Preface

In this book we will explore a number of perspectives on the ethical and privacy issues surrounding electronic surveillance in many of its forms including government surveillance of citizens, cyber-spying, and intrusions on consumer privacy by corporations. No book of this size can do adequate justice to such a wide-ranging and far-reaching subject. However, the chapters contained herein present a variety of important perspectives that will give the general reader a solid basis for understanding the many ways that e-surveillance affects her as an individual and the society as a whole. The vast majority of the book’s chapters deal examines e-surveillance using a variety of means including application of theory, philosophical critique, legal research, empirical study, and case studies. One of the chapters discusses how the fictional representation of surveillance in popular culture, namely film and television, mirrors the privacy and lack of personal control fears that have dominated postmodern societies ever since the advent of sophisticated technologies of spying in the mid-twentieth century.

The book is divided into three sections. In the first section, entitled “Theoretical Perspectives on Electronic Surveillance,” the authors apply a variety of theoretical lenses to the subject. Rebecca Fiske’s chapter, “The Borders of Corruption: Living in the State of Exception”, uses philosophical critique to examine the use of crisis during different historical periods to claim additional surveillance powers. Her chapter frames the issue theoretically within the “State of Exception” model, which she uses to analyze historical, US and precursors’, context of exceptions to rights. The chapter finds that in the name of national security, the limiting of constitutional rights, the sanctioning of torture, and the proliferating of state-sanctioned e-surveillance are fast becoming the norm. A consequence of an endless state of exception is a situation in which the executive power trumps the judiciary, and a new legal order emerges.

Tim Bagwell and Sahreka Jackson are the authors of the next chapter, “The Mode of Information—Due Process of Law and Student Loans: Bills of Attainder Enter the Digital Age”. Bagwell and Jackson apply a post-structuralist mode and model of information use in policy to examine consumer and constitutional rights in the Federal Student Loan program. As the total amount of student debt for college reaches the same stratospheric levels that eventually led to the housing market’s collapse, a great deal of political attention is finally being paid to the student loan program. This chapter contributes to the academic literature on student loans by focusing on the question of whether information use and abuse has led to a new kind of Bill of Attainder – a constitutionally guaranteed prohibition.

Using Duality Theory to Reframe E-Government Challenges is the title of the third chapter by Kathleene Hartzel and Virginia Gerde. Their work examines the conflicts and tensions of providing public services while maintaining privacy and other rights. Using duality theory as a lens for addressing the seemingly conflicting tensions found at various stages of e-government (development, implementation,
and adoption), they apply duality theory for its agility in the management of organizational and management paradox. The chapter analyzes the five dimensions of the duality of e-government challenges and argues that reframing contradictory objectives as dualities can enhance e-government’s effectiveness.

The final chapter in the theoretical section is “Who Screens Security—Cultures of Surveillance” by Vince Casaregola. Dr. Casaregola argues that science fiction films predicted the rise of the surveillance state in the early postwar era and the panoptic society has become a reality as a result of electronic surveillance.

The second section and the largest one in the book are titled “Ethical Issues, Privacy, and Electronic Surveillance”. The chapter that starts the section is “Reconciling Needs for National Security by Kenneth Hacker and Bridget Acquah-Baidoo. Their chapter examines the dialectic of security and privacy within the context of the national security debate and the framework of policy changes. They propose a model for surveillance and privacy debates including eight key issues and questions. In their extensive review of the history of security and surveillance, they summarize in an overlapping diagram the issues of freedom, surveillance and expectations of privacy.

Sam Edwards’ provocatively titled “The Right to Privacy is Dying: Technology is Killing It and We Are Letting It Happen” begins with an extensive review of the origins and establishment of privacy rights. He then takes us through the complex interpretation of privacy rights in a technological era. The chapter culminates in the review of “see-through” surveillance technology and the growing demand of law enforcement to unleash its use, to the detriment of individual freedoms.

