

Content Overview

Introduction	21
I. The Background of the Study	21
II. The Three Jurisdictions	22
III. Presentation of Problems	23
IV. Structure of the Study	24

Part I

Surveillance of Wire and Oral Communications in the U.S.	25
I. Constitutional Protection	26
II. Surveillance of Wire and Oral Communications in Federal Statutes	47
III. Exceptions from the General Prohibition of Warrantless Surveillance	54
IV. Procedure	59
V. Exclusionary Rule	80
VI. Empirical Studies	97
VII. Conclusions	110

Part II

Technological Surveillance in the Federal Republic of Germany	114
I. Telecommunication	114
II. Acoustic Surveillance (akustische Überwachung)	148
III. Procedure	162
IV. "Prohibitions of Evidence" ("Beweisverbote")	173
V. Empirical Reports	194
VI. Conclusions	206

Part III

Technological Investigative Measures in the People's Republic of China	209
I. Telecommunication and Art. 40 of the Chinese Constitution	209
II. The Inviolability of the Residence and Art. 39 of the Chinese Constitution	218
III. Technological Measures in Legislation and Departmental Regulations	226
IV. Procedural Requirements	249
V. Admissibility of Information from TIMs	258
VI. Conclusions	285

Part IV

Conclusions with Horizontal Comparison	288
I. "Reasonable Expectation of Privacy" vs. "Core Area of Privacy"	288
II. Statutory Protections	299
III. Procedure	303
IV. The Exclusionary Rule	308
V. Empirical Studies	325
VI. Final Comments and Suggestions for Reforms in China	328
Appendix	336
Reports on the questionnaires	336
References	357
Index	374

Contents

Introduction	21
I. The Background of the Study	21
II. The Three Jurisdictions	22
III. Presentation of Problems	23
IV. Structure of the Study	24

Part I

Surveillance of Wire and Oral Communications in the U.S. 25

I. Constitutional Protection	26
1. Trespass Doctrine	26
2. From Trespass Doctrine to the Reasonable Expectation of Privacy	31
3. “Reasonable Expectation of Privacy” after <i>Katz</i>	32
4. The Reasonable Expectation of Privacy	35
a) An “Actual (Subjective) Expectation of Privacy”	35
b) An Expectation “that Society is Prepared to Recognize as ‘Reasonable’” ...	37
aa) Social Conceptions of the Expectation of Privacy	38
bb) An Empirical Study of General Attitudes toward Privacy	40
5. The Minimal Expectation of Privacy	42
6. Other Constitutional Aspects of Electronic Surveillance	43
a) 5 th Amendment: Privilege against Self-incrimination	43
b) The Attorney-Client Privilege	44
c) 6 th Amendment: The Right to Counsel	45
d) Summary	46
II. Surveillance of Wire and Oral Communications in Federal Statutes	47
1. Early Regulation	47
2. The Modern Statute	49
a) The Definition of “Wire Communication” under § 2510(1) of <i>Title III</i>	50
b) The Definition of “Oral Communication” under § 2510(2) of <i>Title III</i>	52
c) The Definition of “Intercept” under § 2510(4) of <i>Title III</i>	53

III. Exceptions from the General Prohibition of Warrantless Surveillance	54
1. Plain Hearing	54
2. Consent to Surveillance under <i>Title III</i>	55
IV. Procedure	59
1. Application Process for a Surveillance Warrant at the Federal Level	59
a) Who can Make and Authorize an Application	59
b) Exigent Circumstances	60
c) Crimes that Can be Investigated by Intercepting Communications	62
d) The Contents of an Application	63
e) Review Criteria	65
aa) Legality and Necessity	65
bb) Effectiveness of the Technology	65
cc) Cost	66
2. The Warrant	66
a) Jurisdiction	66
b) Findings and Determinations	67
aa) Probable Cause	68
bb) Specific Communications to be Intercepted	69
cc) Inadequacy of Investigatory Alternatives	69
(1) Failure or the Unlikely Success of Other Measures	70
(2) Dangers Arising from Other Measures	70
(3) The Frustration of the “Last Resort” Requirement	71
dd) Where Communications Can be Intercepted	71
ee) High Approval Rate of Applications	72
c) The Contents of the Warrant (18 U.S. Code § 2518(4)-(6))	72
aa) The Duration Directive	72
bb) The Termination Directive	73
cc) The Minimization Directive	73
dd) The Progress Report System	76
3. The Role of Police and Prosecutors	77
4. Extension of the Warrant	77
5. Sealing the Evidence	78
6. Giving Notice of Electronic Surveillance	79
V. Exclusionary Rule	80
1. Origin and Purpose of the Exclusionary Rule	80
2. Admissibility of Wiretap Evidence under the 4 th Amendment	83
3. Admissibility under Section 605	83
4. Admissibility under <i>Title III</i>	84
a) The Scope of the Exclusionary Rule under <i>Title III</i>	85

