Table of Contents

Volume 1

PART I. LEGISLATION AND DEFINITIONS

CHAPTER 1. BACKGROUND AND OVERVIEW; MESSAGES TO OUR READERS

I. BACKGROUND
   A. OVERVIEW
      § 1:1 Introduction
      § 1:2 The Fourth Amendment
   B. APPLICATION OF THE FOURTH AMENDMENT TO WIRETAPPING AND EAVESDROPPING
      § 1:3 1928–1964
      § 1:4 Berger and Katz
      § 1:5 Procedural and conceptual difficulties
   C. APPLICATION OF THE FOURTH AMENDMENT TO OTHER SURVEILLANCE TECHNOLOGY
      § 1:6 Visual surveillance and its equivalents
      § 1:7 New surveillance technology—1 [Reserved]
      § 1:8 New surveillance technology—2 [Reserved]
      § 1:9 New surveillance technology—3 [Reserved]

II. LEGISLATIVE PROTECTION OF AND REGULATION OF INTERCEPTION OF COMMUNICATIONS
   § 1:10 Title III

© 2018 Thomson Reuters, 12/2018
§ 1:11 Scope and reach of Title III
§ 1:12 —Oral communications
§ 1:13 National Wiretap Commission report and studies
§ 1:14 Foreign Intelligence Surveillance Act of 1978
§ 1:15 Electronic Communications Privacy Act (ECPA); the “Stored Communications Act”
§ 1:16 Communications Assistance for Law Enforcement Act of 1994 (CALEA)
§ 1:17 USA PATRIOT Act of 2001
§ 1:18 —Compensation provision
§ 1:19 —Legislative history
§ 1:20 USA PATRIOT Improvement and Reauthorization Act of 2005 (“USAP-IRA”)
§ 1:21 The “Protect America Act” of 2007
§ 1:22 State statutes

III. LEGISLATION RELATING TO COMPUTERS
§ 1:23 Federal computer legislation
§ 1:24 State computer legislation

IV. SPECIAL MESSAGES
§ 1:25 To prosecutors
§ 1:26 To police supervisors
§ 1:27 To defense attorneys
§ 1:28 To civil practitioners
§ 1:29 To family law practitioners
§ 1:30 To attorneys for employers
§ 1:31 To judges and their law clerks

CHAPTER 2. STATUTORY AND OTHER DEFINITIONS

I. INTRODUCTION
§ 2:1 In general

II. “WIRE COMMUNICATION” AND RELATED TERMS
   A. DEFINING “WIRE COMMUNICATION”
§ 2:2 Background

xx
### Table of Contents

| § 2:3 | “Wire communication”: 18 U.S.C.A. § 2510(1) |
| § 2:5 | “Switching stations” |
| § 2:6 | Deletion of “common carrier” |
| § 2:7 | “Wire, cable, or other like connection” |
| § 2:8 | Wire communications and the expectation of non-interception |
| § 2:9 | Other issues relating to the definition of “wire communication” |
| § 2:10 | State variations on the federal definition |

#### B. APPLICATION TO SPECIFIC SYSTEMS OR EQUIPMENT

1. Cordless phone calls
   - § 2:12 Federal law: 1994 to present
   - § 2:13 State law
   - § 2:14 Summary

2. Electronic Pagers
   - § 2:15 In general
   - § 2:16 “Tone-only” pager
   - § 2:17 Alphanumeric pager
   - § 2:18 “Tone and voice” pagers

3. Other systems or equipment
   - § 2:19 Cellular phone calls
   - § 2:20 Private networks and intracompany communications systems: “Communications affecting interstate or foreign commerce”
   - § 2:21 “Electronic storage,” i.e. stored voice mail

#### III. “ORAL COMMUNICATION”

#### A. STATUTORY DEFINITION AND CONSTITUTIONAL PRINCIPLES

- § 2:23 Nexus to interstate commerce
- § 2:24 Expectation of non-interception
- § 2:25 Comparing “reasonable expectation of privacy” and “justifiable expectation of non-interception”

© 2018 Thomson Reuters, 12/2018
B. EVALUATING THE EXPECTATION OF NON-INTERCEPTION

1. In General

§ 2:42 Relevant factors
§ 2:43 Expectation against whom?
§ 2:43.50 “Oral communication” and “pocket-dialing”

2. Nature of conversation or conduct intercepted

§ 2:44 In general
§ 2:45 Questioning by public officials
§ 2:46 Blatantly criminal behavior

3. Location of communication

§ 2:47 Consensual interceptions in suspect’s home
§ 2:48 Hotel room bug
§ 2:49 “Open fields”
§ 2:50 Public and semi-public meetings and events
§ 2:51 Consent by owner: Alderman v. U.S.
§ 2:52 Eavesdropping by owner: residential premises
Table of Contents

§ 2:53 Eavesdropping by owner: commercial premises
§ 2:54 Police car intercepts
§ 2:55 Miscellany

  4. Public officials’ expectations of non-interception

§ 2:56 In general
§ 2:57 Civilian’s interception of his conversation with public official
§ 2:58 Officer’s recording his being interrogated by others
§ 2:59 Conversations between public officials (no consenting participant)
§ 2:60 Civilian’s video or audio interception of public officials engaged in performance of public duties

IV. INTERCEPT; CONTENTS

A. “INTERCEPT”: THE STATUTORY DEFINITION

§ 2:62 “Intercept” and “record”: view that to record what one can lawfully hear is not an “interception”
§ 2:63 Why this view misconstrues Title III
§ 2:64 Overhearing with the “unaided ear”: constitutional principles
§ 2:65 The “unaided ear” doctrine and the listener’s location
§ 2:66 Application of “unaided ear” doctrine to the definition of “intercept”
§ 2:67 State variations on the definition of “intercept”

B. LOCATION OF INTERCEPTION

§ 2:68 In general
§ 2:69 Interceptions pursuant to interception orders
§ 2:70 Cellular and other mobile phones
§ 2:71 Consensual interceptions across state lines
§ 2:72 Other state law issues

C. OTHER ISSUES RELATING TO THE DEFINITION OF “INTERCEPTION”

§ 2:73 Electronic communications
§ 2:74 Unauthorized access to a restricted web site
§ 2:75 Other issues and holdings

D. “CONTENTS”
§ 2:76 18 U.S.C.A. § 2510(8)
§ 2:77 Additional issues relating to definition of “contents”

V. “ELECTRONIC, MECHANICAL, OR OTHER DEVICE”

A. IN GENERAL
§ 2:81 State variations
§ 2:82 Specialized monitoring or recording equipment
§ 2:83 Which component is the “interception device”
§ 2:86 § 2510(5)(a)(ii) exceptions: law enforcement officers; “ordinary course”

B. APPLICATION TO SPECIFIC EQUIPMENT
1. Telephones
§ 2:87 In general

2. Extension phones
§ 2:88 In general
§ 2:89 Use without the consent of a participant
§ 2:90 Use with the consent of a participant
§ 2:91 Modified by user
§ 2:92 Extension phones and the “law enforcement exemption” of 18 U.S.C.A. § 2510(5)(a)(ii)

3. Other equipment
§ 2:93 Conference calls
§ 2:94 Speaker phones
C. PROHIBITED DEVICES AND ADVERTISING

1. In general

§ 2:100 18 U.S.C.A § 2512
§ 2:101 Devices; advertising; commerce
§ 2:102 Culpable mental states; exceptions

2. “Primarily useful”

§ 2:103 In general
§ 2:103.10 “Surreptitious”
§ 2:104 Legislative history; applicability to consensual surveillance equipment
§ 2:105 Rejecting vagueness challenges
§ 2:106 Discriminatory prosecution
§ 2:107 A pseudo-defense

3. Particular devices and issues

§ 2:108 CATV and subscription radio descramblers
§ 2:109 Illegal advertising
§ 2:110 Miscellany

VI. CULPABLE MENTAL STATES

A. “WILLFULLY”

§ 2:111 “Willfully”—In general
§ 2:112 Defining “willfully”
§ 2:113 Defining “willfully” as “conscious or reckless disregard of the law”
§ 2:114 Defining “willfully” as “bad purpose, evil motive”; “purposely”
§ 2:115 Defining “willfully” as “intentionally”

B. “INTENTIONALLY”

§ 2:116 In general
§ 2:117 Inadvertent interceptions

© 2018 Thomson Reuters, 12/2018
§ 2:118 Intention and motive
§ 2:119 Jury instruction

C. “KNOWING OR HAVING REASON TO KNOW”

§ 2:120 In general
§ 2:121 Applicability to attorneys
§ 2:122 Instructing the jury

VII. OTHER BASIC DEFINITIONS

§ 2:125 “Investigative or law enforcement officer”: 18 U.S.C.A. § 2510(7)
§ 2:129 “Foreign intelligence information”

VIII. DEFINITIONS RELATING TO ELECTRONIC COMMUNICATIONS

§ 2:130 In general

A. ELECTRONIC COMMUNICATION

§ 2:132 The § 2510(12) exceptions
§ 2:133 Radio communications
§ 2:134 47 U.S.C.A. 605(a) (the Communications Act)
§ 2:135 Miscellany

B. OTHER RELATED DEFINITIONS

§ 2:139 “Readily accessible to the general public”: 18 U.S.C.A. § 2510(16); 18 U.S.C.A. § 2511(2)(g)
TABLE OF CONTENTS

§ 2:140 Alphanumeric display pagers
§ 2:142 “Remote computing service”: 18 U.S.C.A. § 2711(2)
§ 2:143 “Protected computer”: 18 U.S.C.A. § 2510(20)

IX. CALEA DEFINITIONS

§ 2:145 Introduction
§ 2:146 “Call-identifying information”: 18 U.S.C.A. § 1001(2)
§ 2:147 “Electronic messaging services”: 18 U.S.C.A. § 1002(4)
§ 2:149 “Telecommunications support services”: 18 U.S.C.A. § 1001(7)
§ 2:151 Other definitions: 18 U.S.C.A. § 1000(3), (5)

X. TERMS RELATING TO THOSE COMPELLED TO COOPERATE WITH GOVERNMENT AGENTS IN THE EXECUTION OF INTERCEPT ORDERS

§ 2:152 In general: 18 U.S.C.A. § 2518(4)
PART II. STATUTORY PROTECTION OF WIRE, ORAL AND ELECTRONIC COMMUNICATIONS

CHAPTER 3. CRIMES AND CIVIL ACTIONS RELATING TO COMMUNICATIONS PRIVACY

I. FEDERAL CRIMINAL PROVISIONS; FEDERAL INJUNCTIONS

A. IN GENERAL

§ 3:1 Introduction
§ 3:2 Unlawful conduct: 18 U.S.C.A. § 2511(1)
§ 3:3 Unlawful interception
§ 3:4 Unlawful interception: personal computers and email
§ 3:5 The meaning of “procure” in 18 U.S.C.A. § 2511(1)

B. UNLAWFUL DISCLOSURE OR USE OF INTERCEPTED COMMUNICATION

1. In General

§ 3:6 Overview
§ 3:7 Mens rea element
§ 3:8 Quantifying disclosures
§ 3:9 Disclosure by attorney
§ 3:10 Unlawful “use”
§ 3:11 Disclosure of inadvertently intercepted communications

2. Defenses

§ 3:12 Defenses: in general
§ 3:13 Public information—Common knowledge
§ 3:14 First Amendment: general principles
§ 3:15 Bartnicki v. Vopper
§ 3:16 The post-Bartnicki landscape

C. FEDERAL PENALTIES AND INJUNCTIONS

§ 3:17 Federal penalties: in general
TABLE OF CONTENTS

§ 3:18 The basic provision: 18 U.S.C.A. § 2511(4)(a)
§ 3:19 —The fine structure
§ 3:20 Less serious criminal violations: § 2511(4)(b)
§ 3:21 Governmental injunctions

D. OTHER FEDERAL CRIMINAL CHARGES

§ 3:22 “Leaking” information about an interception order: 18 U.S.C.A. § 2232(c)
§ 3:23 Other federal criminal charges

II. CONDUCT WHICH IS “NOT UNLAWFUL” UNDER FEDERAL STATUTES

§ 3:24 In general
§ 3:25 Communications service providers: interception, disclosure, use
§ 3:26 Record keeping
§ 3:27 Disclosure of communications, 18 U.S.C.A. § 2511(3)
§ 3:29 Consensual interceptions
§ 3:30 Interception of certain wire and electronic communications
§ 3:31 Interceptions by FCC
§ 3:32 Pen registers, traces, traps; FISA surveillance
§ 3:33 Certain satellite transmissions
§ 3:34 “Adjudicatory disclosure” necessary to prove crime, cause of action or defense

III. FEDERAL CIVIL ACTIONS

A. ACTIONS BASED ON TITLE III

§ 3:35 In general
§ 3:36 Basic civil action provision under Title III
§ 3:37 “Procuring” a violation of Title III; conspiracy; agency
§ 3:38 Elements of civil action
§ 3:39 Suits against the federal government
§ 3:40 Improper disclosure by law enforcement officials
§ 3:41 Administrative discipline & related matters
§ 3:42 Suits against agencies of governments other than the federal government

© 2018 Thomson Reuters, 12/2018
§ 3:43 Actions alleging improper cooperation with law enforcement authorities
§ 3:44 Available relief
§ 3:45 Computation of damages: general rule under Title III
§ 3:46 Punitive damages
§ 3:47 Re certain radio and video communications
§ 3:48 Defenses, in general
§ 3:49 Good-faith reliance defense
§ 3:50 Statute of limitations

B. ACTIONS BASED ON OTHER SOURCES OF LAW

§ 3:51 Section 1983 actions, immunity, and Title III
§ 3:52 Federal Tort Claims Act; discretionary function exception
§ 3:53 Other causes of action
§ 3:54 Attorneys and cellular, cordless, and mobile phones

IV. STATE CRIMES AND CIVIL ACTIONS RELATING TO COMMUNICATIONS PRIVACY

§ 3:55 State crimes and civil actions: in general
§ 3:56 Alabama
§ 3:57 Alaska
§ 3:58 Arizona
§ 3:59 Arkansas
§ 3:60 California
§ 3:61 Colorado
§ 3:62 Connecticut
§ 3:63 Delaware
§ 3:64 District of Columbia
§ 3:65 Florida
§ 3:66 Georgia
§ 3:67 Hawaii
§ 3:68 Idaho
§ 3:69 Illinois
§ 3:70 Indiana
§ 3:71 Iowa
§ 3:72 Kansas
CHAPTER 4. TOLL RECORDS, PEN REGISTERS, AND OTHER INFORMATION ABOUT WIRE COMUNICATIONS AND E-MAIL

§ 4:1 In general
I. TOLL RECORDS AND OTHER TELEPHONE COMPANY RECORDS AND SERVICES

§ 4:2 In general
§ 4:3 Constitutional issues
§ 4:4 18 U.S.C.A. § 2703(c), (d), (e)
§ 4:5 State law

