learning and not on taking shortcuts. This shift requires everyone involved in the creation and support of an online learning program to accept responsibility for his or her role and how it impacts student learning.

The Internet and emerging technologies have opened up learning possibilities and have become the main way that people get information, do business, and communicate. The question of how we govern and disseminate information in the knowledge age is a challenge to all sectors of our society, and is a global concern. A closer look leads us to ponder whether or not the “e” dimension will involve changing the way individuals engage with one another to discuss pertinent issues and access information, or whether Information Technologies will simply reinforce existing power structures around the globe, including educational institutions. The interconnected globe presents a dual challenge of transparency and privacy in communication. Various international organizations have taken the lead to not only define the terminology around e-governance, but also unite e-governments around the world in their approach to governance. The future of cyber education will undoubtedly be influenced by such definitions and approaches.

The global reach of cyber education also brings about legal challenges. Legislative efforts are suddenly insufficient because traditional boundaries are quickly vanishing. Furthermore, the advent of Web-based learning has caused educational institutions to rethink intellectual property policies, which undeniably affect intellectual rights as well as the educational product that is made available to the learner. Equality of resources, access, and learner support are important issues. Materials and resources available to traditional classroom teachers and students may not always be available to those who choose an online program. Future policies must take into consideration global concerns and needs, and must be a joint effort of the global online learning community.

Ethical standards for collecting, using, and interpreting student data are also needed. The prospective benefits of data mining and tracking digital fingerprints and footprints within e-learning platforms hint at improving distance learning programs. The growing digital trail may be used to conceptualize a person’s morality and ethics and used for any wrong purpose, but if used ethically within the virtual learning environment, it could be used to personalize learning in new ways. However, the privacy and the rights of the learner must always be respected.

People choose to behave in certain ways depending on the given situation, but also depending on their sense of identity and their prior experiences. Some indi-
individuals prefer higher levels of visibility and interaction while others desire more privacy. Learner preferences must be taken into account when designing online programs. In the online learning environment, synchronous as well as asynchronous technologies offer different options for cyber educators who seek to promote social presence and create learning communities. Research on the topic of identity and related phenomena has been limited to computer mediated communications (CMS). Current technology innovation, however, makes it necessary to add new categories to the list of ways in which individuals communicate. Digitally mediated communications (DMC), as discussed throughout the manuscript, include text messaging, instant messaging, emails, interactions using social software, Web 2.0 tools, and voice-to-voice interactions using Web-based applications. Any of these can be accessed not just from a computer, but also from various Web-enabled mobile devices. Cyber educators seeking to promote social presence as a way to enhance learning must consider all of these tools.

As cyber educators rethink the design of online learning programs, major pedagogical shifts are needed to move forward with teaching and learning in cyberspace. For example, the ethics and morality of the 21st century learner is impacted by technology and the anonymity many tools provide. Cheating and plagiarism are pervasive issues in face-to-face as well as online learning environments. Some see this as an indication of the decline of morals and ethics among young people today who may blatantly or otherwise inadvertently “borrow” from the repertoire of information available on the Internet. Others believe that it is more difficult to cheat if an online course is well designed. A diligent effort must be made to design for authenticity but also to create learner-centric environments that provide flexibility and choice of assessments.

The lines between right and wrong are often blurred, causing global concerns about academic fraud. Academic integrity must be maintained in order for institutions to keep their credentials. Institutions worldwide must use multiple strategies to ensure academic integrity. Pedagogical approaches and assessment techniques must be more authentic and reliable than ever before. More emphasis must be placed on prevention not only through course design, but also through assessment design. Assessments must mirror the real world, and require the learner to apply new knowledge. Traditional methods of assessment are inappropriate for cyber learning, and do not prepare learners to complete in a global marketplace that requires skills of collaboration, conceptual flexibility, and problem solving, among many others.

Technological advancements shape and re-define the way people communicate for work, leisure, or learning, and how they go about their day-to-day activities. Many praise technology for its ability to make things easier, but the other side of technology is that as it brings us closer together, it may also take away our ability to disconnect from our networks and retreat in privacy. Increased demands on our
time have forced us to blend our activities in order to get things done. This, too, can affect learning. The blending of work, play, and learning is inevitable, but it can be managed.

