Economic Espionage and Industrial Spying

In view of the recent revolution in information technology, this book investigates the current state of industrial espionage, showing the far-reaching effects of advances in computing and wireless communications. Synthesizing views from leading national and international authorities, Professor Hedieh Nasheri explains the historical and conceptual underpinnings of economic espionage, trade secret theft, and industrial spying. She shows how these activities have impacted society, and she tracks the legislative and statutory efforts to control them.

Advance Praise for Economic Espionage and Industrial Spying:

“We criminologists and academic criminal lawyers have been slow to turn our attention to non-traditional crimes and criminals, thereby missing extraordinarily important developments. Hedieh Nasheri has given us a wake up call. Her work on theft of intellectual property should be incorporated into our courses and research agendas.”

– James B. Jacobs, New York University

“Hedieh Nasheri skillfully shows us the dimensions of economic espionage in this era of ever increasing interconnectedness and globalization. She provides a fascinating account of the criminalization of economic espionage, and offers a compelling analysis of the impact and possible evolution of important criminal statutes. Her book also raises complex issues about the use of criminal sanctions in an electronic environment, making it required reading for anyone studying or fighting cyber crime today.”

– Alan J. Lizotte, The University at Albany

“This is a fascinating and timely account of the ways in which new technologies are being employed to steal information in twenty-first century America. It provides a carefully-researched analysis of the appropriateness and effectiveness of criminalization of economic espionage, particularly under the Economic Espionage Act 1996, and considers alternative approaches that may yield greater benefits in terms of prevention and deterrence. An essential reference work for cyber-criminologists and corporate regulators in the information age.”

– Russell G. Smith, Australian Institute of Criminology

Hedieh Nasheri is Associate Professor of Justice Studies at Kent State University.
Economic Espionage and Industrial Spying

Hedieh Nasheri
Kent State University
To my parents
Contents

Preface xi
Acronyms and Abbreviations xv

1. Dimensions of Economic Espionage and the Criminalization of Trade Secret Theft 1

2. Transition to an Information Society – Increasing Interconnections and Interdependence 30

3. International Dimensions of Business and Commerce 49

4. Competitiveness and Legal Collection Versus Espionage and Economic Crime 72

5. Tensions Between Security and Openness 95


7. Multinational Conspiracy or Natural Evolution of Market Economy 170

Appendix A 185
Appendix B 189
Appendix C 190
Preface

The idea for this book developed in October 1996 on the eve of the passage of the Economic Espionage Act (EEA) in discussions with a colleague who specialized in intellectual property law and had been practicing for some 15 years, litigating patents, trade secrets, and infringement cases domestically and internationally in this area. We engaged in an ongoing debate with respect to factors that had contributed to the passage of this new legislation. Our discussions were fruitful because we each had unique perspectives, mine from an academic social science background and his from a practitioner’s legalistic point of view dealing with these issues, not on an abstract level, but rather day in and out handling disputes among corporate entities.

I began analyzing and interpreting the legislative actions at both state and federal levels regarding past and postcriminalization efforts. Accordingly, the objective was to examine the available records on legislative evolution and legislative history that gave rise to the enactment of this statute and Congress’ initiatives. I systematically began reviewing and tracing all prosecutions brought to date under the EEA legislation. Furthermore, I began examining the impact of this law in the United States and related legal regimes in Central and Eastern Europe as well. My project in Central Europe was made possible through a research grant from the State Department of the United States, which provided me with an opportunity to analyze this topic from a comparative perspective in order to gain a better understanding of what some European countries were doing with respect to these issues and their potential impact on western nations. This analysis, however, is still evolving and is not within the scope of the materials presented in this book.

For a number of years, I have been in close contact and collaboration with government officials in the Department of Justice, Federal Bureau of Investigation, who play key roles in prosecution and investigation of these
criminal activities under the EEA, as well as members of the private sector. Furthermore, members of the law enforcement and prosecutorial community were queried regarding their activities related to these types of crimes. This provided an enriching opportunity for understanding the enforcement initiatives that have been taking place in the United States in the past and the present.

The criminalization of trade secret theft raises several important implications for future research and theorizing about the formation of laws at national and international levels. However, any opinions, findings and conclusions, or recommendations expressed in this book are those of the author and do not necessarily reflect the views of any government officials or granting entities.

My research results for the past 10 years have addressed the trends in criminal activities in connection with the rapid growth of computing and communications technologies and the increasingly global nature of commerce and business, both of which have caused an increase in technologically sophisticated criminal activity as well as international economic espionage. My work has concentrated on issues related to economic and industrial espionage. My research has revolved around the following question: Should the taking of information be criminalized as it has been in the United States by the EEA? The U.S. Congress enacted the EEA in 1996, which meant to establish a comprehensive approach to economic espionage, facilitating investigations and prosecution. This enactment raises complex issues about the use of criminal sanctions and civil penalties in the rapidly changing world of technology. Federal criminal prosecution is a powerful weapon, and one that should not be taken lightly. Criminal penalties imposed for the misappropriation of trade secrets under the EEA are far more severe than any other criminal liability for violations of other intellectual property rights. Persons engaged in misappropriation in the United States will no longer have their liability limited to civil remedies and damages imposed for such misconduct.

Economic espionage can be characterized as a new form of white-collar crime that includes technology-related crimes and/or cybercrimes. It has been argued that this will be a defining issue of the twenty-first century for policy makers – as defining as the Cold War was for the twentieth century. My work concentrates on issues related to technology changes. For example, the Internet itself provides opportunities for various kinds of theft, ranging from online banks to intellectual property. However, it also offers new means of committing old crimes, such as fraud, and offers new vulnerabilities relating to communications and data that provide attractive targets for extortion, a crime that has always been a staple of criminal organizations. The synergy between organized crime and the Internet is not only very natural, but it is also likely to flourish and develop even more in the future. The Internet provides
both channels and targets for crime and enables them to be exploited for considerable gain with a very low level of risk. For organized crime figures and white-collar criminals, it is difficult to ask for more.