b) Standing to Demand Suppression	86
aa) Being Party to Communications	86
bb) Possessory Interest	86
cc) The Person against Whom the Interception Was Directed	87
c) Grounds for Excluding Evidence	88
aa) “Unlawfully Intercepted” Communications	88
(1) “Central Role” Test	89
(2) Non-Central Provisions	91
bb) “Insufficient on its Face” (§ 2518(10)(a)(ii))	92
cc) Not “in Conformity with the Order” (§ 2518(10)(a)(iii))	92
dd) Violation of Regulations regarding the Post-Implementation Phase	93
ee) Evidence Derived from Illegal Private Interceptions	94
5. Comments on the Exclusionary Rule	96
VI. Empirical Studies	97
1. Number of Surveillance Applications and Issued Warrants	97
2. Rate of Installed Intercepts	99
3. Types of Surveillance Used	102
4. Major Offenses Named in Warrants	103
5. Duration and Extension	104
6. Cost	106
7. Efficiency of Surveillance	107
a) Rates of Incriminating Information	108
b) Number of Arrests and Convictions	109
VII. Conclusions	110

Part II

Technological Surveillance in the Federal Republic of Germany	114
I. Telecommunication	114
1. Constitutional Protection – Art. 10 German Basic Law	114
a) History	115
b) The Personality Right (“Allgemeines Persönlichkeitsrecht”)	117
aa) The Right to a Private Sphere and the “Core Area of Privacy”	117
bb) The Right to the Spoken Word (“Recht am gesprochenen Wort”)	122
cc) The Relationship between Art. 10, Art. 2 GG and Art. 1 GG	122
c) New Basic Rights	123
aa) The Right to Data Autonomy	123
bb) The Right to the Integrity of Information Systems	124

d) Proportionality (Verhältnismäßigkeit)	125
aa) Suitability	125
bb) Necessity	126
cc) Proportionality in the Narrow Sense	127
e) Summary	129
2. Surveillance of Telecommunication under § 100a StPO	129
a) Protected Area of “Telekommunikation”	130
b) Crime Catalogue under § 100a StPO	131
c) Persons Targeted and Third Persons	132
aa) Persons Targeted	133
bb) Third Persons	133
cc) Lawyer-client Communications	134
d) Chance Finds (“Zufallsfunde”)	135
aa) Background Conversations	135
bb) Admissibility of Chance Finds	137
e) Degree of Suspicion under § 100a I 1 Nr. 1.	139
f) Subsidiarity Principle	140
g) “Core Area of Privacy”	142
3. Telecommunication Traffic Data (§ 100g StPO)	145
a) Collection of Telecommunication Traffic Data under § 96 TKG	145
aa) Definition	145
bb) Offenses Covered by § 100g I StPO	146
b) Collection of Data Stored under § 113b TKG	146
c) Traffic Data in a Cellular Network (Funkzellenabfrage)	147
d) The Subsidiarity Clause in § 100g	147
e) Protection of Professionals (§ 100g IV StPO)	148
II. Acoustic Surveillance (akustische Überwachung)	148
1. Acoustic Surveillance of Home	149
a) Art. 13 GG: Inviolability of the Home	149
aa) Historical Background	149
bb) The Definition of “Home”	150
cc) Restrictions of Inviolability under Art. 13 III GG	152
b) § 100c StPO	152
aa) Definition of “Not Publicly” (“nichtöffentlich”)	153
bb) Crime Catalogue of § 100c StPO	153
cc) Concerned Persons and Concerned Homes	154
dd) Facts to Support Suspicion	155
ee) Subsidiarity Principle	155
ff) The Core Area of Privacy	156

