Inhalt

Geleitwort —— V

Vorwort —— IX

Abkürzungsverzeichnis —— XXVII

Einleitung —— 1

I. Problemstellung und Arbeitshypothese —— **1**
II. Methodik der Untersuchung —— **7**
III. Stand von Forschung und Rechtsprechung —— **8**
IV. Gang der Darstellung —— **11**

Teil 1: **Einführung**

Kapitel 1
Grundlagen —— 15

A. Soziale Netzwerke —— **15**
I. Was ist ein soziales Netzwerk? —— **16**
II. Was ist ein soziales Netzwerk im Internet? —— **17**
B. Persönlichkeitsprofil —— **20**
C. Profilerstellung und -nutzung in Sozialen Netzwerken am Beispiel von Facebook —— **21**
I. Datensammlung —— **22**
1. Registrierung —— **23**
2. Facebook-Website —— **23**
a) Facebook-Anwendungen auf der Facebook-Website —— **24**
b) Anwendungen Dritter auf der Facebook-Website —— **27**
3. Webseiten Dritter —— **27**
a) Cookies —— **28**
b) Pixel-Tags —— **29**
c) Social Plugins —— **30**
d) Open Graph —— **31**
4. Von Dritten bereitgestellte Daten —— **31**
5. Zusammenfassung —— **32**
II. Analyse der gesammelten Daten zu Profilbildungszwecken —— **32**
1. Analysefelder —— **32**

2. Analysemethode: Knowledge Discovery in Databases — 35
a) Clustering — 36
b) Klassifikation — 37
c) Assoziationsregeln — 37
d) Generalisierung — 38
e) Evaluation — 38
3. Konsequenzen — 39
III. Kommerzielle Profilnutzung — 39
1. Werbung — 40
2. Weitergabe statistischer Daten zur Reichweitenanalyse — 41
3. Künftige kommerzielle Nutzungsmöglichkeiten — 41

Kapitel 2
Interessenanalyse — 44
A. Betreiber- und Drittinteressen an der Profilbildung und -nutzung — 44
B. Privatheitsinteressen der Nutzer — 46
I. Besteht ein Interesse an Privatheit noch? — 47
II. Ist die (kostenfreie) Nutzung wichtiger als der Schutz der eigenen Daten? — 51
1. Tatsächliche Nutzung — 52
2. Aussagekraft des Nutzungsverhaltens — 53
a) Uninformiertheit — 55
b) Begrenzte Rationalität — 57
c) Schlussfolgerungen — 59
3. Ergebnis — 60
III. Beeinträchtigung von Privatheitsinteressen der Nutzer durch Profilbildung und -nutzung — 60

Teil 2: **Länderberichte**

Kapitel 3
Deutschland — 67
A. Einführung deutscher Persönlichkeitsschutz — 67
B. Verfassungsrechtliche Vorgaben — 68
I. Verhältnis unions- und mitgliedsstaatlicher Grundrechte — 69
1. Standpunkt des BVerfG — 70
2. Standpunkt des EuGH — 70
3. Auswirkungen der DS-GVO und Schlussfolgerungen — 72
II. Grundrechtlich geschützte Betreiber- und Drittinteressen — 73

1. Grundrechtsschutz für ausländische Personen — 73
a) Anwendbarkeit von Grundrechten auf ausländische juristische Personen — 73
b) Allgemeine Handlungsfreiheit als Auffangtatbestand — 74
2. Meinungs- und Informationsfreiheit — 74
a) Art. 5 I 1 GG — 75
b) Art. 11 GRCh — 76
3. Berufsfreiheit — 77
a) Art. 12 I GG — 77
b) Art. 15 GRCh — 79
4. Eigentumsgarantie — 80
a) Art. 14 I GG — 80
b) Art. 17 GRCh — 81
5. Wirtschaftliche Betätigungsfreiheit — 82
a) Art. 2 I GG — 82
b) Art. 16 GRCh — 83
6. Ergebnis — 83
III. Grundrechtlich geschützte Nutzerinteressen — 84
1. Menschenwürdegarantie — 85
a) Art. 1 I GG — 85
aa) Vollständige Erfassung der Persönlichkeit — 86
bb) Kernbereich privater Lebensgestaltung — 86
b) Art. 1 GRCh — 87
2. Allgemeines Persönlichkeitsrecht — 88
a) Vorstellung der Leitentscheidungen — 89
aa) BVerfGE 65, 1, 43 – Volkszählungsurteil: Recht auf informationelle Selbstbestimmung — 89
bb) BVerfGE 120, 274 – Online Durchsuchung: Vertraulichkeit und Integrität informationstechnischer Systeme — 91
b) Abgrenzung der Schutzbereiche — 95
aa) Streitstand — 95
bb) Herleitung aus der Begründung des neuen Schutzbedarfs — 96
cc) Abgrenzungsformel und Übertragung auf Soziale Netzwerke — 98
c) Schutz durch die EU-Grundrechtscharta — 99
3. Fernmeldegeheimnis — 101
a) BVerfGE 125, 260 – Vorratsdatenspeicherung — 102
aa) Schutzumfang und Eingriff — 103