This topic has generated debate among policy makers, the courts, lawmakers, and the intelligence community worldwide. Criminologists, however, acknowledge that economic espionage is an important topic in the context of cybercrimes and transnational crimes, but very few have even addressed crimes that arise out of electronic communications such as economic espionage. Peter Grabosky points out that the basic principles of criminology apply to computer-related crime no less than they do to bank robbery or to shoplifting. As James Finckenauer pointed out, the whole panoply of so-called cybercrimes are almost by definition transnational crimes because cyberspace is not constrained within borders. Accordingly, Finckenauer noted that ignoring the transnationalization of crime would be akin to adopting a “head in the sand” strategy. Criminologist David Wall asserted that criminologists have been slow to explore these emerging fears and new criminal behaviors, and to engage in debate about them in order to develop useful bodies of knowledge that could enlighten the public and provide the basis for informed policy. In the criminologists’ defense, however, Wall argued that there is wisdom in exercising caution and in waiting for reliable trends of behavior to emerge. He further pointed out that the time has arrived to address these issues. Most recently, Peter Drahos and John Braithwaite argued against expansion of intellectual property rights as a form of “information feudalism” that entrenches economic inequalities. They chronicle examples that, in their view, show an improper balance being struck between individual property rights in knowledge and the interests of society. It is inevitable that social scientists, including criminologists, economists, political scientists, and the like, will need to analyze and address these topics.

My book is designed to provide an analytic overview and assessment of the changing nature of crime in the burgeoning information society, where significant technological advances have revolutionized the nature of criminal activity across national borders, and increasing interconnections and interdependence have created new risks. Bringing together views from leading national and international authorities, it explains the historical and theoretical background surrounding issues of economic espionage, trade secret theft and industrial spying, and its impact on society. It looks at legislative history, the progression of electronic and corporate criminal behavior by introducing the concept of information theft and computer crimes, exploring its definition, its identification, and its development within criminology.

Currently, no countries have enacted legislation similar to the EEA of the United States. The most basic question that Congress and the EEA face is to what extent the legislation will extend in “extraterritorial” application. The book examines issues such as whether expansive extraterritorial legislation
will likely irritate many countries, including those that are not involved in
the theft of sensitive materials. One of the main objectives of the book is to
lay out the legislative initiatives that the United States has taken to combat
criminal activities that fall under the EEA. I hope that discussions on these
and related issues will provide insight for legislatures and policy makers in
other countries to examine similar issues that they encounter and to provide
them with some basis for assessment of their existing laws or lack thereof.

The research for this book was made possible, in part, by a grant from
the International Center at the National Institute of Justice on intellectual
property as part of its research agenda on transnational crime, and through
a Research Fellowship at the Institute of Advanced Legal Studies (IALS)
at the University of London. The institute’s reputation and emphasis on
economic crime and commercial criminal law were an ideal match for my
research agenda and interest. I want to acknowledge, too, the help of a num-
ber of people and institutions. I want to thank the anonymous reviewers for
their helpful comments on the preliminary draft of this project. Special
thanks go to the staff at the IALS Library at the University of London for
providing assistance with research materials and I thank Kent State Univer-
sity for allowing me the time for my research in the U.K. I am indebted to my
colleagues Jay Albanese, James Finckenauer, Peter Grabosky, Henry Pontell,
and David Wall for their expertise, insight, and support as this manuscript
was progressing. Finally, I am grateful to David Farrington whose guidance
and encouragement was invaluable in shaping my thinking.
Acronyms and Abbreviations

ARPA  Advanced Research Projects Agency
ASIS  American Society of Industrial Security
CCIPS  Computer Crime and Intellectual Property Section
CERT/CC  Computer Emergency and Response Team Coordination Center
CFAA  Computer Fraud and Abuse Act
CHIP  Computer Hacking and Intellectual Property
CIA  Central Intelligence Agency
COE  Council of Europe
CSI  Computer Security Institute
CSIS  Canadian Security Intelligence Service
DCI  Director of Central Intelligence
DHS  Department of Homeland Security
DIS  Defense Investigative Service
DoD  Department of Defense
DOE  Department of Energy
DSS  Defense Security Service
EC  European Commission
ECFA  Electronic Communications Privacy Act
FOIA  Freedom of Information Act
GATT  General Agreement on Tariffs and Trade
IFCC  Internet Fraud Complaint Center
ITSPA  Interstate Transportation of Stolen Property Act
MID  Military Intelligence Department
NACIC  National Counterintelligence Center
NAFTA  North American Free Trade Agreement
NCCS  National Computer Crime Squad
NIPC  National Infrastructure Protection Center
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>NSPA</td>
<td>National Stolen Property Act</td>
</tr>
<tr>
<td>OECD</td>
<td>Organization for Economic Cooperation and Development</td>
</tr>
<tr>
<td>OIA</td>
<td>Office of International Affairs</td>
</tr>
<tr>
<td>SCIP</td>
<td>Society of Competitive Intelligence Professionals</td>
</tr>
<tr>
<td>SEC</td>
<td>Securities and Exchange Commission</td>
</tr>
<tr>
<td>TRIPS</td>
<td>Trade-Related Aspects of Intellectual Property Rights</td>
</tr>
<tr>
<td>UTSA</td>
<td>Uniform Trade Secrets Act</td>
</tr>
<tr>
<td>WIPO</td>
<td>World Intellectual Property Organization</td>
</tr>
<tr>
<td>WTO</td>
<td>World Trade Organization</td>
</tr>
</tbody>
</table>