Cyber education is also likely to be transformed by highly interactive and immersive technologies and game options. Virtual environments and avatars, for example, alter social interactions, modify human behavior, and impact current methods of delivering content. Although avatars and some types of virtual environments are recent developments, their ability to deliver learning in context is already recognized by cyber educators and researchers. The benefits of recent technologies such as avatars remain largely unexplored and untapped. The question is how to develop learning environments that apply the technical and pedagogical knowledge currently available.

A virtual environment (VE) can be immersive (IVE) or collaborative (CVE). New technologies have also allowed for the emergence of sophisticated networked collaborative virtual environments (NCVEs) that connect participants in real time via a network. A VE provides synthetic sensory information about the surroundings and the content, yet it is perceived as if it was not synthetic and thus realistic to the user (Blascovich, Loomis, Beall, Swinth, Hoyt and Bailenson, 2002). The different types of VEs hold promise for individualizing instruction in new ways never accomplished before. Avatars and other embodied agents for example, can be used to modify the learner’s behavior depending on his actions, and design an individualized learning path that guides the learner toward the learning objective.

Many educators are already using new technologies to create virtual environments to foster learning through simulations and virtual games. Games today make use of strategies, simulations, role playing, sports, puzzles, inquiry, problem solving, and adventures. They have gone from single player games to Massively Multi-player Online Games (MMOGs) and Massively Multi-player Online Role Playing Games (MMORPGs). These technologies present a great opportunity for cyber educators, yet much research and empirical studies needs to be conducted to how games are and can be used to promote learning (Squire, 2003). Digital Game Based Learning (DGBL) is in essence the term used for the application of digitally mediated gaming environments for learning (Prensky, 2003). Cyber educators must continue to explore game design and acceptable pedagogy.

The global expansion of cyber education exposes the issues of trust, identity, anonymity, and authenticity. Trust is directly influenced by authenticity of learning using both synchronous and asynchronous digitally mediated communications. While it is appealing to think that technologies can provide a reliable means for delivering learning content and assessing learning, some doubts remain in the minds of the most well intentioned cyber educators. Many of these doubts are centered on the issue of assessment and the validity of results. Other doubts are related to design or
pedagogy. Nonetheless, it is critical that cyber educators explore new technologies and new pedagogical approaches. The anonymity provided by the technology is quickly diminishing; therefore, future approaches to cyber education must maintain the balance between the need for anonymity and the benefits of gathering data to individualize instruction. Approaches for reshaping cyber education must maintain the learner at the center while leveraging digitally mediated technologies to support learning.

ORGANIZATION OF THE BOOK

The book is organized into three sections with a total of twelve chapters. Each section explores a theme and the implications of digitally mediated communications in cyber education. Anonymity, identity, authenticity, and trust are the main common threads throughout the manuscript, with each chapter delving deeper into concerns, benefits, legal ramifications, as well as action items and potential solutions for the future global campus. It is guided by three relevant questions:

1. What is anonymity and why should you be concerned?
2. What is identity and how does it impact learning?
3. What are the approaches for moving forward with teaching and learning in cyber space?

Section 1: What is Anonymity and Why Should You be Concerned?

Chapter 1 discusses two different types of trust: trust in the technology and trust in the humans behind the technology. This chapter explores the problems as well as the benefits associated with anonymity, and how the concealment of identities often leads to concealment of intentions that could be exploited for the purpose of deceiving others. This chapter identifies the ethical responsibilities of cyber educators as well as learners to foster trust in digitally mediated communications through repeated meaningful and trustworthy transactions and interactions.

Chapter 2 exposes current ethical codes in global learning and proposes a shift in ethical guidelines that refocus the attention of all stakeholders in online learning programs back on the learner. This chapter discusses the challenges brought about by the rapid expansion of distance learning worldwide. It redefines the roles and ethical responsibilities of stakeholders in an online learning program, including instructors, administrators, instructional designers, and Instructional Technology
staff. It explores how the constraints of privacy, integrity, and freedom of speech influence these redefined roles.

Chapter 3 addresses the dynamics and challenges of escalating present day intellectual property concerns in a world of limited boundaries and digital anonymity. Not only have the geographical boundaries that traditionally supported legislative efforts been minimized by the online connection, the framework for intellectual property rights has been eroded in an avalanche of open source, collaborative sharing and freebies. In this chapter the mentality of “what is mine is yours and what is yours is mine” is explored in the context of how Web 2.0 technologies facilitate sharing in new ways, and the challenges associated with legislative efforts to protect intellectual property rights globally.