bb) Schranken und Schranken-Schranken — **103**
b) Schutz durch die EU-Grundrechtscharta — **104**
IV. Gesetzgeberischer Gestaltungsauftrag zur Profilbildung durch Private — **105**
1. Vertraulichkeitsgarantien — **106**
a) Schutzauftrag aus der Grundrechtsausprägung der Vertraulichkeit und Integrität informationstechnischer Systeme? — **106**
aa) Persönlichkeitsbilder neuartiger Tiefe und Breite — **107**
bb) Anzahl mitbetroffener Personen — **107**
cc) Qualitativ mit einer heimlichen Infiltration vergleichbarer Eingriff — **108**
dd) Berechtigte Vertraulichkeitserwartungen — **109**
ee) Würdigung und Ergebnis — **109**
b) Schutzauftrag aus Art. 10 I GG — **110**
2. Autonomie — **111**
a) Beeinträchtigung der freien Entfaltung durch Profilbildung Sozialer Netzwerkbetreiber — **111**
b) Abgeleitete Vorgaben für Profile Sozialer Netzwerke — **112**
aa) Einschränkungen der Profilbildung — **112**
bb) Schaffung der Voraussetzungen von Autonomie — **114**
cc) Reichweite des Schutzbereichs — **115**
V. Ergebnis — **116**
C. Einfachgesetzliche Regelungen des Persönlichkeitsschutzes — **117**
I. Anwendbarkeit deutschen Datenschutzrechts — **117**
1. Internationale Anwendbarkeit — **117**
a) Anwendbares Kollisionsrecht — **118**
aa) Zulässige Rechtswahl? — **118**
bb) Spezialgesetzliche Kollisionsnorm — **119**
b) Anwendbares Datenschutzrecht nach der Kollisionsnorm des § 1 V BDSG — **120**
aa) Betreiber Sozialer Netzwerke als verantwortliche Stellen — **120**
bb) Relevanter Standort der verantwortlichen Stelle — **122**
cc) Ergebnis — **129**
2. Sachliche Anwendbarkeit — **130**
a) Einordnung Sozialer Netzwerke — **130**

b) Gemeinsame Anwendungsvoraussetzungen der datenschutzrechtlichen Vorschriften des TMG und BDSG — 131
aa) Datenverwendung — 132
bb) Personenbezogene Daten — 134
cc) Ergebnis — 140
II. Datenschutzrechtliche Anforderungen an Profile Sozialer Netzwerkseiten — 140
1. Vorgaben des TMG — 141
a) Spezielle Anwendungsvoraussetzung des TMG: Anbieter-Nutzer-Verhältnis — 141
aa) Anbieter-Nutzer-Verhältnis bei Third-Party-Tools — 141
bb) Ergebnis — 143
b) Pseudonyme Nutzungsprofile nach § 15 III TMG — 144
aa) Erfasste Datenarten — 144
bb) Rechtmäßig erhobene Daten — 148
cc) Begriffsauslegung Nutzungsprofil — 150
dd) Pseudonym — 152
ee) Zweckbindung — 153
ff) Kein Widerspruch des Betroffenen gegen Erstellung eines Nutzungsprofils — 154
gg) Datennutzung zum Zweck des Direktmarketings nach der DS-GVO — 154
hh) Ergebnis — 154
c) Löschpflicht — 155
d) Anonyme oder pseudonyme Dienstenutzung — 156
e) Ergebnis — 156
2. Vorgaben des BDSG — 157
a) Spezielle Anwendungsvoraussetzungen des BDSG — 157
b) Rechtmäßigkeit der Datenerhebung — 157
aa) Einordnung Sozialer Netzwerke in §§ 28, 29 BDSG — 157
bb) Vorgaben des § 28 I BDSG — 159
c) Rechtmäßigkeit der Datenverwendung zu Werbezwecken — 160
d) Rechtmäßigkeit der Datenverwendung zu sonstigen Zwecken — 160
aa) Sicherheit und Diensteoptimierung — 160
bb) Weitere Geschäftsmodelle — 162
e) Berichtigung und Löschpflicht, § 35 BDSG — 164