II. PEN REGISTERS; TOUCH-TONE DECODERS; TRAPS AND TRACES; ELECTRONIC COMMUNICATIONS EQUIVALENTS

A. IN GENERAL

§ 4:6 Pen registers; cell phone counterparts
§ 4:7 Smith v. Maryland
§ 4:8 Trap and trace devices
§ 4:9 Federal legislation: overview
§ 4:10 Definitions: 18 U.S.C.A. § 3127
§ 4:11 18 U.S.C.A. § 3121(a), (d): prohibition; penalty
§ 4:12 18 U.S.C.A. § 3121(b): use by communication service providers

B. SURVEILLANCE BY LAW ENFORCEMENT OFFICIALS

§ 4:14 Court order; judge’s role; jurisdiction: 18 U.S.C.A. § 3123(a)
§ 4:14.50 “Ongoing criminal investigation”
§ 4:15 Contents of order: 18 U.S.C.A. § 3123(b)
§ 4:16 Application to e-mail and other forms of electronic communications
§ 4:17 Issues relating to technology used: 18 U.S.C.A. § 3121(c)
§ 4:17.50 Post-cut-through dialed digits (PCTDDs)
§ 4:18.50 Determining a target’s cell phone number: “stingray”; “triggerfish”; cell site simulator; digital analyzer
§ 4:19 Compelling cooperation: 18 U.S.C.A. § 3124
§ 4:20 Annual reports
§ 4:21 State law
§ 4:22 18 U.S.C.A. § 3124(d), (e), (f): compensation; civil and criminal defense
III. EVIDENTIARY AND OTHER ISSUES

§ 4:23 Standing to challenge
§ 4:24 No suppression remedy
§ 4:25 Computerized records, hearsay and the Confrontation Clause
§ 4:26 Caller identification service
§ 4:27 Miscellaneous holdings
§ 4:28 Use of cell phones to track the possessor’s location

CHAPTER 5. CONSENSUAL INTERCEPTIONS

§ 5:1 In general
§ 5:2 Whose consent governs

I. CONSENSUAL INTERCEPTIONS BY LAW ENFORCEMENT OFFICIALS

A. CONSTITUTIONAL ISSUES

1. First, Fourth, and Fifth Amendments

§ 5:3 First Amendment
§ 5:4 Fourth Amendment
§ 5:5 Fifth Amendment, in general
§ 5:6 —Mandatory recording of custodial interrogation

2. Sixth Amendment

§ 5:7 Massiah v. U.S.
§ 5:7.10 Montejo v Louisiana
§ 5:8 Investigations into uncharged crimes: Maine v. Moulton
§ 5:9 Maine v. Moulton—Statements concerning pending charges elicited during investigation uncharged crimes
§ 5:10 Limitations on Moulton exclusionary rule; subsequent case law
§ 5:11 —Statements concerning uncharged crimes elicited after prosecution has commenced on other charges
§ 5:12 “Passive listening posts”: Kuhlmann v. Wilson
§ 5:13 Statements elicited from a represented but uncharged suspect
§ 5:14 Miscellaneous issues and holdings

B. TITLE III AND CORRESPONDING STATE LAW

1. Title III


§ 5:15.10 Compelling technical assistance

§ 5:16 Motives of cooperating civilian

2. State Law

§ 5:17 In general

§ 5:18 Alabama

§ 5:19 Alaska

§ 5:20 Arizona

§ 5:21 Arkansas

§ 5:22 California

§ 5:23 Colorado

§ 5:24 Connecticut

§ 5:25 Delaware

§ 5:26 District of Columbia

§ 5:27 Florida

§ 5:28 Georgia

§ 5:29 Hawaii

§ 5:30 Idaho


§ 5:31.70 Public encounters between law enforcement officials and civilians; public conduct of police officers

§ 5:31.80 Other Article 14 provisions

§ 5:31.90 History of Article 14

§ 5:72 South Dakota
§ 5:73 Tennessee
§ 5:74 Texas
§ 5:75 Utah
§ 5:76 Vermont
§ 5:77 Virginia
§ 5:78 Washington
§ 5:79 —“Private communication, private conversation”
§ 5:80 —Establishing all-party consent
§ 5:81 —Extent of suppression
§ 5:82 —Consensual interceptions by federal officials
§ 5:83 —The warrant requirement
§ 5:84 —The RCW § 9.73.030(2) exceptions
§ 5:85 —The RCW § 9.73.090 exception
§ 5:86 —RCW § 9.73.230—The drug investigation exception
§ 5:87 —RCW § 9.73.210—The “reasonable risk of danger” exception
§ 5:88 West Virginia
§ 5:89 Wisconsin
§ 5:90 Wyoming

C. OTHER POTENTIAL RESTRICTIONS ON LAW ENFORCEMENT USE

1. Other sources of law
§ 5:91 Effect of state restrictions on federal officials
§ 5:92 Agency regulations
§ 5:93 Suppressed interception order intercepts

2. Rules or Code of Professional Conduct and the Uncharged But Represented Suspect
§ 5:94 Overview
§ 5:95 Rules or Code of Professional Conduct
§ 5:96 The “McDade Act”: 28 U.S.C. § 530B(a)
§ 5:97 “Authorized by law”: how the states line up
§ 5:98 The U.S. v. Hammad approach
§ 5:99 The U.S. v. Hammad approach—The “alter ego” test
§ 5:100 Impact of violation

xxxvi
TABLE OF CONTENTS

II. CONSENSUAL INTERCEPTIONS BY PRIVATE PERSONS
   A. FEDERAL LAW; SPECIFIC ISSUES
      § 5:101 Overview
      § 5:102 18 U.S.C.A. § 2511(2)(d)
      § 5:103 “Criminal or tortious” purpose: in general
      § 5:104 “Criminal or tortious” purpose: specific applications
      § 5:105 “Other injurious act”
      § 5:106 Special issues relating to oral communications
   B. STATE LAW
      § 5:107 Alabama
      § 5:108 Alaska
      § 5:109 Arizona
      § 5:110 Arkansas
      § 5:111 California
      § 5:112 Colorado
      § 5:113 Connecticut
      § 5:114 District of Columbia
      § 5:115 Delaware
      § 5:116 Florida
      § 5:117 Georgia
      § 5:118 Hawaii
      § 5:119 Idaho
      § 5:120 Illinois
      § 5:121 Indiana
      § 5:122 Iowa
      § 5:123 Kansas
      § 5:124 Kentucky
      § 5:125 Louisiana
      § 5:126 Maine
      § 5:127 Maryland
      § 5:128 Massachusetts
      § 5:129 Michigan
      § 5:130 Minnesota
      § 5:131 Mississippi
      § 5:132 Missouri
      § 5:133 Montana
      § 5:134 Nebraska
      § 5:135 Nevada
§ 5:136 New Hampshire
§ 5:137 New Jersey
§ 5:138 New Mexico
§ 5:139 New York
§ 5:140 North Carolina
§ 5:141 North Dakota
§ 5:142 Ohio
§ 5:143 Oklahoma
§ 5:144 Oregon
§ 5:145 Pennsylvania
§ 5:146 Rhode Island
§ 5:147 South Carolina
§ 5:148 South Dakota
§ 5:149 Tennessee
§ 5:150 Texas
§ 5:151 Utah
§ 5:152 Vermont
§ 5:153 Virginia
§ 5:154 Washington
§ 5:155 West Virginia
§ 5:156 Wisconsin
§ 5:157 Wyoming

C. RELATED STATE LAW ISSUES

§ 5:158 Criminal cases: statutory restrictions and due process of law
§ 5:159 Statutory restrictions on defense attorneys
§ 5:160 Bar rules governing attorney conduct: defense counsel and civil litigants
§ 5:161 Applying bar rules to criminal defense attorneys: the problem exemplified
§ 5:162 Bar codes and rules: suppression remedy in civil litigation

III. DEFINING AND PROVING CONSENT

§ 5:163 Defining consent
§ 5:164 —Electronic communications
§ 5:165 Proving consent
§ 5:166 “Implied consent” in non-investigative contexts: in general
§ 5:167 “Implied consent”: specific factual settings
§ 5:168 —Oral communications

xxxviii
CHAPTER 6. OTHER EXCEPTIONS AND SITUATIONS

§ 6:1 Overview

I. INTERCEPTIONS BY PRIVATE CITIZENS

§ 6:2 In general

A. EMPLOYER MONITORING OF EMPLOYEE CONVERSATIONS

§ 6:3 Introduction
§ 6:4 Government as employer: Fourth Amendment; *O'Connor v. Ortega*

© 2018 Thomson Reuters, 12/2018
§ 6:4.50 Government as employer: Fourth Amendment; City of Ontario v. Quon
§ 6:5 “Implied consent”
§ 6:8 “Ordinary course of business”—Monitoring employees’ conversations with customers and other business contacts
§ 6:9 —Employee suspected of misconduct
§ 6:10 —Monitoring where personal calls are prohibited
§ 6:11 —Other purposes
§ 6:12 Excessive or indiscriminate monitoring
§ 6:13 Excessive or indiscriminate monitoring: problems of proof
§ 6:14 Office e-mail; employer-supplied computer
§ 6:15 Employee voice mail
§ 6:16 Miscellany

B. INTRAFAMILY INTERCEPTIONS

§ 6:17 Introduction
§ 6:18 Is there a “family home” or “marital home exemption?”
§ 6:19 —Related causes of action
§ 6:20 18 U.S.C.A. § 2510(5)(a)(i) and the “extension phone” exception
§ 6:21 The “extension phone” exception and recording equipment
§ 6:22 Extension phones and recording equipment: conversations not involving children
§ 6:23 “Extension phone exception”: parental recording of a child’s phone conversations
§ 6:24 Parental “vicarious consent”
§ 6:25 —Similar relationships
§ 6:26 Oral communications
§ 6:27 Admissibility of recordings in divorce, custody and similar proceedings
§ 6:28 Civil action against the “tapper” and associates
§ 6:29 Miscellany
§ 6:30 Intrafamily issues relating to computers
### C. OTHER PRIVATE INTERCEPTION SITUATIONS

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 6:31</td>
<td>Interception by switchboard operators: 18 U.S.C.A. § 2512(2)(a)(I); corresponding state law</td>
</tr>
<tr>
<td>§ 6:32</td>
<td>Private interceptions: miscellaneous holdings</td>
</tr>
<tr>
<td>§ 6:32.50</td>
<td>Unlawful recording as evidence of innocence</td>
</tr>
</tbody>
</table>

### D. PROSECUTORIAL USE OF COMMUNICATIONS INTERCEPTED BY PRIVATE PERSONS

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 6:33</td>
<td>Lawful interceptions</td>
</tr>
<tr>
<td>§ 6:34</td>
<td>Use of unlawful interceptions of wire or oral communications: constitutional principles</td>
</tr>
<tr>
<td>§ 6:35</td>
<td>Same: 18 U.S.C.A. § 2515</td>
</tr>
<tr>
<td>§ 6:37</td>
<td>Same: how the jurisdictions line up currently</td>
</tr>
<tr>
<td>§ 6:38</td>
<td>Recordings seized during physical searches</td>
</tr>
<tr>
<td>§ 6:39</td>
<td>Recordings given to law enforcement officials by private citizens</td>
</tr>
<tr>
<td>§ 6:40</td>
<td>Matters of pleading and proof</td>
</tr>
<tr>
<td>§ 6:41</td>
<td>Electronic communications</td>
</tr>
</tbody>
</table>

### II. PRISONERS, INMATES, PAROLEES AND PROBATIONERS

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 6:42</td>
<td>Introduction</td>
</tr>
<tr>
<td>§ 6:43</td>
<td>Prisoners and inmates, in general</td>
</tr>
<tr>
<td>§ 6:44</td>
<td>Post-arrest, pre-arraignment detention; “police car” recordings</td>
</tr>
<tr>
<td>§ 6:45</td>
<td>Telephone conversations</td>
</tr>
<tr>
<td>§ 6:46</td>
<td>—“Implied consent” theory</td>
</tr>
<tr>
<td>§ 6:48</td>
<td>18 U.S.C.A. § 2510(a)(ii): law enforcement exception to definition of “device”—Same: equipment; policy; purpose; notice</td>
</tr>
<tr>
<td>§ 6:49</td>
<td>Are prison officials “investigative and law enforcement officers?”</td>
</tr>
<tr>
<td>§ 6:50</td>
<td>Disclosure of phone calls as evidence</td>
</tr>
<tr>
<td>§ 6:51</td>
<td>Admissibility against non-prisoner participant</td>
</tr>
<tr>
<td>§ 6:52</td>
<td>Other issues relating to prisoner’s phone calls</td>
</tr>
</tbody>
</table>
CHAPTER 7. STORED WIRE AND ELECTRONIC COMMUNICATIONS

I. INTRODUCTION

A. OVERVIEW AND definitions

1. Overview

§ 7:1 In General; “Title II”; “Stored Communications Act”; “SCA”

2. Definitions

§ 7:2 In general
§ 7:3 Definitions, in general—“Electronic storage”: 18 U.S.C.A § 2510(17)
§ 7:4 “Temporary, intermediate storage”: § 2510(17)(A)
§ 7:5 “Storage . . . for purposes of back-up protection”: 18 U.S.C.A § 2510(17)(B)
§ 7:7 18 U.S.C.A § 2510(17)(B): broad view
§ 7:8 18 U.S.C.A § 2510(17)(B): evaluation
§ 7:9 State law

B. CRIMINAL PROVISION

1. Generally

§ 7:10 18 U.S.C.A § 2701(a): unlawful access
§ 7:11 Exceeding authorization
§ 7:12 “Access”
§ 7:13 Penalties: 18 U.S.C.A § 2701(b)
§ 7:14 Exceptions: 18 U.S.C.A § 2701(c)
§ 7:15 Exceptions: 18 U.S.C.A § 2701(c)(1)—By the provider of the communication service
§ 7:16 Exceptions: 18 U.S.C.A § 2701(c)(2)—“By a user of that service”
TABLE OF CONTENTS

§ 7:17 18 U.S.C.A. § 2701(c)(3): Authorized by other statutes

2. Specific Applications

§ 7:20 Access by Internet Service Provider: 18 U.S.C.A. § 2701(c)
§ 7:21 Employer access to employee electronic communications: Employer as ISP
§ 7:22 Government access as employer and ISP
§ 7:23 Access to Internet web sites
§ 7:24 “User” and consensual interceptions
§ 7:25 Miscellany
§ 7:26 Other specific applications—1 [Reserved]
§ 7:27 Other specific applications—2 [Reserved]
§ 7:28 Other specific applications—3 [Reserved]

C. CIVIL ACTIONS; ADMINISTRATIVE SANCTIONS

§ 7:29 In general

1. Unlawful Access

§ 7:30 Actionable conduct: 18 U.S.C.A. § 2707(a)
§ 7:30.10 Actionable conduct: “secondary liability”
§ 7:31 Culpable mental states

