

PROSECUTING COMPUTER CRIMES

Computer Crime and
Intellectual Property Section
Criminal Division

Michael Battle
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE Litigation Series

Ed Hagen
Assistant Director,
OLE

Scott Eltringham
Computer Crime
and Intellectual
Property Section
Editor in Chief



Published by
Office of Legal Education
Executive Office for
United States Attorneys

The Office of Legal Education intends that this book be used by Federal prosecutors for training and law enforcement purposes, and makes no public release of it. Individuals receiving the book in training are reminded to treat it confidentially.

The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. See *United States v. Caceres*, 440 U.S. 741 (1979).

Table of Contents

Preface and Acknowledgements	v
Chapter 1. Computer Fraud and Abuse Act	1
A. Key Definitions.....	3
B. Obtaining National Security Information.....§ 1030(a)(1).....	10
C. Compromising Confidentiality.....§ 1030(a)(2).....	15
D. Trespassing in a Government Computer.....§ 1030(a)(3).....	19
E. Accessing to Defraud and Obtain Value.....§ 1030(a)(4).....	22
F. Damaging a Computer or Information.....§ 1030(a)(5).....	29
G. Trafficking in Passwords.....§ 1030(a)(6).....	46
H. Threatening to Damage a Computer.....§ 1030(a)(7).....	49
I. Legislative History.....	51
Chapter 2. Wiretap Act	55
A. Intercepting a Communication.....§ 2511(1)(a).....	56
B. Disclosing an Intercepted Communication.....§ 2511(1)(c).....	63
C. Using an Intercepted Communication.....§ 2511(1)(d).....	66
D. Statutory Exceptions.....	67
E. Defenses.....	74
F. Statutory Penalties.....	74
Chapter 3. Other Network Crime Statutes	77
A. Unlawful Access to Stored Communications§ 2701.....	77
B. Identity Theft.....§ 1028(a)(7).....	84
C. Aggravated Identity Theft.....§ 1028A.....	85
D. Access Device Fraud.....§ 1029.....	85
E. CAN-SPAM Act.....§ 1037.....	86
F. Wire Fraud.....§ 1343.....	90
G. Communication Interference.....§ 1362.....	91

Chapter 4. Special Considerations	93
A. Jurisdiction.....	93
B. Venue.....	95
C. Statute of Limitations.....	99
D. Juveniles.....	99
Chapter 5. Sentencing	109
A. Base Offense Levels.....	109
B. Adjustments Under Section 2B1.1.....	110
C. CAN-SPAM Act.....	121
D. Wiretap Act.....	121
E. Generally-Applicable Adjustments.....	122
F. Conditions of Supervised Release.....	124
Appendices	
A. Unlawful Online Conduct and Applicable Federal Laws.....	127
B. Best Practices for Working with Companies.....	135
C. Best Practices for Victim Response and Reporting.....	139
D. Network Crime Resources.....	147
Index	151

Preface and Acknowledgements

This manual is a product of the Computer Crime and Intellectual Property Section (CCIPS) of the United States Department of Justice. Just as in *Searching and Seizing Computers and Electronic Evidence* (2d ed. 2002) and *Prosecuting Intellectual Property Crimes* (3d ed. 2006), we emphasize real world practice issues for working prosecutors.

This manual examines the federal laws that relate to computer crimes. Our focus is on those crimes that use or target computer networks, which we interchangeably refer to as “computer crime,” “cybercrime,” and “network crime.” Examples of computer crime include computer intrusions, denial of service attacks, viruses, and worms. We make no attempt to cover issues of state law and do not cover every type of crime related to computers, such as child pornography or phishing.

We refer to people committing the crimes covered in this manual as “intruders” or “attackers” instead of the more widely-used but less-specific term “hackers.”

This manual is a joint effort of the Computer Crime team of CCIPS, under the supervision of Martha Stansell-Gamm, Chief, and Christopher Painter, Principal Deputy Chief. Scott Eltringham is the primary editor, but this manual exists because of the work and experience of many CCIPS attorneys, both present and former, including Leonard Bailey, Howard Cox, Richard Downing, Tom Dukes, Josh Goldfoot, Jessica Herrera, Todd Hinnen, Amanda Hubbard, Nathan Judish, Kimberly Peretti, Richard Salgado, Jared Strauss, Joel Schwarz, Betty Shave, Joe Springsteen, Michael Stawasz, Michael Sussmann, Anthony Teelucksingh, Eric Wenger, Lisa Willmer, and William Yurek, paralegals Kathleen Baker and Aubrey Rupinta, as well as many of our legal interns.

We are grateful to Ed Hagen, Nancy Bowman, and others at the Office of Legal Education for their assistance in publishing this manual.

This manual is intended as assistance, not authority. The research, analysis, and conclusions herein reflect current thinking on difficult and dynamic areas of the law; they do not represent the official position of the Department of Justice or any other agency. This manual has no regulatory effect, confers no rights or remedies, and does not have the force of law or a U.S. Department of Justice directive. See *United States v. Caceres*, 440 U.S. 741 (1979).

If you have questions about anything in this manual, we invite you to call CCIPS at (202) 514-1026. Attorneys are on duty every day for the specific purpose of answering such calls and providing support to U.S. Attorneys' offices, law enforcement agencies, and other public- and private-sector partners.

Electronic copies of all three of our manuals are available at <http://www.cybercrime.gov>. The electronic version will be periodically updated, and prosecutors and agents are advised to check the website for the latest developments.

John T. Lynch, Jr.
Deputy Chief
Computer Crime & Intellectual Property Section
Criminal Division
Department of Justice