The theme of personal liberties coming under assault from new technologies of surveillance is continued by Garry Robson and C.M. Olvarria in “Big Collusion: Corporations, and the Digital Surveillance”. Robson and Olvarra re-introduces us to the Snowden case in the context of cooperation “collusion” between government agencies such as the NSA and a range of corporations including telecom providers and Internet-based companies such as Google. They present a “trifecta” model that includes consumer participation in the process with notable treatment of the “Terms & Conditions” agreement that most consumers accept as perfunctory. They end the chapter by examining the possibility of breaking the cycle of consumer participation and corporate surveillance.

Neil Rowe continues the focus on law enforcement that began with Edwards. His chapter, “Privacy Concerns with Digital Forensics” provides extensive insights into the law enforcement dimension of digital forensics. He presents a nine-point list and model of privacy concerns related to digital forensics, many hinging on the interpretation of data. Finally he recommends procedures for individual protection of private information especially on digital media and accounts controlled by the consumer.

The notion of achieving some sort of balance between the security needs of governments and corporations with the private liberties of individuals is taken up by Ordor Ngowari Rosette, Fatemeh Kazemeyni, Shaun Aghili, and Ron Ruhl. They examine the issue of employer (corporate) surveillance of employee data behaviors (dataveillance) and frame the issue in terms of “big data.” Rosette, et al., review privacy frameworks and the current status of proposals to control corporate dataveillance, by focusing on Australian and Canadian contributions in this area.

The theme of government, corporate, hacker and personal forms of cyber espionage toward consumers and citizens is taken up by Mohamed Firdhous in “Cyber-espionage: How Safe Are We?” Firdhous reviews and examines many of the technical avenues open to surveillance and left open by consumers for possible attack. He concludes his chapter with a series of recommendations about how individuals can avoid being the victims of cyber-espionage.
The section’s final chapter, “E-Government Surveillance in the United States: Public Opinion on Wiretapping Powers” by Ramona McNeil, Mary Schmeida, and Justin Holmes, presents the findings of their empirical research study of public perception of wiretapping, pre- and post- Snowden. They begin by reviewing the history and development of wiretapping authority in the U.S. Their study utilizes a Right Wing Authoritarianism scale to index public opinions on the topic and its many dimensions.

The book concludes with a section of individual case studies from both the U.S. and abroad that deal with issues of electronic surveillance, titled “Case Studies of E-Surveillance.” Kirstin Loutzenhisser’s contribution is titled “Public Administrators, School Safety and Forms of Surveillance: Ethics and Social Justice in the Surveillance of Students with Disabilities”. She takes up the important issue of school surveillance of students with disabilities, which has received far less academic attention than it deserves. Loutzenhisser uses the Exceptional Student Education (ESE) and Individuals with Disabilities Education Act (IDEA) as the Federal policy context of surveillance of students with disabilities. In her case study, Loutzenhisser reviews cases of student death and endangerment from lack of surveillance. The chapter concludes with a call for methods to balance surveillance with needs for safety.

The next two case studies, which conclude this book, extend the analysis of electronic surveillance to developing countries. Not surprisingly, similar issues appear in countries as diverse as Mexico and Malaysia. “E-Government, E-Surveillance and Ethical Issues from Malaysian Perspective by Maslin Masrom reviews the status of e-government in Malaysia. The author examines forms of surveillance as utilized by Malaysian authorities. Masrom delves extensively into many electronic and digital surveillance and storage processes authorized by the government and the regulation of those processes. Finally, the author applies a model of public policy development, law and surveillance as related to the Malaysian experience.

Government and corporate surveillance, facilitated by current and emerging technology, is commonplace today. The authors of the chapters in this book find that current laws are struggling to keep up with practices that place in peril many of the basic human rights that we take for granted in the U.S. and elsewhere. Rather than meek surrender to the inevitable, however, several authors recommend solutions or point in the direction of possible alternatives both at the individual and societal levels. It is the editors’ sincere hope that this volume will contribute to an important debate over the boundaries and limits of responsible e-surveillance, balancing the needs of society in an uncertain global political environment with personal liberty and fundamental human rights.