2. Disclosure by Service Provider

§ 7:32 In general
§ 7:33 Disclosure prohibited: § 2702(a)
§ 7:34 Permitted disclosures: § 2702(b)
§ 7:34.10 Scope of 18 U.S.C.A. § 2702(b)(3), the “consent” provision
§ 7:35 18 U.S.C.A. § 2702(b); Permitted disclosures to government agencies
§ 7:36 Disclosure of information other than contents: 18 U.S.C.A. § 2702(c)

3. Improper Disclosure by Public Officials

§ 7:37 In general: 18 U.S.C.A. § 2707(g)

4. Relief and Damages

§ 7:38 Relief: § 2707(b)
II. GOVERNMENT ACCESS TO COMMUNICATIONS AND INFORMATION

A. ACCESS TO COMMUNICATIONS AND INFORMATION

§ 7:45 In general; 18 U.S.C.A. § 2703
§ 7:46 Internet services provided by cable operators
§ 7:47 Contents of certain communications in electronic storage 180 days or less: 18 U.S.C.A. § 2703(a); Federal court jurisdiction
§ 7:48 Contents of “stored” electronic communications and communications more than 180 days “old”: 18 U.S.C.A. § 2703(b)(1)
§ 7:48.50 Particular description of communications sought
§ 7:49 Contents of other stored electronic communications—By search warrant: 18 U.S.C.A. § 2703(b)(1)(A)
§ 7:50 —By subpoena
§ 7:51 —By court order: 18 U.S.C.A. § 2703(d)
§ 7:51.10 The § 2703(d) factual standard: overview and history
§ 7:51.20 Section 2703(d) factual standard: “specific and articulable facts”
§ 7:51.30 Section 2703(d) factual standard: “reasonable grounds to believe”
§ 7:51.40 Section 2703(d) factual standard: “relevant and material to an ongoing criminal investigation”
§ 7:51.50 Contents of communications
§ 7:52 Information other than contents: 18 U.S.C.A. § § 2703(c) to 2703(e)
§ 7:52.50 “Emergency” disclosure pursuant to 18 U.S.C.A. § 2702(c)(4)
Table of Contents

§ 7:53 Interjurisdictional subpoenas
§ 7:54 18 U.S.C.A. §§ 2709, 3511: “national security letters” for transactional records, etc., in counterintelligence investigations
§ 7:54.10 18 U.S.C.A. § 2709
§ 7:54.30 Nondisclosure orders: termination procedure
§ 7:55.50 “Standing” to challenge government acquisition of contents
§ 7:56 Compensation to companies providing information: 18 U.S.C.A. § 2706

B. POSTPONING NOTIFICATION; BACKUP PRESERVATION

§ 7:58 Preclusion of notice to suspect
§ 7:59 Constitutionality of withholding and postponing notice without a showing of probable cause
§ 7:60 18 U.S.C.A. § 2704: Backup preservation—Introduction
§ 7:61 —Customer challenge
§ 7:62 —Comment

Volume 2

PART III. TITLE III AND FISA APPLICATIONS AND ORDERS

CHAPTER 8. APPLICATION AND ORDER

I. INTRODUCTION

§ 8:1 In general
§ 8:2 Applicability of Fourth Amendment case law
§ 8:3 A word to law enforcement officials: the importance of candor

© 2018 Thomson Reuters, 12/2018
II. THE AUTHORIZING OFFICIAL

A. WHO CAN AUTHORIZE AN APPLICATION

§ 8:4 In general

1. Federal Applications

§ 8:5 Federal wire or oral interceptions: 18 U.S.C.A. § 2516(1); U.S. v. Giordano

§ 8:6 Federal applications, electronic communications:
18 U.S.C.A. § 2516(3)

2. State applications

§ 8:7 State applications: 18 U.S.C.A. § 2516(2); state law

§ 8:8 Jurisdictional restrictions on state officials

§ 8:9 Federal law on state intrajurisdictional issues

§ 8:10 State law

§ 8:11 Cellular and other mobile phones [Deleted]

B. IDENTIFYING THE OFFICIAL; DEFINING HIS OR HER ROLE

§ 8:12 Role of authorizing official


§ 8:14 Form of authorization

§ 8:15 Administrative reports

C. DELEGATION OF AUTHORITY

1. Federal applications

§ 8:16 18 U.S.C.A. § 2516(1)

2. State Applications

§ 8:17 18 U.S.C.A. § 2516(2)

§ 8:18 State law

§ 8:19 Authority of acting state official

§ 8:20 Authority to sign application

III. AGENCY AND AFFIANT

§ 8:21 The law enforcement agency: 18 U.S.C.A. § 2510(7)
TABLE OF CONTENTS

§ 8:23 Civilian monitors: contents of application and interception order
§ 8:24 Civilian monitors: state law
§ 8:25 Joint federal-state investigations
§ 8:26 The affiants

IV. PERSONS TO BE INTERCEPTED

§ 8:28 Conversations between identified and non-identified participants
§ 8:29 Conversations between participants not named in the order: U.S. v. Kahn
§ 8:30 Who must be identified as a probable interceptee; and suppose some who should, are not? Kahn; U.S. v. Donovan
§ 8:32 Implications (2): “Of others, as yet unknown”
§ 8:33 Naming those for whom probable cause is lacking
§ 8:34 State variations

V. “DESIGNATING” AND SPECIFYING CRIMES

A. DESIGNATED OFFENSES

§ 8:35 Federal applications and orders: 18 U.S.C.A. § 2516(1)
§ 8:36 State discretion; 18 U.S.C.A. § 2516(2)
§ 8:37 —State statutes
§ 8:38 —“Dangerous to life, limb or property”
§ 8:39 Designating federal crimes in state intercept orders
§ 8:40 Electronic communications

B. SPECIFYING CRIMES

§ 8:42 Related designated offenses
§ 8:43 Related non-designated offenses
§ 8:44 Interstate issues

© 2018 Thomson Reuters, 12/2018
VI. FACILITIES OR LOCATION; DESCRIPTION OF COMMUNICATIONS
§ 8:45 In general

A. FACILITIES OR LOCATION
§ 8:47 Wiretaps
§ 8:47.50 Cell phone as “facility”; phone calls; text messages
§ 8:47.75 Authority to track or determine location of phone
§ 8:48 “Cloned” or “burnout” cell phones
§ 8:49 Public telephones
§ 8:49.50 Phone as inadvertent “bug”
§ 8:50 Bugs
§ 8:51 Incorrect address or phone number

B. PARTICULAR DESCRIPTION OF COMMUNICATIONS

VII. PROBABLE CAUSE
A. STATUTORY AND CONSTITUTIONAL CONSIDERATIONS
§ 8:53 18 U.S.C.A. § 2518(1)(b); 18 U.S.C.A. § 2518(3)(a), (b), (d)
§ 8:54 Defining probable cause: Illinois v. Gates and its progeny
§ 8:55 The Leon “good-faith exception”
§ 8:56 Judicial treatment of the issue: an overview
§ 8:57 Discoverability of applications and supporting affidavits

B. SOURCES OF PROBABLE CAUSE
§ 8:58 In general
§ 8:59 Confidential informants
§ 8:60 —State variations
§ 8:61 Other sources of probable cause
§ 8:61.50 Pen register-trap-and-trace analysis
§ 8:62 Circumstantial evidence
TABLE OF CONTENTS

§ 8:63  Expert opinion

C. PARTICULAR PROBLEMS AND ISSUES
§ 8:64  “Moving target”; changing phone numbers
§ 8:65  Staleness
§ 8:65.50  Probable cause and particular offenses

D. LITIGATING PROBABLE CAUSE
§ 8:66  Role of reviewing court
§ 8:67  Factual misstatements and omissions: *Franks v. Delaware*
§ 8:68  —Applying *Franks* to interception order applications
§ 8:69  Tainted information
§ 8:70  Standard of appellate review

VIII. “NECESSITY”: OTHER INVESTIGATIVE PROCEDURES; GOALS OF THE INVESTIGATION

A. IN GENERAL
§ 8:71  The “necessity” requirement
§ 8:73  Judicial gloss: an overview
§ 8:74  State variations

B. GOALS OF THE INVESTIGATION
§ 8:75  Necessity in light of investigative goals
§ 8:76  Need for additional evidence against the targeted individuals
§ 8:77  Time-sensitive investigations
§ 8:78  Investigations into larger conspiracies
§ 8:79  The severity of the crimes under investigation
§ 8:80  Words of caution

C. CONTOURS OF THE “OTHER PROCEDURES” REQUIREMENT
§ 8:81  “Other” procedures
§ 8:81.10  Multi-jurisdictional investigations
§ 8:82  “Full and complete statement”
§ 8:83 “Tried and failed”
§ 8:84 “Unlikely to succeed; too dangerous”—In general
§ 8:85 Unlikely to succeed or too dangerous: specific techniques
§ 8:86 Taps and bugs as “other procedures”

D. SPECIAL PROBLEMS AND ISSUES
§ 8:87 The moving target
§ 8:88 The multiple location application
§ 8:89 New crimes, targets, telephones or premises

E. LITIGATING THE “NECESSITY” REQUIREMENT
§ 8:90 Factual misstatements and omissions
§ 8:91 Evaluating the government’s showing; the “boilerplate” issue
§ 8:92 Standard of trial judge and appellate review

IX. TIMING, EXTENT AND DURATION OF SURVEILLANCE
§ 8:93 In general
§ 8:94 Multiple interceptions: 18 U.S.C.A. § 2518(1)(d)
§ 8:95 18 U.S.C.A. § 2518(5)
§ 8:96 Effective date: in general
§ 8:97 “As soon as practicable”; delay between issuance and commencement of interceptions
§ 8:98 Period of interception, termination date: 18 U.S.C.A. §§ 2518(1)(d), 2518(4)(e), 2518(5)
§ 8:99 Intensity of surveillance (hours per day)
§ 8:100 “Attainment of objective” termination clause

X. MINIMIZATION; PRIVILEGED COMMUNICATIONS
A. MINIMIZATION
§ 8:101 In general
§ 8:102 Minimization: an introduction
§ 8:103 The absence of a minimization clause
§ 8:104 Wording the clause
§ 8:105 Foreign language intercepts; coded, guarded, cryptic language
§ 8:105.50 Minimizing text messages and other electronic communications
§ 8:106 A word to judges
§ 8:107 Minimizing interception of faxes and e-mails

B. PRIVILEGED COMMUNICATIONS
§ 8:108 Statutory treatment
§ 8:109 Addressing the problem in application and order

XI. PRIOR APPLICATIONS
§ 8:110 Prior applications: 18 U.S.C.A. § 2518(1)(e)
§ 8:111 What is required; what is advisable
§ 8:112 Prior “applications,” not prior “interceptions”
§ 8:113 Prior facilities or places “specified” in the [pending] application, vs. those merely “mentioned”
§ 8:114 Prior applications “known” to the investigative team
§ 8:115 Remedy for non-compliance

XII. OTHER SUGGESTIONS, ISSUES AND PROVISIONS
§ 8:116 Incorporation by reference
§ 8:117 Extensions
§ 8:118 Pre-intercept notice to the target
§ 8:119 Covert entry
§ 8:120 Compelling cooperation
§ 8:121 Progress reports: 18 U.S.C.A. § 2518(6)
§ 8:122 Factual findings; Contents of order: 18 U.S.C.A. § 2518(3)–(5)

XIII. SUBMISSION, CUSTODY, AND SEALING THE PAPERS
A. THE JUDGE
§ 8:123 In general
§ 8:127 State orders
§ 8:128 State orders: mobile and cellular phones
§ 8:129 Choosing among “eligible” judges

B. SUBMITTING, SEALING, AND UNSEALING THE PAPERS
§ 8:130 Submitting the application and order to the judge
§ 8:131 Signing and swearing to the affidavits; signing the order
§ 8:132 Sealing; Custody and copies: 18 U.S.C.A. § 2518(8)(b)
§ 8:133 —Substantial compliance; non-compliance
§ 8:134 —Unsealing; destruction

XIV. JUDICIAL RESPONSIBILITY
§ 8:135 In general
§ 8:136 Additional information; ex parte proceeding: 18 U.S.C.A. § 2518(2)
§ 8:137 Decision to issue: 18 U.S.C.A. § 2518(3)
§ 8:138 Reports to Administrative Office

CHAPTER 9. EXTENSIONS AND SECOND-GENERATION ORDERS
§ 9:1 In general

I. EXTENSIONS
§ 9:3 Number and duration of extensions
§ 9:4 Definition of “extension”
§ 9:5 Application to cellular phones
§ 9:6 Decision to seek an extension
§ 9:7 When extension application must be submitted
§ 9:8 Results or explanation: 18 U.S.C.A. § 2518(1)(f)
§ 9:9 Multiple extensions

II. ISSUES AND REQUIREMENTS COMMON TO EXTENSIONS AND SECOND-GENERATION APPLICATIONS AND ORDERS
§ 9:10 Incorporation of original application and interception order
CHAPTER 10. ROVING INTERCEPTIONS

I. INTRODUCTION

§ 10:1 Statutory authority: 18 U.S.C.A. §§ 2518(11), (12)
§ 10:2 State provisions

II. APPLICATION AND ORDER: SPECIAL REQUIREMENTS

§ 10:3 Authorization for application
§ 10:4 Identity of intended interceptee
§ 10:5 Showing of need: oral intercept
§ 10:6 Showing of need: wiretaps and electronic communications
§ 10:7 Showing of need: comparing the two standards
§ 10:8 Description of communications—Oral intercepts (bugs)
§ 10:9 —Wiretaps; electronic communications

III. IMPLEMENTATION OF ROVING INTERCEPT ORDERS

§ 10:10 Knowledge of facilities or location
§ 10:11 The “dual purpose” order; scope of the roving oral intercept provision
§ 10:12 Knowledge, advance installation: wiretaps, electronic communications
§ 10:13 Knowledge, advance installation: bugs
§ 10:14 Roving interceptions and minimization
§ 10:15 Telephone and other service provider cooperation

IV. POST-EXECUTION PROCEDURES

§ 10:16 Reports to Administrative Office
CHAPTER 11. EMERGENCY SURVEILLANCE
§ 11:1 In general
§ 11:2 Grounds for an order; “emergency situation”
§ 11:3 The “immediate danger” clause
§ 11:4 The “organized crime” provision
§ 11:5 Pre-interception authorization
§ 11:6 Obtaining assistance
§ 11:7 Post-interception order of authorization
§ 11:8 State variations

CHAPTER 12. FOREIGN INTELLIGENCE AND NATIONAL SECURITY SURVEILLANCE OF TARGETS WHO ARE WITHIN THE UNITED STATES

I. BACKGROUND: ELECTRONIC SURVEILLANCE CONDUCTED OUTSIDE THE UNITED STATES
§ 12:1 Overview
§ 12:2 Interceptions outside the United States by officials of a foreign government
§ 12:3 Interception by foreign officials with U.S. involvement
§ 12:4 Foreign interceptions by American officials without foreign government involvement

II. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA): INTRODUCTION
§ 12:5 In general; FISA is “exclusive means” of lawful surveillance
§ 12:6 Constitutionality: Fourth Amendment
§ 12:6.50 50 USCA 1881a (“Section 702”)
§ 12:6.70 Clapper v. Amnesty International
§ 12:6.75 Litigation subsequent to Clapper v. Amnesty International
§ 12:7 Legislative history and other source material
§ 12:8 Summary of FISA Title I and of this chapter
§ 12:9 Foreign Intelligence Surveillance Court (FISC): 50 U.S.C.A. § 1803
### Table of Contents

§ 12:10 Foreign Intelligence Surveillance Court of Review (FISA-CR): 50 U.S.C.A. § 1803(b)

§ 12:11 FISA inapplicable to non-foreign intelligence surveillance

§ 12:12 “United States person”: 50 U.S.C.A. § 1801(i)

### II. FISA: “FOREIGN INTELLIGENCE INFORMATION”; PURPOSE OF SURVEILLANCE; “ELECTRONIC SURVEILLANCE”

#### A. “FOREIGN INTELLIGENCE INFORMATION”

§ 12:13 “Foreign intelligence information”: 50 U.S.C.A. § 1801(e)

#### B. PURPOSE OF SURVEILLANCE

§ 12:14 Foreign intelligence information “a significant purpose”of surveillance: 50 U.S.C.A. § 1804(a)(6)(B)

§ 12:15 Post-PATRIOT ACT litigation: In re Sealed Case, 2002

§ 12:16 In re Sealed Case: The criminal-foreign intelligence “dichotomy”

§ 12:17 In re Sealed Case: Impact of the USA PATRIOT ACT

§ 12:18 In re Sealed Case: Constitutionality of the “a significant purpose” test

§ 12:19 United States v. Mayfield and its aftermath

§ 12:20 Subsequent litigation

§ 12:21 Future legislative developments [Reserved]

#### C. “ELECTRONIC SURVEILLANCE”

§ 12:22 “Electronic surveillance” defined: 50 U.S.C.A. § 1801(f)

§ 12:23 Wire and radio communications, in general


§ 12:27 Surveillance of international wire or radio communications: 50 U.S.C.A. § 1801(f)(1)

© 2018 Thomson Reuters, 12/2018
§ 12:28 Other surveillance to acquire “information”:
50 U.S.C.A. § 1801(f)(4)
§ 12:29 Oral communications; “electronic communications”; stored communications; computer searches; visual surveillance; electronic tracking
§ 12:30 Technological developments [Reserved]
§ 12:31 Pen registers; Trap and trace surveillance: 50 U.S.C.A. § 1842
§ 12:32 Unprotected conduct
§ 12:33 Unregulated surveillance
§ 12:33.50 Communication “metadata” and other records: 50 U.S.C.A. §§ 1861 to 1862
§ 12:33.70 American Civil Liberties Union v. Clapper

IV. FOREIGN POWERS, FOREIGN AGENTS

§ 12:34 In general
§ 1801(a)(1)–(3)
§ 1801(a)(4)–(7)
§ 12:37 Agent of a foreign power—Non-U.S. person: 50 U.S.C.A. § 1801(b)(1)
§ 1805(a)(2)(A)

V. PRE-SURVEILLANCE PROCEDURES: APPLICATIONS AND ORDERS

A. INTRODUCTION

§ 12:40 In general; retention of certifications, applications and orders, 50 U.S.C.A. § 1805(g)
§ 12:41 Categories of surveillance

B. LIMITED SURVEILLANCE OF AN OFFICIAL FOREIGN POWER WITHOUT A COURT ORDER

§ 12:43 Targets; certification; no court order required
§ 12:44 Minimization: 50 U.S.C.A. § 1801(h)(4)
C. OTHER SURVEILLANCE: REQUIREMENTS IN COMMON

§ 12:46 50 U.S.C.A. § 1804(a); 50 U.S.C.A. § 1805

1. Application

§ 12:47 Application: 50 U.S.C.A. § 1804(a); pen register, trap and trace, § 1805(i)

§ 12:48 Required information


§ 12:50 Minimization; duration of surveillance

§ 12:51 Multiple devices

§ 12:52 Additional requirements

2. Certification of need


3. Judicial Findings

§ 12:54 Judicial findings: 50 U.S.C.A. § 1805(a),(b)

4. Surveillance order

§ 12:55 Surveillance order: 50 U.S.C.A. § 1805(c); 50 U.S.C.A. § 1801(i)

§ 12:56 Required information: 50 U.S.C.A. § 1805(c)(1)

§ 12:57 Required directives: 50 U.S.C.A. § 1805(c)(2)

§ 12:58 Additional requirements

5. Other provisions

§ 12:59 Duration of surveillance order; extensions: 50 U.S.C.A. § 1805(d)


D. GENERAL SURVEILLANCE OF AN OFFICIAL FOREIGN POWER; POTENTIAL SURVEILLANCE OF AN INNOCENT U.S. PERSON

§ 12:61 50 U.S.C.A. § 1805(d)

§ 12:62 Application: deleted provision

§ 12:63 Surveillance order: 50 U.S.C.A. § 1805(d)
E. SURVEILLANCE OF UNOFFICIAL FOREIGN AGENCIES AND AGENTS

§ 12:64 In general

F. INTENTIONAL SURVEILLANCE OF A U.S. PERSON

§ 12:65 Intentional surveillance of a U.S. person

G. OTHER SURVEILLANCE

§ 12:66 Emergency surveillance: 50 U.S.C.A. § 1805(e)
§ 12:68 Miscellaneous surveillance: 50 U.S.C.A. § 1805(f)
§ 12:69 Subsequent technological innovations [Reserved]

VI. CONDUCT OF SURVEILLANCE

§ 12:70 Minimization: 50 U.S.C.A. § 1801(h)
§ 12:71 Comparing minimization under Title III and FISA: U.S. persons; “acquisition, retention, dissemination”; other differences
§ 12:72 50 U.S.C.A. § 1801(h)(1)
§ 12:75 Enforcement mechanisms
§ 12:76 Determining compliance: “Good-faith effort” requirement

VII. DISCLOSURE, USE, LITIGATION

§ 12:77 In general: 50 U.S.C.A. § 1806

A. DISCLOSURE AND USE

§ 12:78 50 U.S.C.A. § 1806(a): minimization; privileged communications; lawful purposes
§ 12:79 Disclosure for law enforcement purposes; required statement, 50 U.S.C.A. § 1806(b)
§ 12:81 Destruction of unintentionally acquired information: 50 U.S.C.A. § 1806(i)
§ 12:82 Use of FISA information in foreign criminal prosecutions

B. NOTICE
§ 12:83 In general
§ 12:84 Notification prior to evidentiary use—In general
§ 12:85 Notification prior to evidentiary use, federal proceedings: 50 U.S.C.A. § 1806(c)
§ 12:86 Notification prior to evidentiary use, state and local proceedings: 50 U.S.C.A. § 1806(d)
§ 12:87 “Aggrieved person,” 50 U.S.C.A. § 1801(k); “Brady” and Jencks Act material
§ 12:88 Notice of emergency surveillance not subsequently approved: 50 U.S.C.A. § 1806(j)

C. DISCOVERY AND SUPPRESSION: STANDARDS
§ 12:89 Standing to seek discovery and suppression: 18 U.S.C.A. § 3504; other bases
§ 12:90 Grounds for suppression: 50 U.S.C.A. § 1806(e)

D. DISCOVERY AND SUPPRESSION: PROCEDURE
§ 12:91 Introduction
§ 12:92 50 U.S.C.A. 1806(f): In camera procedure
§ 12:93 Deciding the motion; post-denial disclosure: 50 U.S.C.A. § 1806(g)
§ 12:94 Finality and appealability of orders: 50 U.S.C.A. § 1806(h)
§ 12:95 Scope of review
§ 12:96 Government’s right to refuse disclosure; suppression; dismissal

VIII. CRIMINAL SANCTIONS; CIVIL LIABILITY
§ 12:97 Criminal sanctions: 50 U.S.C.A. § 1809
§ 12:99 Release from liability: 50 U.S.C.A. §§ 1805(h), 1885a
§ 12:100 Future developments [Reserved]

IX. REPORTS AND OVERSIGHT
PART IV. EXECUTION OF A TITLE III INTERCEPTION ORDER

CHAPTER 13. [Reserved]

CHAPTER 14. ROLES AND RESPONSIBILITIES; INVESTIGATIVE DISCLOSURE AND USE

I. ROLES AND RESPONSIBILITIES

§ 14:1 Role of police
§ 14:2 Role of prosecutor
§ 14:3 Judicial supervision
§ 14:4 Meetings between judge and prosecutor

II. TIME, TASKS AND TACTICS

§ 14:5 Pre-interception delays
§ 14:6 What (and how) to record: 18 U.S.C.A. § 2518(8)(a)
§ 14:7 Pager logs
§ 14:8 Investigative tactics
§ 14:9 Identifying participants
§ 14:10 Extending hours of surveillance

III. INVESTIGATIVE DISCLOSURE AND USE

§ 14:12 In general: 18 U.S.C.A. § 2517
§ 14:13 Investigative use: 18 U.S.C.A. § 2517(2)
§ 14:14 Investigative disclosure: 18 U.S.C.A. § 2517(1)
§ 14:15 18 U.S.C.A. § 2517(1): to whom may information be given
§ 14:16 The California “hand-off” debacle; lessons to be learned
§ 14:17 Remedies for improper disclosure
§ 14:18 Use of illegal interceptions
§ 14:19 Interjurisdictional disclosure and use: criminal cases
TABLE OF CONTENTS

§ 14:20 Interjurisdictional disclosure and use: civil cases

IV. DISCLOSURE FOR NATIONAL SECURITY AND FOREIGN INTELLIGENCE PURPOSES

§ 14:21 18 U.S.C.A. § 2517(6)–(8)

CHAPTER 15. MINIMIZATION

I. IN GENERAL

§ 15:1 Overview
§ 15:2 Interception, retention, distribution
§ 15:3 Approaches to minimization
§ 15:4 Intrinsic minimization
§ 15:5 Extrinsic minimization
§ 15:6 Dual recorder minimization
§ 15:7 After-the-fact minimization
§ 15:8 Scott v. U.S.
§ 15:9 Comment

II. FACTORS EFFECTING MINIMIZATION

§ 15:10 In general
§ 15:11 Goals of the investigation; scope of the criminal activity
§ 15:12 Nature and use of phone or premises
§ 15:13 Foreign language
§ 15:14 Use of coded, guarded, or cryptic language

III. MINIMIZATION PROCEDURES

§ 15:15 “Subject to interception”
§ 15:16 Initial minimization procedures
§ 15:17 Monitoring the beginning of each conversation
§ 15:18 Spot monitoring
§ 15:19 Patterns and categories of conversations

IV. SPECIAL MINIMIZATION PROBLEMS

§ 15:20 Bugs
§ 15:21 Public phone, public premises
§ 15:22 Minimization and electronic communications; faxes; audio files
§ 15:23 Potentially privileged communications

© 2018 Thomson Reuters, 12/2018
CHAPTER 16. OTHER CRIMES AND CRIMINALS

§ 16:1 In general

I. INTERCEPTION; INVESTIGATIVE DISCLOSURE AND USE; AMENDING THE INTERCEPT ORDER

§ 16:2 Interception: “plain view doctrine” analogy
§ 16:3 Interception: state variations
§ 16:5 Adding crimes by amendment
§ 16:6 Adding crimes by amendment: state variations
§ 16:6.50 Different criminals, different crimes
§ 16:7 New individuals

II. TESTIMONIAL USE OF “OTHER CRIMES” EVIDENCE

§ 16:8 Overview: 18 U.S.C.A. § 2517(5); state law

A. DEFINING “OTHER OFFENSES”

§ 16:9 In general
§ 16:10 Similar or related crimes: federal law
§ 16:11 Similar or related crimes: state variations
§ 16:12 “Umbrella” crimes: RICO and the like
§ 16:13 Inter-jurisdictional issues
§ 16:14 Evaluation
§ 16:15 Non-designated offenses: federal law
§ 16:16 Non-designated offenses: state law

B. OTHER ISSUES

§ 16:17 Defining “evidence derived”
§ 16:18 Form of subsequent application and judicial approval order
§ 16:19 State variations
§ 16:20 Role of the issuing or approving judge; role of suppression hearing judge
Table of Contents

§ 16:21 “As soon as practicable” requirement
§ 16:22 “As soon as practicable”: interjurisdictional issues
§ 16:23 Availability of suppression remedy
§ 16:24 Attacking subsequent applications
§ 16:25 Testimonial use in non-criminal proceedings

CHAPTER 17. [Reserved]

CHAPTER 18. INVENTORY AND NOTICE
§ 18:1 In general
§ 18:2 Filing “return”
§ 18:3 Whom to serve
§ 18:4 Contents and service of inventory
§ 18:5 Postponing service
§ 18:6 —Form and contents of postponement order
§ 18:7 Effects of non-compliance: U.S. v. Donovan
§ 18:8 Subsequent additions to inventory list
§ 18:9 Showing prejudice
§ 18:10 Notice prior to trial or hearing
§ 18:11 New York rule
§ 18:12 Administrative reports

CHAPTER 19. SEALING, CUSTODY AND STORAGE OF RECORDINGS

I. OVERVIEW
§ 19:1 In general
§ 19:2 18 U.S.C.A. § 2518(8)(a)
§ 19:3 What else must be “sealed”?
§ 19:4 “Extensions” of an intercept order
§ 19:5 Procedure
§ 19:6 Communications recorded by computer
§ 19:7 Suppression remedy; standing to assert non-compliance
§ 19:8 “Evidence derived”; extent of suppression; 18 U.S.C. § 2517(2)

II. THE “IMMEDIACY” REQUIREMENT
§ 19:9 In general
§ 19:10 U.S. v. Ojedia Rios; subsequent federal case law

© 2018 Thomson Reuters, 12/2018
§ 19:11 State courts
§ 19:12 Termination of interception prior to termination of the order
§ 19:13 Less than “immediate” response by the judge

III. “SATISFACTORY EXPLANATION”
§ 19:14 In general; Ojeda Rios
§ 19:15 Relevant factors
§ 19:16 Litigating the issue: burden of proof; standard of appellate review
§ 19:17 Length of delay; protection against tampering
§ 19:18 Reason for the delay: misunderstanding as to legal requirements
§ 19:19 Other reasons for a delay in sealing

IV. AUTHORIZED UNSEALING; RESEALING, AND DESTRUCTION OF RECORDINGS
§ 19:20 In general
§ 19:21 Authorized unsealing
§ 19:22 Unsealing procedure
§ 19:23 Resealing
§ 19:24 Application of suppression remedy
§ 19:25 “Satisfactory explanation”
§ 19:26 Destruction of recordings