gg) Protection of Close Relationships	157
hh) Protection of Professionals	157
2. Acoustic Surveillance in Public Areas (§ 100f StPO)	158
a) The Borderline Cases between § 100c and § 100f StPO	158
b) Conditions for Acoustic Surveillance outside Homes (§ 100f I StPO)	160
c) Persons Affected by the Measure	160
III. Procedure	162
1. Jurisdiction of the Issuing Court and of the Prosecution	162
a) Jurisdiction of the Issuing Court	162
aa) Telecommunication Surveillance under § 100a StPO	162
bb) Acoustic Surveillance of a Home	162
b) Jurisdiction of the Prosecutor “bei Gefahr im Verzug”	163
c) Judicial Control	165
2. Criteria for Judicial Review of an Application	166
3. The Contents of a Surveillance Order	167
4. Duration and Extension of Surveillance	168
5. Implementation of Surveillance	168
6. Termination of the Order	169
7. Notice to Persons under Surveillance	170
8. Legal Remedies against Surveillance	172
9. Deletion and Storage of the Obtained Information	172
IV. “Prohibitions of Evidence” (“Beweisverbote”)	173
1. The Scope of “Prohibitions of Evidence” and its Subgroups	174
2. Theories of “Prohibitions of Using Evidence”	174
a) Rechtskreistheorie	175
b) “Protective Purpose” Doctrine (“Schutzzwecklehre”)	176
c) Balancing Theory	178
d) Summary	180
3. Grounds for Excluding Evidence	182
a) Grounds Directly Based on Constitutional Law	182
aa) Evidence Falling within the “Core Area of Privacy”	182
bb) The Nemo Tenetur Principle and § 136a StPO	183
b) Violating Procedural Rules as Grounds for Excluding Evidence	185
aa) Richtervorbehalt	186
(1) Without Judicial Order because of “Gefahr im Verzug”	186
(2) Without Judicial Order in Other Situations	187
bb) Offense not Listed	187
cc) Insufficient Facts to Support Suspicion	187
dd) Duration	188

c) Evidence from Private Investigation	188
4. Exclusion of Derivative Evidence? (“Fernwirkung”)	191
V. Empirical Reports	194
1. Numbers of Judicial Orders under § 100a and § 100c StPO	194
2. Reasons for Non-Implementation of Judicial Orders under § 100c StPO	196
3. Types of Intercepted Telecommunications	196
4. Catalogue Crimes Cited (“Anlassstraftaten”)	198
a) Number of Procedures of Telecommunication Surveillance	198
b) Number of Procedures of Home Surveillance	201
5. Duration and Extension	202
a) Extension of Judicial Orders under § 100a StPO	202
b) Duration and Extension of Home Surveillance under § 100c StPO	203
c) Cost	204
6. Efficiency	205
VI. Conclusions	206

Part III

Technological Investigative Measures in the People’s Republic of China	209
I. Telecommunication and Art. 40 of the Chinese Constitution	209
1. The Concept of Human Dignity in China	209
a) History	209
b) Human Rights and Human Dignity	211
c) Privacy in the Constitution	214
2. Freedom and Privacy of Correspondence	215
a) Definition of “Correspondence”	215
b) Privacy of Correspondence and the Power of the Courts to Order Evidence	216
c) Interception of Letters of Prisoners	218
II. The Inviolability of the Residence and Art. 39 of the Chinese Constitution	218
1. Definition of Residence	219
2. The Limited Understanding of “Illegal Search” and “Illegal Intrusion”	223
III. Technological Measures in Legislation and Departmental Regulations	226
1. The Purpose of Criminal Procedure	226
2. Power Distribution in Criminal Investigations	227
a) The Dominant Role of the Police during the Investigation	227
b) Early Participation of Prosecutors in the Investigation	228

c) The “Inspection” Power of Supervision Committees	232
aa) Supervision Committees	232
bb) The “Inspection” Power	233
cc) Technological Measures during Inspection	234
d) Investigations by Prosecutors as a Supplement to Supervision Committees	235
3. The Covert Nature of TIMs	237
4. Concept and Types of TIMs	239
5. Crime Catalogues of TIMs	241
a) Crime Catalogues under Art. 150 of the CCPL	241
b) Art. 263 of the Procedures for Criminal Cases 2020	242
c) The Use of TIMs for the Purpose of Arresting Suspects	243
d) Crime Catalogue under the Supervision Law and the Rules on the Jurisdiction of the Supervision Committee (Trial)	244
6. Degree of Suspicion	245
7. “For the Needs of the Investigation” and “as Needed”	245
8. Targeted Persons	246
9. Privacy Clause	248
IV. Procedural Requirements	249
1. The Approval Procedure of Police, the Supervision Committees and the Pro- secution Offices	249
a) Police	250
b) Prosecution Offices	251
c) Supervision Committees	252
2. Contents of the Warrant	254
3. Implementation	255
4. Duration and Extension of TIMs	256
5. Termination of the Measure	257
6. Obligation to Delete Information	257
V. Admissibility of Information from TIMs	258
1. Art. 154 of the CCPL 2018: New Legislation Concerning Evidence Gathered via TIMs	259
2. The Interpretation of “Other Serious Consequences”	260
3. Three Forms of Evidence	260
4. Examination of the Reliability of TIM Evidence <i>in Camera</i> : A Challenge to the Defense Right	261
5. Defense Strategy	264
6. A Practical Example: Evidence from TIMs in Drug Cases	265
7. The General Rule on Exclusion	266
8. Exclusion of Evidence during Investigation, Prosecution or Inspection	268
a) Police	268