Chapter 4 explores the obstacles that educational institutions face in developing and managing a global campus. For the purpose of this discussion, the global campus includes all higher education as well as K-12 organizations that focus on online learning, whether private or public. This chapter also presents challenges to consider before embarking on e-governance reforms, approaches for the e-governance of the global campus, and suggestions for overcoming potential hurdles that could undermine success.

Section 2: What is Identity and How Does it Impact Learning?

Chapter 5 discusses key definitions and then explores the harms as well as the potential benefits of data mining, profiling, and tracking of digital fingerprints and footprints in digitally mediated communications. It analyzes how these same invasive technologies that are used to pry into private information could potentially be applied in cyber education for the purpose of improving distance learning programs.

Chapter 6 discusses computer mediated communications (CMS) and digitally mediated communications DMC as defined in the literature, however the authors propose using DMC as the revised definition to be used when exploring technologies used in cyber education today. The new definition includes synchronous and asynchronous collaborative tools and social networking. The chapter also raises awareness of how learning is affected by the different degree of deindividuation or individuation experienced by the learner, along with each individual’s interaction preferences and how technology enables the emergence of new identities.

Chapter 7 discusses ethics and morality in the age of digitally mediated communications that influence cheating, plagiarism, and falsification of records. It explores why students may cheat and what strategies may be set in motion by educators and administrators to minimize such behaviors. The authors propose strategies to deter and identify academic dishonesty, and methods for educational institutions to promote academic integrity among students, faculty, as well as administrators.
Chapter 8 reviews current trends in telecommuting, distance learning, and how technological advancements, especially mobile technologies have re-shaped the way individuals communicate, work, play, and learn using these technologies. The authors propose and define the term “pajama effect” to understand the phenomenon of successfully blending work, play and learning, and how the lines between private and professional lives continue to be erased by technology. The benefits and constraints of the pajama effect are discussed, as well as the potential dangers caused by the erosion of private time, thus the authors emphasize the need to manage the different roles cautiously. This chapter explores how the pajama effect influences our lives now, and how it may look in the future.

Section 3: What are Some Approaches for the Future of Teaching and Learning Using Digitally Mediated Communications?

Chapter 9 warns against mindsets that hinder the progress of education and highlights the importance of interaction in the virtual learning environment. It discusses the pedagogical shift needed to keep up with advancements in technology, especially taking into consideration the anonymity inherent in digitally mediated communications. This chapter also proposes strategies for creating engaging, meaningful virtual learning environments that are learner centric and meet the needs of the 21st century learner.

Chapter 10 differentiates between authentication and authenticity. The authors urge cyber educators to take proactive steps in the design and implementation of authentic assessments, and discuss approaches to designing for authenticity in both, synchronous and asynchronous digitally mediated learning environments.

Chapter 11 explores the possible implications of virtual environments (VEs) as they relate to the learner’s behavior and learning. The terms VE and virtual worlds are used interchangeably throughout the discussion because virtual worlds are themselves virtual environments. Immersive (IVEs) and collaborative (CVEs) as well as networked collaborative virtual environments (NCVEs) are explored in this chapter, along with the use of avatars that can transform the social interactions experienced by learners within a virtual learning community.

Chapter 12 takes a futuristic look at digital game based learning (DGBL) and discusses its possible applications as well as challenges. The word “game” is used in this chapter to discuss games in general, including Massively Multi-player Online Games (MMOGs), Massively Multi-player Online Role Playing Games (MMORPGs) and DGBL environments that promote learning. It explores the important question facing cyber educators of how to effectively use virtual games and simulations in education.
The intention of this book is to provide cyber educators, scholars, and any stakeholder of an online program with information on key issues associated with anonymity, authenticity, and trust using digitally mediated communications in cyber education. The book raises important questions and explores their implications; thus, it provides stakeholders with building blocks for further research. The information in this book will enable stakeholders to identify areas where future decisions must be made, and areas where the impact of anonymity may be felt. This manuscript evaluates both sides of each issue and presents them in a way that helps cyber educators, instructional designers, and other stakeholders understand the social, cultural, and educational implications of anonymity.

The authors wish to raise the awareness of key issues discussed in each chapter. The depth and breadth of anonymity, authenticity, and trust using digitally mediated communications in cyber education is rarely discussed among stakeholders, yet this phenomenon affects everyone: online learners, instructional designers, online instructors, administrators, lawmakers, and the general public. By gaining an understanding of the implications of these issues and how they are shaped by digitally mediated communications, the stakeholders will be better equipped to develop creative, learner-centric solutions.

REFERENCES