CHAPTER 20. [Reserved]

Volume 3

PART V. COMPUTERS, THE INTERNET AND THE LAW

CHAPTER 21. INTERNET TECHNOLOGY AND CYBERCRIME: AN OVERVIEW

I. THE INTERNET TECHNOLOGY
§ 21:1 Overview
§ 21:2 The Internet technology
§ 21:3 Terminology and definitions; common abbreviations
§ 21:4 The Internet and Voice over Internet Protocol or VoIP
§ 21:5 VoIP case decisions and VoIP issues under current statutory scheme

PART II. INTERNET BASED SURVEILLANCE TECHNOLOGY

§ 21:6 An Overview of Internet Surveillance Technology
§ 21:7 Packet Sniffers
§ 21:8 Filters
§ 21:9 Spyware
§ 21:10 Cookies
§ 21:11 Key Logger Systems

PART III. INTERNET CRIMES AND CIVIL ACTIONS: AN OVERVIEW

§ 21:12 The Internet and Cybercrime
§ 21:13 Phishing
§ 21:14 Botnets
§ 21:15 Child pornography
§ 21:16 Civil actions arising from Internet crimes

CHAPTER 22. COMPUTERS, THE INTERNET AND THE FOURTH AMENDMENT

§ 22:1 Overview
§ 22:2 Department of Justice: Guidelines and Manuals
§ 22:3 Legislative considerations
§ 22:4 International considerations in searching computers
§ 22:5 Applying the Fourth Amendment to computer searches
§ 22:5.50 The Fourth Amendment: IP addresses and blogger identities
§ 22:6 Is a computer a “container” for Fourth Amendment purposes?
§ 22:7 Does an Internet connection change one’s reasonable expectation of privacy?
CHAPTER 23. SEARCHING COMPUTERS: WARRANT EXCEPTIONS

§ 23:1 Overview
§ 23:2 Private searches: in general
§ 23:3 “Private” searcher versus a “government” searcher
§ 23:4 Private searches: burden of proof and standard of review
§ 23:5 Employment-related searches
§ 23:6 Private-sector employment searches
§ 23:7 Public-sector employment searches
§ 23:8 School and university computer system searches
§ 23:9 Posting notice to the user
§ 23:10 Parent/child computer searches and surveillance
§ 23:11 Consent to search
§ 23:12 Scope of consent
§ 23:13 Drafting consent forms
§ 23:14 Third party consent; in general
§ 23:15 Third party consent: actual authority to consent
§ 23:16 Third-party consent: apparent authority
§ 23:17 Third party consent: spousal/partner consent and passwords
§ 23:18 Miscellaneous third party consent issues
§ 23:19 Border searches
§ 23:20 Parole searches
§ 23:21 Search incident to arrest
§ 23:22 Evidence of other crimes; “plain view”
§ 23:23 Exigent circumstances
§ 23:24 Special needs exception
§ 23:25 Internet postings; Internet access; share software

CHAPTER 24. SEARCHING COMPUTERS: WARRANT REQUIREMENTS

§ 24:1 Introduction
§ 24:2 Legislation and statutory warrant requirements
TABLE OF CONTENTS

§ 24:3 Pre-warrant, application, and affidavit considerations
§ 24:4 Drafting the warrant
§ 24:5 Drafting the application and affidavit in support
§ 24:6 Insufficiencies and errors in application and affidavit
§ 24:7 Supporting documentation: photographs, digital images, video clips
§ 24:8 Probable cause
§ 24:9 Law enforcement search logistics: what gets seized; where the search takes place—When data is no longer on the device but in the cloud
§ 24:10 Time of search
§ 24:11 Specificity, particularity, and scope of the search
§ 24:12 Search methodology or protocols
§ 24:13 Search for additional contraband or records of the same type

CHAPTER 25. FEDERAL COMPUTER LEGISLATION

§ 25:1 Overview
§ 25:2 Constitutional considerations and federal legislation
§ 25:5 ECPA’s Stored Communications Act, 18 U.S.C.A. §§ 2701–2712
§ 25:7 Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030
§ 25:8 Fraud and related activity in Connection with access devices, 18 U.S.C.A. § 1029
§ 25:9 Identity theft, 18 U.S.C.A. § 1028(a)(7)
§ 25:10 Aggravated identity theft, 18 U.S.C.A. § 1028A
§ 25:12 Cable Act, 47 U.S.C.A. § 551
§ 25:15 Copyright statutes
§ 25:16 Copyright Infringement Act and No Electronic Theft Act, 18 U.S.C.A. § 506

© 2018 Thomson Reuters, 12/2018
CHAPTER 26. COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C.A. § 1030

§ 26:1 Introduction
§ 26:2 Overview of CFAA, 18 U.S.C.A. § 1030
§ 26:3 Federal Jurisdiction under CFAA, 18 U.S.C.A. § 1030
§ 26:3.10 Venue under CFAA, 18 U.S.C.A § 1030
§ 26:4 CFAA definitions
§ 26:5 Access “without authorization” or “exceeding authorized access”
§ 26:5.50 CFAA—Anti-hacker statute or employer-employee regulation?
§ 26:6 Stating a civil claim under CFAA
§ 26:7 CFAA's statute of limitations for civil claims
§ 26:8 What constitutes “loss”; meeting the statutory threshold requirement
§ 26:9 Injunctive relief in CFAA-based litigation
§ 26:10 CFAA and criminal case issues

CHAPTER 27. STATE LEGISLATION

§ 27:1 Overview
**I. FEDERAL LEGISLATION: A MODEL FOR STATE LEGISLATION**

§ 27:2 Federal legislation—Computer crime

§ 27:3 Federal legislation: Email regulation and the CAN-SPAM Act

§ 27:4 Federal legislation *(Reserved)*

§ 27:5 Federal Uniform Electronic Transactions Act

**II. STATE LEGISLATION**

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 27:6</td>
<td>State legislation: In general</td>
</tr>
<tr>
<td>§ 27:7</td>
<td>Alabama</td>
</tr>
<tr>
<td>§ 27:8</td>
<td>—Computer Crime</td>
</tr>
<tr>
<td>§ 27:9</td>
<td>—Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:10</td>
<td>—Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:11</td>
<td>—Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:12</td>
<td>—Unmanned Aircraft Vehicles (UAVs or Drones)</td>
</tr>
<tr>
<td>§ 27:13</td>
<td>—Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:14</td>
<td>Alaska</td>
</tr>
<tr>
<td>§ 27:15</td>
<td>—Computer crime</td>
</tr>
<tr>
<td>§ 27:16</td>
<td>—Deceptive business practices</td>
</tr>
<tr>
<td>§ 27:17</td>
<td>—Computer contaminants: malicious software activities</td>
</tr>
<tr>
<td>§ 27:18</td>
<td>—Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:19</td>
<td>—Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:20</td>
<td>—Regulation of email</td>
</tr>
<tr>
<td>§ 27:21</td>
<td>—Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:22</td>
<td>—Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:23</td>
<td>—Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:24</td>
<td>Arizona</td>
</tr>
<tr>
<td>§ 27:25</td>
<td>—Computer crime</td>
</tr>
<tr>
<td>§ 27:26</td>
<td>—Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:27</td>
<td>—Computer contaminants: malicious software activities</td>
</tr>
<tr>
<td>§ 27:28</td>
<td>—Regulation of email</td>
</tr>
<tr>
<td>§ 27:29</td>
<td>—Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:30</td>
<td>—Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:31</td>
<td>—Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:32</td>
<td>Arkansas</td>
</tr>
<tr>
<td>§ 27:33</td>
<td>—Computer crime</td>
</tr>
<tr>
<td>§ 27:34</td>
<td>—Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:35</td>
<td>—Computer contaminants: malicious software activities</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>§ 27:36</td>
<td>Internet privacy</td>
</tr>
<tr>
<td>§ 27:37</td>
<td>Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:38</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:39</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:40</td>
<td>California</td>
</tr>
<tr>
<td>§ 27:41</td>
<td>Computer crime</td>
</tr>
<tr>
<td>§ 27:42</td>
<td>Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:43</td>
<td>Cyber piracy</td>
</tr>
<tr>
<td>§ 27:44</td>
<td>Internet privacy</td>
</tr>
<tr>
<td>§ 27:45</td>
<td>Internet privacy-Elected Officials</td>
</tr>
<tr>
<td>§ 27:46</td>
<td>Regulation of email</td>
</tr>
<tr>
<td>§ 27:47</td>
<td>Computer contaminants: malicious software activities</td>
</tr>
<tr>
<td>§ 27:48</td>
<td>Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:49</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:50</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:51</td>
<td>Colorado</td>
</tr>
<tr>
<td>§ 27:52</td>
<td>Computer crime</td>
</tr>
<tr>
<td>§ 27:53</td>
<td>Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:54</td>
<td>Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:55</td>
<td>Internet privacy</td>
</tr>
<tr>
<td>§ 27:56</td>
<td>Regulation of email</td>
</tr>
<tr>
<td>§ 27:57</td>
<td>Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:58</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:59</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:60</td>
<td>Connecticut</td>
</tr>
<tr>
<td>§ 27:61</td>
<td>Computer crime</td>
</tr>
<tr>
<td>§ 27:62</td>
<td>Cyber piracy</td>
</tr>
<tr>
<td>§ 27:63</td>
<td>Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:64</td>
<td>Internet privacy</td>
</tr>
<tr>
<td>§ 27:65</td>
<td>Regulation of email</td>
</tr>
<tr>
<td>§ 27:66</td>
<td>Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:67</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:68</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:69</td>
<td>Delaware</td>
</tr>
<tr>
<td>§ 27:70</td>
<td>Computer crime</td>
</tr>
<tr>
<td>§ 27:71</td>
<td>Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:72</td>
<td>Internet privacy</td>
</tr>
<tr>
<td>§ 27:73</td>
<td>Court of Chancery</td>
</tr>
<tr>
<td>§ 27:74</td>
<td>Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:75</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:76</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
</tbody>
</table>
## Table of Contents

| § 27:77  | Florida |
| § 27:78  | —Computer crime |
| § 27:79  | —Child sex offenses involving computers |
| § 27:80  | —Regulation of email |
| § 27:81  | —Civil cause of action by statute |
| § 27:82  | —Unmanned Aircraft Surveillance |
| § 27:83  | —Uniform Electronic Transactions Act |
| § 27:84  | Georgia |
| § 27:85  | —Computer crime |
| § 27:85.50  | —Computer Contaminants |
| § 27:86  | —Regulation of email |
| § 27:87  | —Civil cause of action by statute |
| § 27:88  | —Unmanned Aircraft Surveillance |
| § 27:89  | —Uniform Electronic Transactions Act |
| § 27:90  | Hawaii |
| § 27:91  | —Computer Crime |
| § 27:92  | —Internet privacy |
| § 27:93  | —Civil cause of action by statute |
| § 27:94  | —Unmanned Aircraft Surveillance |
| § 27:95  | —Uniform Electronic Transactions Act |
| § 27:96  | Idaho |
| § 27:97  | —Computer crime |
| § 27:98  | —Child sex offenses involving computers |
| § 27:99  | —Regulation of email |
| § 27:100  | —Civil cause of action by statute |
| § 27:101  | —Unmanned Aircraft Surveillance |
| § 27:102  | —Uniform Electronic Transactions Act |
| § 27:103  | Illinois |
| § 27:104  | —Computer crime and regulation of email |
| § 27:105  | —Child and adult sex offenses involving computers |
| § 27:106  | —Cyberstalking |
| § 27:107  | —Online property offenses |
| § 27:108  | —Regulation of email |
| § 27:109  | —Internet privacy |
| § 27:110  | —Registration of an Internet Auction Listing Service |
| § 27:111  | —Civil cause of action by statute |
| § 27:112  | —Unmanned Aircraft Surveillance |
| § 27:113  | —UETA and the Electronic Commerce Security Act |
| § 27:114  | Indiana |
| § 27:115  | —Computer crime |

