PREFACE: PLAN AND PURPOSE OF THE BOOK

Today's business clients present a mix of traditional business matters and questions about cybersecurity liability. How should a future business lawyer prepare to address the cybersecurity issues? This book answers that question.

A CASELAW APPROACH

Organized around three central themes, our answer is a traditional one. The traditional, proven-effective way to teach law students presents doctrinal and policy issues in the concrete setting of specific cases. Accordingly, this book provides a collection of thematically organized cases supplemented by hypotheticals, notes, and questions that illuminate key features of the cases and explore the relevant policy issues. Additionally, "Technology Notes" throughout the book offer accessible explanations of the technological facts and assumptions that arise in and, in some instances, underlie the cases. This allows a future business lawyer to acquire not just an understanding of the relevant technology, but also an understanding of the roles that technology plays in judicial decisions.

A DISTINCTIVE SET OF CYBERSECURITY ISSUES

This book focuses on a distinctive set of *cybersecurity* issues and is organized around three central themes:

- *Liability for failure to prevent access to a computer or network*—covering torts, contracts, selected Wiretap Act issues, as well as compliance liability from agency action and related statutes.
- *Liability for accessing a computer or network*—covering the common law of trespass, selected Wiretap Act issues, and the Computer Fraud and Abuse Act.
- *Rights protecting against the seizure of data by the government*—covering the Fourth and Fifth Amendment issues that arise when the government seeks to seize and examine data.

Chapter 1 introduces students to the foundational principles necessary for understanding the subjects examined in the rest of the book. This chapter

covers the definitions of a computer, a network, and access to a computer. It also provides an introduction to the attack and defense of computers and networks as well as an introduction to risk assessment and cyber insurance.

WHO IS THIS BOOK FOR?

Motivated in part by conversations with practicing attorneys, the inspiration for this book is the recognition that there is a widespread need and demand for future business lawyers with a case-centered understanding of basic cybersecurity law. This book aims to provide those future business lawyers with the cybersecurity basics they need, and, for those law students who wish to become cybersecurity experts, this book is a first step toward achieving that goal. Developing expertise as a cybersecurity specialist requires, among other things, more detailed and extensive technical knowledge than this book provides as well as an understanding of how to deal with post-cyberattack forensics and governmental investigations—all subjects beyond the scope of this book. Such specialists would also need a deeper knowledge of at least some areas of law covered in depth by other substantive law courses—administrative law, for example—and a more through grounding in statutory requirements.

THE TECHNOLOGY NOTES

The Technology Notes following cases are a unique feature of the book. Written by the computer scientist of the three-author team, they illuminate the relevant technological facts and issues while still being accessible to students who lack technological expertise. The combination of cases and technology equips students to respond effectively to the problems they will encounter in practice as advocates or policy makers.

WHY WE INCLUDE IN-DEPTH EXAMINATION OF THE COMPUTER FRAUD AND ABUSE ACT

Why does the book cover the Computer Fraud and Abuse Act (CFAA), a "criminal" statute? Because it is not just a criminal statute. It is a hybrid statute whose substantive provisions are the basis for criminal prosecutions *and* for seeking civil remedies.

Analysis of the reported cases shows that the CFAA the CFAA's various provisions provide remedies for a broad swath of commercial misconduct ranging from theft of trade secrets and proprietary information to cyber trespass. Importantly, in its use in civil cases, the CFAA serves as a uniform set of statutes that provides a broad base of civil remedies nationwide. By contrast, the actions in tort, contract, and equity cases, which this book discusses, are all state-law based, and their availability and basis can differ from state to

state. Further, because of the *Erie* doctrine, they remain state law based when brought in federal court.

WHY WE INCLUDE THE FOURTH AND FIFTH AMENDMENTS

A future business lawyer's defense of data includes defense against non-consensual government intrusions. To that end we include examination of Fourth and Fifth Amendment principles as they apply to the seizure of data by government agents. The book does not provide a comprehensive discussion of all Fourth and Fifth Amendment law, but instead is limited to the Fourth and Fifth Amendment principles that are implicated when the government seeks to obtain data without the consent of the possessor of that data. The following example illustrates why understanding those principles is important for the future business lawyer.

Imagine the owner of a medium-sized business has been served with a grand jury subpoena requiring the production of encryption keys or records; or, more intrusively, that government agents appear at the business to execute a search warrant of the business's computers. In need of immediate advice, the owner calls the lawyer the owner regularly uses for the mix of business and technology legal issues that the owner encounters as part of day-to-day business operations. The lawyer needs to have enough of an understanding of the Fourth and Fifth Amendments to respond competently.

In addition, the Fourth and Fifth Amendments raise issues about government power of considerable interest to students drawn to cybersecurity.