b) Prosecutors	268
c) Supervision Committees	269
9. Exclusion of Evidence by Judges	270
a) Exclusion of Evidence at the Pre-trial Hearing	271
b) Exclusion of Evidence at Trial	274
10. Reasons for the Infrequency of the Exclusion of Evidence	275
a) Exclusion of Evidence and the Emphasis on Truth-finding	275
b) The Heavy Burden of Proof on the Defense and the Lack of Impact of an Exclusion on Convictions	276
c) The Possibility of Correcting Defective Evidence	277
11. Review and Exclusion of Evidence of TIMs	278
12. The “Legitimization” of Evidence: the Move from “Illegal” to “Legal”	281
a) Admissibility of Repeated Confessions	281
b) Indirect Admissibility: the “Delicious” Fruits of the Poisonous Tree	281
c) Incidentally Discovered Evidence	282
13. Admissibility of Evidence Collected by Private Persons in Criminal Proceedings	283
a) Legality of the Collection of Evidence by Private Persons	283
b) Legitimization of Private Evidence	285
VI. Conclusions	285

Part IV

Conclusions with Horizontal Comparison	288
I. “Reasonable Expectation of Privacy” vs. “Core Area of Privacy”	288
1. Different Constitutional Approaches to the Right to Privacy	288
2. “Reasonable Expectation of Privacy” and “Core Area of Privacy”	291
a) The Subjective Element of the Reasonable Expectation of Privacy	291
b) The Objective Element of the Reasonable Expectation of Privacy	292
c) The Minimum Expectation of Privacy	293
3. Constitutionally Protected Spaces in the Three Jurisdictions	293
4. Values behind Different Constitutional Approaches	295
5. Different Methods of Legal Interpretation	296
6. Reasonableness, Balancing of Interests, and Proportionality	298
II. Statutory Protections	299
1. Different Statutory Approaches to Regulating Surveillance	300
2. The Relationship to Other Constitutional Rights	301
a) Self-incrimination	301
b) Attorney-client Privilege	302

III. Procedure	303
1. The Preeminence of the Police in Cases involving Surveillance	303
2. Warrants and Judicial Control	304
3. The Legislative Requirements for a Warrant	305
4. Other Issues Influencing the Issuing of Warrants	305
5. The Last Resort vs. Subsidiarity Principle	306
6. Mechanisms to Enhance Transparency	307
IV. The Exclusionary Rule	308
1. The Role of the Courts	309
2. The Function and Purpose of the Exclusionary Rule	310
a) Deterring Police Misconduct	310
b) Truth-finding	312
c) Human Rights	313
3. Theories relating to the Exclusionary Rule	314
a) Balancing Theory	314
b) “Protective Purpose” Theory	314
c) Inevitable Discovery Rule	315
4. Grounds for Excluding Surveillance Evidence	317
5. Exceptions	318
a) Plain Hearing	318
b) Consent Surveillance	319
c) Emergency Situations	319
d) Good Faith	320
6. The “Fruit of the Poisonous Tree” vs. the Distance Effect of Exclusion	321
7. When to Exclude Evidence	322
a) United States	322
b) Germany	323
c) China	323
8. Evidence Obtained by Private Parties	324
V. Empirical Studies	325
1. Number of Surveillance Warrants	325
2. Types of Surveillance Measures	326
3. Major Offenses in Surveillance Orders	327
4. Cost	327
5. Efficiency	327
VI. Final Comments and Suggestions for Reforms in China	328
1. Constitutional Level	329

2. Legislation Level	330
a) Greater Clarification of TIMs in Legislation and in Practice	330
b) Greater Detail in Application Materials and Warrants	331
c) Warrants to be Approved by Prosecutors	332
d) Limiting the Use of Chance Findings and Tracking Technology	333
e) Reporting System and Statistics	333
f) Reform of the Application of the Exclusionary Rule	334
3. Prospects for Better Criminal Justice	335
Appendix	336
Reports on the questionnaires	336
Report on Model A (for Police)	337
Report on Model B (for Prosecutors and Judges)	347
References	357
Index	374