© 2018 Thomson Reuters, 12/2018  lxxi
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 27:116</td>
<td>Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:117</td>
<td>Professional gambling</td>
</tr>
<tr>
<td>§ 27:118</td>
<td>Computer contaminants: malicious software activities</td>
</tr>
<tr>
<td>§ 27:119</td>
<td>Regulation of email</td>
</tr>
<tr>
<td>§ 27:120</td>
<td>Indiana—Civil cause of action by statute [Reserved]</td>
</tr>
<tr>
<td>§ 27:121</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:122</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:123</td>
<td>Iowa [Reserved]</td>
</tr>
<tr>
<td>§ 27:124</td>
<td>Computer Crime</td>
</tr>
<tr>
<td>§ 27:125</td>
<td>Computer contaminants: malicious software activities</td>
</tr>
<tr>
<td>§ 27:126</td>
<td>Regulation of email</td>
</tr>
<tr>
<td>§ 27:127</td>
<td>Civil Actions Arising from Computer Crime</td>
</tr>
<tr>
<td>§ 27:128</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:129</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:130</td>
<td>Kansas</td>
</tr>
<tr>
<td>§ 27:131</td>
<td>Computer crime</td>
</tr>
<tr>
<td>§ 27:132</td>
<td>Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:133</td>
<td>Regulation of email</td>
</tr>
<tr>
<td>§ 27:134</td>
<td>Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:135</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:136</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:137</td>
<td>Kentucky</td>
</tr>
<tr>
<td>§ 27:138</td>
<td>Computer crime</td>
</tr>
<tr>
<td>§ 27:139</td>
<td>Child and adult sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:140</td>
<td>Requirements for in-state pharmacy doing business via Internet</td>
</tr>
<tr>
<td>§ 27:141</td>
<td>Civil Actions Arising from Computer Crime Legislation</td>
</tr>
<tr>
<td>§ 27:142</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:143</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:144</td>
<td>Louisiana</td>
</tr>
<tr>
<td>§ 27:145</td>
<td>Computer crime</td>
</tr>
<tr>
<td>§ 27:146</td>
<td>Professional Gambling</td>
</tr>
<tr>
<td>§ 27:147</td>
<td>Computer contaminants: malicious software activities</td>
</tr>
<tr>
<td>§ 27:148</td>
<td>Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:149</td>
<td>Computer contaminants: malicious software activities</td>
</tr>
<tr>
<td>§ 27:150</td>
<td>Anti-phishing legislation</td>
</tr>
<tr>
<td>§ 27:151</td>
<td>—Regulation of email</td>
</tr>
<tr>
<td>§ 27:152</td>
<td>Louisiana—Civil cause of action by statute [Reserved]</td>
</tr>
<tr>
<td>§ 27:153</td>
<td>—Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:154</td>
<td>—Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:155</td>
<td>Maine</td>
</tr>
<tr>
<td>§ 27:156</td>
<td>—Computer crime</td>
</tr>
<tr>
<td>§ 27:157</td>
<td>—Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:158</td>
<td>—Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:159</td>
<td>—Regulation of email</td>
</tr>
<tr>
<td>§ 27:160</td>
<td>Maine—Civil cause of action by statute [Reserved]</td>
</tr>
<tr>
<td>§ 27:161</td>
<td>—Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:162</td>
<td>—Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:163</td>
<td>Maryland</td>
</tr>
<tr>
<td>§ 27:164</td>
<td>—Computer crime</td>
</tr>
<tr>
<td>§ 27:165</td>
<td>—Regulation of email</td>
</tr>
<tr>
<td>§ 27:166</td>
<td>—Internet privacy</td>
</tr>
<tr>
<td>§ 27:167</td>
<td>—Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:168</td>
<td>—Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:169</td>
<td>—Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:170</td>
<td>Massachusetts</td>
</tr>
<tr>
<td>§ 27:171</td>
<td>—Computer crime</td>
</tr>
<tr>
<td>§ 27:172</td>
<td>—Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:173</td>
<td>—Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:174</td>
<td>—Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:175</td>
<td>Michigan</td>
</tr>
<tr>
<td>§ 27:176</td>
<td>—Computer crime</td>
</tr>
<tr>
<td>§ 27:177</td>
<td>—Internet privacy</td>
</tr>
<tr>
<td>§ 27:178</td>
<td>—Regulation of email</td>
</tr>
<tr>
<td>§ 27:179</td>
<td>—Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:180</td>
<td>—Anti-Terrorism Act</td>
</tr>
<tr>
<td>§ 27:181</td>
<td>—Civil causes of action by statute</td>
</tr>
<tr>
<td>§ 27:182</td>
<td>—Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:183</td>
<td>—Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:184</td>
<td>Minnesota</td>
</tr>
<tr>
<td>§ 27:185</td>
<td>—Computer crime</td>
</tr>
<tr>
<td>§ 27:186</td>
<td>—Regulation of email</td>
</tr>
<tr>
<td>§ 27:187</td>
<td>—Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:188</td>
<td>—Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:189</td>
<td>—Internet privacy</td>
</tr>
<tr>
<td>§ 27:190</td>
<td>—Regulation of email</td>
</tr>
<tr>
<td>§ 27:191</td>
<td>—Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:192</td>
<td>—Unmanned Aircraft Surveillance</td>
</tr>
</tbody>
</table>
§ 27:193 —Uniform Electronic Transactions Act
§ 27:194 Mississippi
§ 27:195 —Computer crime
§ 27:196 —Adult and child sex offenses involving computers
§ 27:197 —Internet or computer-assisted hunting
§ 27:198 —Civil Causes of Action
§ 27:199 —Unmanned Aircraft Surveillance
§ 27:200 —Uniform Electronic Transactions Act
§ 27:201 Missouri
§ 27:202 —Computer crime
§ 27:203 —Child sex offenses involving computers
§ 27:204 —Internet privacy
§ 27:205 —Regulation of email
§ 27:206 —Civil cause of action by statute
§ 27:207 —Unmanned Aircraft Surveillance
§ 27:208 —Uniform Electronic Transactions Act
§ 27:209 Montana
§ 27:210 —Computer crime
§ 27:211 —Internet privacy and identity theft
§ 27:212 —Civil cause of action by statute
§ 27:213 —Unmanned Aircraft Surveillance
§ 27:214 —Uniform Electronic Transactions Act
§ 27:215 Nebraska
§ 27:216 —Computer crime
§ 27:217 —Child sex offenses involving computers
§ 27:218 —Internet privacy
§ 27:219 —Internet or computer-assisted hunting
§ 27:220 —Unmanned Aircraft Surveillance
§ 27:221 —Uniform Electronic Transactions Act
§ 27:222 Nevada
§ 27:223 —Computer crime
§ 27:224 —Regulation of email
§ 27:225 —Adult and Child sex offenses involving computers
§ 27:226 —Internet pharmacies
§ 27:227 —Internet privacy
§ 27:228 —Civil cause of action by statute
§ 27:229 —Unmanned Aircraft Surveillance
§ 27:230 —Uniform Electronic Transactions Act
§ 27:231 New Hampshire
§ 27:232 —Computer crime

lxxiv
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 27:233</td>
<td>Adult and child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:234</td>
<td>Computer contaminants: malicious software activities</td>
</tr>
<tr>
<td>§ 27:235</td>
<td>Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:236</td>
<td>Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:237</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:238</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:239</td>
<td>New Jersey</td>
</tr>
<tr>
<td>§ 27:240</td>
<td>Computer crime</td>
</tr>
<tr>
<td>§ 27:241</td>
<td>Adult and child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:242</td>
<td>Regulation of Internet dating</td>
</tr>
<tr>
<td>§ 27:243</td>
<td>Internet privacy</td>
</tr>
<tr>
<td>§ 27:244</td>
<td>Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:245</td>
<td>Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:246</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:247</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:248</td>
<td>New Mexico</td>
</tr>
<tr>
<td>§ 27:249</td>
<td>Computer crime</td>
</tr>
<tr>
<td>§ 27:250</td>
<td>Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:251</td>
<td>Identity Theft and Internet Privacy</td>
</tr>
<tr>
<td>§ 27:252</td>
<td>Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:253</td>
<td>Regulation of email</td>
</tr>
<tr>
<td>§ 27:254</td>
<td>Civil cause of action by statute</td>
</tr>
<tr>
<td>§ 27:255</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:256</td>
<td>Uniform Electronic Transactions Act</td>
</tr>
<tr>
<td>§ 27:257</td>
<td>New York</td>
</tr>
<tr>
<td>§ 27:258</td>
<td>Computer Crime</td>
</tr>
<tr>
<td>§ 27:259</td>
<td>Child sex offenses involving computers</td>
</tr>
<tr>
<td>§ 27:260</td>
<td>Internet or computer-assisted hunting</td>
</tr>
<tr>
<td>§ 27:261</td>
<td>Cyber piracy</td>
</tr>
<tr>
<td>§ 27:262</td>
<td>Internet privacy</td>
</tr>
<tr>
<td>§ 27:263</td>
<td>Computer contaminants: malicious software activities</td>
</tr>
<tr>
<td>§ 27:264</td>
<td>Regulation of email</td>
</tr>
<tr>
<td>§ 27:265</td>
<td>Consumer Protection</td>
</tr>
<tr>
<td>§ 27:266</td>
<td>New York—Civil cause of action by statute [Reserved]</td>
</tr>
<tr>
<td>§ 27:267</td>
<td>Unmanned Aircraft Surveillance</td>
</tr>
<tr>
<td>§ 27:268</td>
<td>Uniform Electronic Transaction Act</td>
</tr>
<tr>
<td>§ 27:269</td>
<td>North Carolina</td>
</tr>
<tr>
<td>§ 27:270</td>
<td>Computer crime</td>
</tr>
</tbody>
</table>

© 2018 Thomson Reuters, 12/2018
§ 27:271 —Cyberstalking
§ 27:272 —Child sex offenses involving computers
§ 27:273 —Internet privacy
§ 27:274 Internet ticket sales
§ 27:275 North Carolina—Civil cause of action by statute
§ 27:276 —Unmanned Aircraft Surveillance
§ 27:277 —Uniform Electronic Transactions Act
§ 27:278 North Dakota
§ 27:279 —Computer crime
§ 27:280 —Child sex offenses involving computers
§ 27:281 —Anti-phishing
§ 27:282 —Regulation of email
§ 27:283 —Internet livestock market
§ 27:284 —Civil cause of action by statute
§ 27:285 —Unmanned Aircraft Surveillance
§ 27:286 —Uniform Electronic Transactions Act
§ 27:287 Ohio
§ 27:288 —Computer crime
§ 27:289 —Cyberstalking
§ 27:290 —Regulation of email
§ 27:291 —Internet privacy
§ 27:292 —Civil cause of action by statute
§ 27:293 —Unmanned Aircraft Surveillance
§ 27:294 —Uniform Electronic Transactions Act
§ 27:295 Oklahoma
§ 27:296 —Computer crime
§ 27:297 —Child sex offenses involving computers
§ 27:298 —Internet or computer-assisted hunting
§ 27:299 —Internet privacy
§ 27:300 —Regulation of email
§ 27:301 —Anti-Phishing
§ 27:302 —Civil cause of action by statute
§ 27:303 —Unmanned Aircraft Surveillance
§ 27:304 —Uniform Electronic Transactions Act
§ 27:305 Oregon
§ 27:306 —Computer crime
§ 27:307 —Child sex offenses involving computers
§ 27:308 Oregon—Civil cause of action by statute [Reserved]
§ 27:309 —Unmanned Aircraft Surveillance
§ 27:310 —Uniform Electronic Transactions Act
§ 27:311 Pennsylvania
§ 27:352 — Unmanned Aircraft Surveillance
§ 27:353 — Uniform Electronic Transactions Act
§ 27:354 Texas
§ 27:355 — Computer Crime
§ 27:356 — Child sex offenses involving computers
§ 27:357 — Internet Hunting
§ 27:358 — Regulation of email
§ 27:359 — Anti-Phishing
§ 27:360 — Computer Contaminants: Malicious Software Activities
§ 27:361 — Internet privacy
§ 27:362 — Internet Contracts
§ 27:363 — Civil cause of action by statute
§ 27:364 — Unmanned Aircraft Surveillance
§ 27:365 — Uniform Electronic Transactions Act
§ 27:366 Utah
§ 27:367 — Computer Crime
§ 27:368 — Child sex offenses involving computers
§ 27:369 — Internet or computer-assisted hunting
§ 27:370 — Computer contaminants: malicious software activities
§ 27:371 — Unfair Competition
§ 27:372 — Civil cause of action by statute
§ 27:373 — Unmanned Aircraft Surveillance
§ 27:374 — Uniform Electronic Transactions Act
§ 27:375 Vermont
§ 27:376 — Computer Crime
§ 27:377 — Internet Hunting
§ 27:378 — Uniform Electronic Transactions Act
§ 27:378.50 — Unmanned Aircraft Surveillance
§ 27:379 Virginia
§ 27:380 — Computer Crime
§ 27:381 — Regulation of email
§ 27:382 — Adult and child sex offenses involving computers
§ 27:383 — Internet or computer-assisted hunting
§ 27:384 — Internet privacy
§ 27:385 — Civil cause of action by statute
§ 27:386 — Unmanned Aircraft Surveillance
§ 27:387 — Uniform Electronic Transactions Act
§ 27:388 Washington
§ 27:389 — Computer Crime
§ 27:390 — Cyberstalking

lxviii
PART VI. SURVEILLANCE WITH OTHER ELECTRONIC DEVICES; RADIO AND TELECOMMUNICATIONS

CHAPTER 28. CELLULAR PHONES: TECHNOLOGY, INVESTIGATION AND TRACKING

I. TECHNOLOGY, INVESTIGATION AND TRACKING

§ 28:1 Introduction
§ 28:2 Cellular phone technology
§ 28:3 Cellular phones, the Fourth Amendment and Title III
§ 28:4 Cell phone as tracking device: overview; vocabulary
§ 28:5 The statutory scheme: 18 U.S.C.A. § 2703(d) in context
§ 28:6 Does obtaining cell site location information from a telecommunications service provider constitute a Fourth Amendment “search”?
§ 28:6.10 Is it a search?—Traditional Fourth Amendment doctrine
§ 28:6.20 — U.S. v. Jones; California v. Riley
§ 28:7 HCSLI: federal case law
§ 28:7.50 State law
§ 28:7.60 HCSLI: The issues, in brief
§ 28:7.70 HCSLI: evaluation
§ 28:8 “Tower dumps”
§ 28:9 Prospective CSLI
§ 28:10 Jurisdictional issues with cellular and other mobile phones
§ 28:11 Cellular phone calls: penalties for unlawful interception, use, disclosure
§ 28:12 Cellular evidence
§ 28:13 Cellular phone calls: miscellany
§ 28:14 Cordless telephones: the technology and the law
§ 28:15 Scanner issues with respect to cellular and cordless phones
§ 28:16 Disposable and “throw-away” cellular telephones: recommendations for law enforcement

§§ 28:16.50 through 28:28 [Reserved]
§ 28:29 Cellular site location: trial issues

II. SEIZING, ANSWERING AND SEARCHING CELL PHONES

A. PRELIMINARY MATTERS

§ 28:30 Introduction
§ 28:31 Seizing an arrestee’s cell phone
§ 28:32 Pre-arrest (a) seizures of a suspect’s phone, or (b) police calls to a detainee’s cell phone
B. SEARCHING CELL PHONES INCIDENT TO ARREST: RILEY V. CALIFORNIA

§ 28:33 Search “incident to arrest”: constitutional principles
§ 28:34 Riley v. California: background
§ 28:35 Riley: summary
§ 28:36 Riley: cell phones and the justifications for the search incident doctrine
§ 28:37 Riley: privacy interests—The nature of a cell phone
§ 28:38 Riley: categorical, not nuanced, approach
§ 28:39 Pre-Riley searches and the “good faith exception”

C. APPLYING THE WARRANT REQUIREMENT TO CELL PHONE SEARCHES

§ 28:40 Introduction
§ 28:41 Probable cause
§ 28:42 “Particularly describing the place to be searched”
§ 28:43 “Particularly describing . . . the . . . thing to be seized”
§ 28:44 “Minimization”

D. SEARCHING A CELL PHONE WITHOUT A WARRANT IN EXIGENT CIRCUMSTANCES

1. In General
§ 28:45 The “exigent circumstances” doctrine: constitutional principles
§ 28:46 Riley’s discussion of exigent circumstances
§ 28:47 “Imminent danger” exigencies; apprehend fleeing felon
§ 28:48 Evidence-destruction exigencies

2. Applying the “evidence-destruction” exigency to cell phones
§ 28:48 Answering the phone; reading incoming text messages; returning or initiating calls or messages
§ 28:49 Where probable cause exists that defendant used the phone to commit the arrest offense

E. OTHER ISSUES

§ 28:50 Exigent circumstances in the absence of a probable cause connection
§ 28:51 Exigent searches of a cell phone’s memory
§ 28:52 Duration of exigency

III. OTHER ISSUES
§ 28:53 Answering a cell phone during a search of a premises
§ 28:54 Standing to challenge admissibility of evidence obtained from or regarding a suspect’s cell phone

CHAPTER 29. ELECTRONIC TRACKING DEVICES

I. IN GENERAL
§ 29:1 Introduction
§ 29:2 Overview of electronic tracking case-law
§ 29:3 Tracking devices, 18 U.S.C.A. § 3117(b)
§ 29:4 Definitions

II. INSTALLATION
§ 29:5 Installation: in general
§ 29:6 Consensual installations
§ 29:7 Consensual installations: the Karo decision: precursor chemicals
§ 29:8 Consensual installations: post-Karo state decisions
§ 29:9 Other consensual installations; in general
§ 29:10 Consensual installations: vehicles
§ 29:11 Consensual installations: installation into contraband; “tainted” transactions
§ 29:12 Trespassory installation; in general
§ 29:13 Trespassory installation; vehicles

III. MONITORING
§ 29:14 In general
§ 29:15 In-transit monitoring; Knotts
§ 29:16 In-transit monitoring; Knotts: devices that reveal that the container has been opened
§ 29:17 Private location monitoring; Karo
§ 29:18 Post-Karo state action
§ 29:19 General vicinity monitoring; Knotts and Karo
CHAPTER 30. TECHNOLOGICALLY ENHANCED VISUAL SURVEILLANCE; OTHER FORMS OF SURVEILLANCE TECHNOLOGY

I. OVERVIEW
§ 30:1 Introduction
§ 30:2 Katz v. United States
§ 30:3 Kyllo v. United States: case background
§ 30:4 Kyllo v. United States: defining “search”
§ 30:5 Kyllo v. United States: technology and the Katz test
§ 30:6 Kyllo v. United States: “constitutionally protected area”
§ 30:7 Kyllo v. United States: the dissent
§ 30:8 Kyllo v. United States: an evaluation
§ 30:9 Three factors

II. ARTIFICIAL ILLUMINATION
§ 30:10 Items and conduct exposed to the public
§ 30:11 Illumination of private locations

III. AERIAL SURVEILLANCE
§ 30:12 In general; California v. Ciraolo
§ 30:13 Altitude and reasonable expectations; Florida v. Riley
§ 30:14 Satellite imagery

IV. IMAGE MAGNIFICATION
A. BINOCULARS AND TELESCOPES
§ 30:15 Telescopes and binoculars: in general
§ 30:16 Officer’s location when using telescope or binoculars
§ 30:17 Location and matters observed by binoculars
§ 30:18 Surveillance of “intimate details”

B. HIGH RESOLUTION PHOTOGRAPHY AND THE DOW CHEMICAL CASE
§ 30:19 In general
§ 30:20 Dow and the sophistication of surveillance
§ 30:21 Dow: measures and countermeasures

C. DOW: EVALUATION

§ 30:22 Dow: an overview
§ 30:23 Comparison of visual surveillance to interception of communications
§ 30:24 Dow and Kyllo: sophistication and “general availability”

V. HEAT-SENSING SURVEILLANCE

§ 30:25 Thermal imaging
§ 30:26 Kyllo v. United States: the legality of warrantless thermal imaging searches
§ 30:27 Thermal imaging cases post-Kyllo
§ 30:28 Application of Kyllo to other forms of technologically enhanced surveillance

VI. ELECTRONIC VIDEO SURVEILLANCE

§ 30:29 Electronic video surveillance: in general
§ 30:30 The Fourth Amendment and video surveillance
§ 30:31 Videotaping in public areas
§ 30:32 Videotaping in schools
§ 30:33 Videotaping in the workplace
§ 30:34 Videotaping on private property or in the home
§ 30:35 Video surveillance warrants: judicial authority and application considerations
§ 30:36 Videotape evidence: admissibility, authentication and other issues
§ 30:37 Video surveillance as a crime or civil cause of action
§ 30:38 Video surveillance and invasion of privacy
§ 30:39 Closed Circuit Television (CCTV)

VII. SURVEILLANCE AND UNMANNED AERIAL VEHICLES (UAVS) OR DRONES

§ 30:41 An overview
§ 30:42 Terminology
§ 30:43 UAV capabilities for technologically enhanced surveillance

© 2018 Thomson Reuters, 12/2018
§ 30:44 UAVs: usage by law enforcement: an overview
§ 30:45 Legally appropriate UAV usage by law enforcement
§ 30:46 Law enforcement UAV usage and Fourth Amendment
§ 30:47 UAVs and use by domestic law enforcement: a case law overview
§ 30:48 Federal Aviation Administration and UAV regulation
§ 30:49 UAV legislative regulation: an overview
§ 30:50 UAV: potentially applicable existing electronic surveillance legislation
§ 30:51 UAV-targeted or specific legislation

VIII. WIRELESS NETWORKS
§ 30:52 Private industry surveillance
§ 30:53 Government surveillance

CHAPTER 31. BIOMETRICS
§ 31:1 Biometrics: introduction
§ 31:2 Biometrics: a history
§ 31:3 [Reserved]
§ 31:4 Biometrics: a general overview of biometric technology
§ 31:5 Biometrics: developing technology trends and legal implications
§ 31:6 Biometric identification: finger scan, fingerprint and palm print
§ 31:7 Biometric identification: hand geometry
§ 31:8 Biometric identification: voice recognition
§ 31:9 Biometric identification: retina scan
§ 31:10 Biometric identification: iris scan
§ 31:11 Biometric identification: facial or face recognition
§ 31:12 Biometric identification: vein recognition
§ 31:13 Biometric identification: skin texture characteristics
§ 31:14 Biometric identification: age group recognition
§ 31:15 Dynamic signature
§ 31:16 Biometric identification: gait analysis
§ 31:17 Biometric identification: DNA
| § 31:18   | Biometric identification: mobile multimodal biometric identification |
| §§ 31:19 to 31:24 | [Reserved] |
| § 31:25   | Biometric legislation in the United States: an overview |
| § 31:26   | Biometric legislation: Privacy Act of 1974 |
| § 31:27   | Enhanced Border Security and Visa Reform Entry Act of 2002 |
| § 31:28   | Biometric legislation: Intelligence Reform and Terrorism Act of 2004 |
| § 31:29   | Biometric legislation: REAL ID Act of 2005 |
| § 31:30   | Biometrics and State Legislation: an overview |
| § 31:30.10 | Illinois' Biometric Privacy Information Act |
| § 31:30.20 | Texas' Capture or Use of Biometric Identifier Act |
| § 31:30.30 | Existing legislation: Adding biometric data to the definition of “personal information” under state data breach notification statutes |
| § 31:30.40 | Pending legislation |
| §§ 31:31 to 31:35 | [Reserved] |
| § 31:36   | Government use of biometrics: an overview |
| § 31:37   | Department of Defense (DOD): use of biometrics |
| § 31:38   | Department of Homeland Security (DHS): use of biometrics |
| § 31:39   | Department of Justice (DOJ): use of biometrics |
| § 31:40   | Department of State (DOS): use of biometrics |
| § 31:41   | State use of biometrics: an overview |
| § 31:42   | State Use of biometrics: drivers' licenses and identification cards |
| § 31:43   | State use of Biometrics: prevention of welfare fraud |
| § 31:44   | Biometrics: private industry use |
| § 31:45   | Biometrics and social media |
| § 31:46   | Biometrics: other private industry uses |
| § 31:47   | Biometrics and the law: in general |
| § 31:48   | Biometrics and the “right to privacy” |
| § 31:49   | Biometrics and the Fourth and Fifth Amendments |
| § 31:50   | Biometrics: the threat to privacy |
| § 31:51   | [Reserved] |
| § 31:52   | Biometrics in the courts: Federal decisions—Facial recognition |
§ 31:53 —Biometrics and standing
§§ 31:54 to 31:58 [Reserved]
§ 31:59 Biometrics in the courts: Cases on the horizon
§ 31:60 Biometrics: other objections, concerns and conclusions

Volume 4

PART VII. PRETRIAL LITIGATION

CHAPTER 32. GRAND JURY USE OF INTERCEPTED COMMUNICATIONS

I. INTRODUCTION
§ 32:1 In general
§ 32:2 Utilizing conversations
§ 32:3 —Transcript distribution
§ 32:4 Voice identification
§ 32:5 Indictment strategy
§ 32:6 Aliases
§ 32:7 Discovery
§ 32:8 Immunity
§ 32:9 Perjury

II. THE RECALCITRANT WITNESS, CONTEMPT AND THE EXCLUSIONARY RULE
§ 32:11 Standing to assert claim
§ 32:12 Timing of claim
§ 32:13 Sufficiency of claim
§ 32:14 —“Detailed claim” requirement
§ 32:15 Claims relating to conversations of attorney
§ 32:16 Prosecutor’s response
§ 32:17 Form and contents of denial
§ 32:18 Surveillance pursuant to warrant
§ 32:19 Foreign surveillance

lxxxviii
§ 32:20 No suppression hearing
§ 32:21 Contempt hearing
§ 32:22 Subpoenas duces tecum; exemplars and documents
§ 32:23 If the surveillance was unlawful
§ 32:24 State procedures
§ 32:25 Criminal contempt

III. OTHER INVESTIGATIVE BODIES AND AGENCIES
§ 32:26 In general

CHAPTER 33. PRELIMINARY DEFENSE STRATEGY AND MOTIONS

I. PRIOR TO ARREST
§ 33:1 Anticipatory countermeasures
§ 33:2 On receipt of notice
§ 33:3 On being subpoenaed

II. AFTER INDICTMENT
§ 33:4 Discovery: 18 U.S.C.A. § 2518(9); 18 U.S.C.A. § 2510(a)
§ 33:5 Rules of Criminal Procedure
§ 33:6 18 U.S.C.A. § 3504
§ 33:7 Freedom of Information Act
§ 33:8 Motion for discovery
§ 33:9 Failure to disclose: consequences
§ 33:10 Disclosure of transcripts
§ 33:11 Examinations for tampering
§ 33:12 Discovery of technical data
§ 33:13 Progress reports
§ 33:14 Other materials
§ 33:15 Bill of particulars
§ 33:16 Supplemental discovery motion
§ 33:17 Motion to inspect grand jury minutes
§ 33:18 Discovery and suppression strategy
§ 33:19 Motion to sever
§ 33:20 Plea bargaining
§ 33:21 Motion to suppress

© 2018 Thomson Reuters, 12/2018  lxxxix
CHAPTER 34. GROUNDS FOR SUPPRESSION

I. INTRODUCTION
§ 34:1 In general
§ 34:2 Constitutionality

II. THE GENERAL EXCLUSIONARY PROVISIONS OF TITLE III
§ 34:3 18 U.S.C.A. § 2515
§ 34:4 18 U.S.C.A. § 2517(3): Testimonial use
§ 34:5 18 U.S.C.A. § 2518(10)(a)
§ 34:6 State variations

III. “UNLAWFULLY INTERCEPTED” COMMUNICATIONS
A. STATUTORY PROVISIONS
§ 34:8 Electronic communications: 18 U.S.C.A. § 2518(10)(c)

B. “CENTRAL” AND NON-“CENTRAL” PROVISIONS
§ 34:9 “Central” provisions: U.S. v. Giordano
§ 34:10 Applicability of the U.S. v. Leon “good-faith exception”
§ 34:11 Technical but insubstantial error; Sheppard v. Massachusetts
§ 34:12 Technical but insubstantial error: state variations
§ 34:13 Other “central” holdings and issues
§ 34:14 “Non-central” provisions

IV. OTHER GROUNDS FOR SUPPRESSION
§ 34:16 What constitutes “facial insufficiency”? U.S. v. Chavez

xc
§ 34:16.30 What constitutes “facial insufficiency”—Dahda v. U.S.
§ 34:17 Does facial insufficiency mandate suppression?

B. VIOLATIONS OF THE INTERCEPTION ORDER

§ 34:18 18 U.S.C.A. § 2518(10)(a)(iii)

C. VIOLATION OF POST-EXECUTION PROVISIONS

§ 34:19 In general
§ 34:20 Valid bases for suppression
§ 34:21 “Central” post-execution provisions
§ 34:22 —18 U.S.C.A. § 2518(8)(a)—The sealing provision
§ 34:23 —18 U.S.C.A. § 2518(9)—Pretrial notice
§ 34:24 —18 U.S.C.A. § 2517(5)—Evidence of other crimes
§ 34:25 Violations which prejudice a defendant’s right to a fair trial
§ 34:26 Deliberate violations

D. UNAUTHORIZED DISCLOSURE

§ 34:28 Unauthorized disclosure coincidental with authorized disclosure and testimony
§ 34:29 Testimony concerning interceptions by someone who had no legal authority to learn about them
§ 34:29.50 Potentially privileged communications

V. INTER-JURISDICTIONAL BASES FOR SUPPRESSION

§ 34:30 Federal-state issues
§ 34:30.10 Federal evidence, state prosecutions
§ 34:30.20 State evidence, federal prosecutions
§ 34:31 Other interjurisdictional issues
§ 34:32 Federal choice of law issues

© 2018 Thomson Reuters, 12/2018
CHAPTER 35. LITIGATING THE SUPPRESSION MOTION

I. INTRODUCTION

§ 35:1 In general
§ 35:2 Recusal of suppression hearing judge
§ 35:3 Timeliness of motion
§ 35:4 Timing of hearing
§ 35:5 Burden of proof at hearing
§ 35:6 Exclusion of the public

II. STANDING

§ 35:7 In general

A. “AGGRIEVED PERSON”

§ 35:8 18 U.S.C.A. § 2510(11)
§ 35:9 “Party”
§ 35:10 “Person against whom the interception is directed”: Alderman v. United States
§ 35:11 “Against whom directed”: post-Alderman case law
§ 35:12 “Against whom directed”: defendant’s relationship to premises
§ 35:13 “Against whom directed”: residential premises
§ 35:14 “Against whom directed”: interceptions at the workplace
§ 35:14.50 “Against whom directed”: cell phone
§ 35:15 “Against whom directed”: electronic communications
§ 35:16 “Against whom directed”: other situations
§ 35:17 Victim of private, unlawful interceptions
§ 35:18 State variations
§ 35:19 “Aggrieved person” requirement—“ Personally aggrieved” requirement
§ 35:20 State case law

B. “TRIAL, HEARING OR PROCEEDING” REQUIREMENT

§ 35:21 18 U.S.C.A. § 2518(10)
Nondefendant, nonwitness’s standing to oppose use of intercepted communication at trial
Extensions and second-generation interception orders

III. VALIDITY OF PAPERS
Facial sufficiency
Authorization
Misstatements of facts
Claiming pretext

IV. LITIGATING TAINT ISSUES
A. OVERVIEW
In general
Raising the issue: 18 U.S.C.A. § 3504

B. DEFENDANT'S CLAIM, PROSECUTOR'S RESPONSE
Defendant's claim
Government’s response
Consequences of inadequate denial
Consequences of adequate denial
Admission of lawful but irrelevant surveillance
Raising the issue: state proceedings

C. TRIAL WITNESS'S CLAIM
Trial witness challenge to basis of questions asked him
Trial witness’ attorney

D. PROVING OR DISPROVING TAINT
Burden of proof
Discovery
Destroyed recordings
Demonstrating taint
Contesting taint
Independent source
Severing the taint
Segregating the investigators
§ 35:46 Attenuation; voluntary testimony
§ 35:47 Inevitable discovery
§ 35:48 Subsequent or unrelated crime
§ 35:49 Unanswered questions

V. LITIGATING MINIMIZATION

§ 35:50 In general

A. STANDING

§ 35:51 Overview
§ 35:52 View that nonresident lacks standing
§ 35:53 View that nonresidents enjoy only limited standing
§ 35:54 View that a nonresident can challenge the entire minimization performance
§ 35:55 Oral intercepts
§ 35:56 Oral intercepts: private residence
§ 35:57 Oral intercepts: public locations
§ 35:58 Oral intercepts: “social club”
§ 35:59 Evaluation
§ 35:60 State variations

B. OTHER ISSUES

§ 35:61 Burden of proof
§ 35:62 Discovery
§ 35:63 Prima facie showing
§ 35:64 Statistical analysis
§ 35:65 Defense planning
§ 35:66 Defense tactics at hearing

C. EXTENT OF SUPPRESSION

§ 35:67 In general
§ 35:68 Suppression by “pattern or category”
§ 35:69 The “general warrant” approach
§ 35:70 Comment

VI. MISCELLANEOUS ISSUES

§ 35:71 Post-execution violations
§ 35:72 Government appeals: 18 U.S.C.A. § 2518(10)(b); state law

xciv
TABLE OF CONTENTS

§ 35:73 Interlocutory defense appeals
§ 35:74 Habeas corpus relief

PART VIII. THE TRIAL

CHAPTER 36. TRANSCRIPTS AND TRANSLATIONS

§ 36:1 Overview

I. ENGLISH LANGUAGE CONVERSATIONS

A. WHO SHOULD PREPARE THE TRANSCRIPT

§ 36:2 In general
§ 36:3 Should a participant in the conversation transcribe it?
§ 36:4 Transcript as group project

B. THE TRANSCRIPT’S ROLE

§ 36:5 Overview
§ 36:6 “Transcript as aid to understanding the recording”
§ 36:7 Transcript as opinion evidence of contents
§ 36:8 —Expert or lay witness opinion

C. TRANSCRIPT CONTENTS

§ 36:9 In general
§ 36:10 Identifying the speakers
§ 36:11 Words and sounds: transcript as “mirror” of the recording
§ 36:12 Prohibition against “explanatory” material
§ 36:13 “Creative” punctuation, type face changes, etc

D. TESTING TRANSCRIPT ACCURACY

§ 36:14 In general
§ 36:15 Roles of judge and jury
§ 36:16 Advice for the offering party

© 2018 Thomson Reuters, 12/2018
II. FOREIGN LANGUAGE CONVERSATIONS

§ 36:17 Overview

A. TRANSLATION OF FOREIGN LANGUAGE CONVERSATION AS EXPERT OPINION EVIDENCE

§ 36:18 In general
§ 36:19 The translator
§ 36:20 Participant as translator
§ 36:21 Multiple translators, single witness
§ 36:22 Methods and procedures
§ 36:23 Advice to offering party (particularly prosecutors)

B. ADVERSE PARTY’S CHALLENGE TO TRANSCRIPT ACCURACY

§ 36:24 In general
§ 36:25 Timing of the challenge
§ 36:26 Cross-examining the offering party’s expert
§ 36:27 Adverse party’s expert witness

C. ASSESSING ACCURACY: ROLES OF JUDGE AND JURY

§ 36:28 Judge and jury

D. CONTENTS OF TRANSLATIONS TO BE PRESENTED TO THE JURY

§ 36:29 In general
§ 36:30 Colloquialisms; slang
§ 36:31 Jargon; fact-specific references within the translation

E. PRESENTING CONVERSATIONS AND TRANSLATIONS TO THE JURY

§ 36:32 In general
§ 36:33 Should the recording be played for the jury?
§ 36:34 The alternatives

F. JURY INSTRUCTIONS; JURY ACCESS TO TRANSLATIONS DURING DELIBERATIONS

§ 36:35 Jury instructions
TABLE OF CONTENTS

§ 36:36 Jury access to translations during deliberations

G. MISCELLANEOUS ISSUES

§ 36:37 Court Reporter Act; Jones Act
§ 36:38 Privileged communications

CHAPTER 37. AUTHENTICATION, AUDIBILITY AND INTELLIGIBILITY
§ 37:1 Overview

I. AUTHENTICATION

A. THE DIFFERENT STANDARDS

§ 37:2 Introduction
§ 37:3 The strict Solomon-McKeever-McMillan test
§ 37:4 Fed. R. Evid. 901(a) and corresponding state law: “sufficient to support a finding”
§ 37:5 Defining “sufficient to support a finding”: Fed. R. Evid. 104(b) and 901(a)
§ 37:6 Other approaches

B. SATISFYING THE AUTHENTICATION REQUIREMENT

§ 37:7 In general
§ 37:8 Testimony by a participant in the conversation
§ 37:9 Conversations recorded by, or with, a non-testifying participant’s consent
§ 37:10 Testimony by someone who overheard or monitored the conversation
§ 37:11 Conversations automatically recorded by equipment designed to do so
§ 37:12 Found or seized recordings
§ 37:13 Interception order recordings

C. SPECIFIC REQUIREMENTS AND CIRCUMSTANCES

§ 37:14 Date and time
§ 37:15 Chain of custody
§ 37:16 Integrity
§ 37:17 Device; operator; accuracy
§ 37:18 “Voluntariness”
§ 37:19 Rerecordings; enhanced rerecordings
§ 37:20 Procedural issues

II. AUDIBILITY & INTELLIGIBILITY

§ 37:21 In general
§ 37:22 Partial inaudibility or untelligibility
§ 37:23 Improving audibility in the courtroom
§ 37:24 Inaudibility does not bar testimony as to the conversation

CHAPTER 38. VOICE IDENTIFICATION

I. IN GENERAL

§ 38:1 Introduction; abbreviations
§ 38:2 Burdens of production and persuasion; “ultimate issue of fact”

II. VOICE IDENTIFICATION BY LAY WITNESSES, JURORS AND JUDGES

§ 38:3 Fed. R. Evid. 901; Unif. R. Evid. 901; state rules
§ 38:4 Testimony by an eye-witness to the conversation
§ 38:5 Recognition identification testimony: Fed. R. Evid. 901(b)(5) & corresponding state rules
§ 38:6 —Arrest and post-arrest processing
§ 38:7 Self-identification by phone conversation participant: Fed. R. Evid. 901(b)(6)(A)
§ 38:8 Circumstantial identification; Fed. R. Evid. 901(b)(4)
§ 38:9 Identifying and authenticating calls to and from business numbers: Fed. R. Evid. 901(b)(6)(B)
§ 38:10 Jury (or judge) comparing “X’s” voice to a voice on a contested recording; Fed. R. Evid. 901(b)(3)
§ 38:11 Identifying a voice’s race or ethnic origin

III. VOICE EXEMPLARS

§ 38:12 Constitutional considerations
§ 38:13 Uses of voice exemplars
§ 38:14 Practical considerations
§ 38:15 Defendant’s right to exhibit his voice without testifying
## IV. EXPERT TESTIMONY; SCIENTIFIC EVIDENCE

### A. OVERVIEW

- § 38:16 In general
- § 38:17 Ineffective assistance claims

### B. VOICE IDENTIFICATION AS A SUBJECT OF EXPERT TESTIMONY GENERALLY

- § 38:18 Unrecorded conversations and encounters
- § 38:19 Recorded conversations and encounters: introduction
- § 38:20 Expertise based on language, dialect, phonetics, linguistics, etc
- § 38:21 Linguistic analysis and the like
- § 38:22 Other situations

### C. SPECTROGRAPHIC ANALYSIS (“VOICE PRINTS”)

- § 38:23 Description; prognosis
- § 38:24 Federal courts: *Frye* and *Daubert*
- § 38:25 State law
- § 38:26 Miscellaneous matters

## V. VOICE IDENTIFICATION, THE RIGHT TO COUNSEL, AND DUE PROCESS; “SUGGESTIVENESS” CLAIMS

- § 38:27 Pretrial discovery; raising the issue
- § 38:28 Background: Supreme Court eye-witness identification case law
- § 38:29 Background: Supreme Court eyewitness identification case law—Application to voice identification: presence of counsel
- § 38:30 Application to voice identification: suggestiveness issues
- § 38:31 —Identifying a voice in a recorded conversation
- § 38:32 Identifying a voice recalled from an unrecorded conversation or encounter
- § 38:33 “Voice lineups”

## VI. OTHER ISSUES

- § 38:34 Voice identification and trial strategy

© 2018 Thomson Reuters, 12/2018

xcix
CHAPTER 39. [Reserved]
E-mail Authentication

CHAPTER 40. [Reserved]
Computer and Network Data Evidentiary Issues

CHAPTER 41. OTHER ISSUES AT TRIAL

I. PRELIMINARY MATTERS
§ 41:1 In general
§ 41:2 Prosecutorial trial strategy
§ 41:3 Defense trial strategy
§ 41:4 Recusal of trial judge
§ 41:5 Prosecutor's pre-trial preparation
§ 41:6 Defense counsel's pre-trial preparation
§ 41:7 Prejudicial or irrelevant matter
§ 41:8 Jury selection
§ 41:9 Opening statement
§ 41:10 Introductory witnesses

II. PRESENTING RECORDINGS
§ 41:11 In general
§ 41:12 Chain of custody
§ 41:13 Identifying the conversation
§ 41:14 Composite recordings
§ 41:15 Re-recording of missing original
§ 41:16 Sequential presentation
§ 41:17 Cross-examination
§ 41:18 Disclosure of technical data
§ 41:19 Manner of proof: a suggested scenario
§ 41:20 Additional issues and considerations [Reserved]

III. INTERPRETING INTERCEPTED COMMUNICATIONS: CODES, JARGON; RELATED ISSUES

A. IN GENERAL
§ 41:21
The need for interpretive or explanatory testimony

§ 41:22 Requirement that testimony be “helpful” to fact-finder

§ 41:23 “Expert” or “lay witness” testimony

§ 41:23.20 Specificity of objection

§ 41:24 Lay witness opinion testimony: Fed. R. Evid. 701; state equivalents

§ 41:24.10 Police interpretive testimony and Fed.R.Evid. 701

§ 41:24.20 Lay witness testimony by a participant in the conversation

§ 41:24.30 Lay witness testimony by a former member of the conspiracy; other person with knowledge

§ 41:24.40 Officer's lay witness testimony not based on participation in the conversation(s)

B. EXPERT OPINION TESTIMONY

§ 41:25 The need for expert testimony; qualifications

§ 41:26 Fed. R. Evid. 702; state equivalents

C. REQUIREMENTS AND RESTRICTIONS

§ 41:26.10 Witness's qualifications

§ 41:26.20 Other requirements and restrictions: in general

§ 41:26.30 Pretrial discovery: sample Rule 702 affidavits

§ 41:26.40 “Principles and methodologies”: introduction

§ 41:27 Interpreting conversations in light of other, admitted evidence; “overview witness”

§ 41:28 Interpreting conversations in light of other, unadmitted evidence

§ 41:28.10 Use of legal vs. non-legal terminology

D. TESTIMONY BY AN OFFICER BASED ON PARTICIPATION IN THE INVESTIGATION

§ 41:29 Introduction

§ 41:29.10 —The strict “expert testimony” approach

§ 41:29.20 —Lay opinion based on participation in and knowledge of that investigation

§ 41:29.30 —Combined lay and expert testimony

§ 41:29.40 —Distinction based on the witness's “reasoning process”

© 2018 Thomson Reuters, 12/2018 ci
§ 41:29.50 —All such testimony is lay testimony

E. “STATE OF MIND” ISSUES

§ 41:30 In general
§ 41:31.10 Fed. R. Evid. 704; state equivalents

F. OTHER ISSUES AND PROBLEMS

§ 41:32 Special problems in narcotics cases
§ 41:33 Agent as fact witness and expert witness
§ 41:34 Sufficiency of expert testimony to support a conviction
§ 41:35 Other uses of expert testimony relating to recorded conversations
§ 41:35.50 Interpretation of communications by attorney in summation

IV. HEARSAY; CONFRONTATION CLAUSE

A. HEARSAY

§ 41:36 Miscellaneous issues
§ 41:37 Admissions, adopted admissions, implied admissions; “context”
§ 41:38 The coconspirator exception; related conspiracy issues
§ 41:39 Other hearsay exceptions and situations

B. SIXTH AMENDMENT CONFRONTATION CLAUSE

§ 41:40 In general
§ 41:41 The pre-2004 Confrontation Clause
§ 41:42 The “new” Confrontation Clause: Crawford v. Washington
§ 41:43 Statements by the defendant
§ 41:44 Statements made by suspects during interviews by law enforcement officials
§ 41:44.50 Statements by victims and witnesses to police; 911 calls
§ 41:45 Statements by and among coconspirators
§ 41:46 Statements made by confidential informants

V. THE “BEST EVIDENCE RULE”

§ 41:47 In general
§ 41:48 Unrecorded conversations
§ 41:49 Testimony in lieu of lost recording
§ 41:50 Re-recordings; enhanced re-recordings and video recordings
§ 41:51 Transcripts in addition to recordings
§ 41:52 Transcripts in lieu of recordings
§ 41:53 Interceptions regulated by statute

VI. OTHER TRIAL ISSUES

§ 41:54 Collateral use of inadmissible recordings
§ 41:55 Use of unlawful interceptions for impeachment: constitutional principles
§ 41:56 —Use by the prosecutor
§ 41:56.50 Translations and the Confrontation Clause
§ 41:57 Use of unlawful interceptions for impeachment—Use by defendant
§ 41:57.50 Rule of Completeness; Fed. R. Evid. 106 and state equivalents
§ 41:58 Use in civil litigation
§ 41:58.50 Civil discovery of interceptions previously revealed in a criminal case
§ 41:59 Transcripts without recordings
§ 41:60 Opening statement and summation
§ 41:61 Issues relating to jury instruction
§ 41:62 Playing recordings during jury deliberations; transcripts
§ 41:63 Miscellaneous issues relating to recordings and transcripts

VII. TESTIMONIAL USE OF COURT-ORDERED SURVEILLANCE IN NON-CRIMINAL PROCEEDINGS

§ 41:64 In general; 18 U.S.C.A. § 2517(3)
§ 41:65 Use in civil tax cases
§ 41:66 Federal forfeiture proceedings
§ 41:67 State forfeiture proceedings
§ 41:68 Use in disciplinary proceedings
§ 41:69 Use by private parties in civil litigation

APPENDICES

Appendix A. Sample Network Banner Language
Appendix B. Stored Communications Act, 18 U.S.C. § 2703(d)

Appendix C. Sample Language for Preservation Request Letters under 18 U.S.C. 2703(f)

Appendix D. Sample Application and Order for Pen Register/Trap and Trace for Web-Based Email Account

Appendix E. Sample Application and Order for Pen Register/Trap and Trace to Collect Addresses on Email Sent to/from Target Account

Appendix F. Sample Application and Order for Pen Register/Trap and Trace on a Computer Network Intruder

Appendix G. Sample Subpoena Language

Appendix H. Sample Letter for Provider Monitoring

Appendix I. Search Warrants and Accompanying Affidavits to Search and Seize Computers

Appendix J. Sample Authorization for Monitoring of Computer Trespasser Activity

Table of Laws and Rules

Table of Cases

Index