f) Ergebnis — 165
3. Unterrichtungs- und Benachrichtigungspflichten der Betreiber gegenüber Nutzern — 166
4. Einwilligung in Profilbildung und -nutzung — 167
a) Einholung der Einwilligung — 168
b) Wirksamkeitsvoraussetzungen der Erklärung — 169
aa) Freiwillige Einwilligung, § 4a I 1 BDSG — 169
bb) Informierte Einwilligung, § 4a I 2 BDSG — 172
cc) Form der Einwilligung, § 13 II TMG, § 4a I 3 BDSG — 175
dd) Hervorhebungsgebot bei AGB, § 4a I 4 BDSG — 178
ee) Widerruflichkeit — 179
c) Ergebnis — 179
5. Rechtsansprüche des Betroffenen — 179
a) Auskunftsrecht, § 34 BDSG — 180
b) Schadensersatzanspruch, § 7 BDSG — 181
6. Rechtmäßigkeit der Datenübermittlung in die USA — 181
a) Ungültigkeit der Safe Harbor-Entscheidung nach dem EuGH-Urteil vom 06.10.2015 — 182
aa) Ausgangsverfahren und Vorlagefragen — 183
bb) Entscheidungsinhalt und -begründung — 184
b) Konsequenzen für die Datenübermittlung an Facebook Inc. — 187
aa) Prüfung der Angemessenheit des Datenschutzniveaus durch Behörden — 187
bb) Alternativen zu Safe Harbor? — 188
c) Neuverhandlung von Safe Harbor — 189
aa) Weitere Kritikpunkte an der bisherigen Safe Harbor-Entscheidung — 189
bb) Verhandlungsergebnis — 192
d) Ergebnis — 193
7. Gesamtergebnis — 194
III. Zivilrechtliches allgemeines Persönlichkeitsrecht — 194
1. Anwendbarkeit — 195
2. Anwendung auf Profile — 195
IV. Durchsetzungsmechanismen — 196
1. Zivilrechtliche Rechtsdurchsetzung — 196
2. Hoheitliche Rechtsdurchsetzung — 197
a) Ordnungsrechtliche Maßnahmen — 197
aa) Sanktionsmechanismen — 197

bb) Zuständigkeit — 198
b) Straftatbestände — 199
3. Ergebnis — 200
D. Selbstregulierung — 200
I. Gesetzlich vorgesehene Möglichkeiten — 200
1. Normgebende Selbstregulierung — 200
2. Transparenzschaffende Selbstregulierung — 202
II. Initiativen — 203
1. FSM-Verhaltenskodex für Anbieter Sozialer Netzwerke — 204
2. Safer Social Networking Principles for the EU — 204
3. Ergebnis — 204
E. Gestaltungsbedarf — 205
I. Unsicherheit über die Anwendbarkeit nationalen Datenschutzrechts — 205
II. Mängel des materiellen Rechts — 206
1. Unterschätzung pseudonymer Nutzungsprofile — 206
2. Unzulänglichkeit von Transparenz- und Einwilligungserfordernissen — 206
a) Informiertheit — 207
b) Freiwilligkeit — 208
3. Fehlende Konkretisierung der Löschpflichten — 208
4. Ergebnis — 209
III. Durchsetzungsdefizit prozeduraler Natur — 209
IV. Ergebnis — 210

Kapitel 4
USA — 211
A. Einführung zum US-amerikanischen Schutz der Interessen an Privacy — 211
I. Rechtsquellen — 211
1. Common Law & Equity — 211
2. Kodifiziertes Recht — 212
3. Verhältnis Common Law und kodifiziertes Recht — 213
4. Selbstregulierung — 213
II. Rechtsgeschichtliche Entwicklung des Schutzes der Interessen an Privacy in den USA — 213
1. Begriff — 213
2. Entwicklung der Information Privacy im Privatrecht — 214
a) Right to be let alone — 214
b) Common Law Privacy Torts — 214

c) Fair Information Practice Principles — 215
d) Gesetzgebung zur Information Privacy von Bund und Bundesstaaten — 216
B. Verfassungsrechtliche Vorgaben — 217
I. Reichweite des verfassungsrechtlichen Schutzes — 217
II. Föderaler verfassungsrechtlicher Schutz — 218
1. Verfassungsrechtlich geschützte Betreiber- und Drittinteressen — 218
a) Sorrell v. IMS Health — 219
b) Bedeutung für Privacy-Gesetzgebung im privaten Bereich — 220
aa) Datenverarbeitung und -weitergabe — 221
bb) Datenerhebung — 222
cc) Einordnung kostenloser Sozialer Netzwerke und Folgen für die Regulierung — 223
c) Ergebnis — 226
2. Verfassungsrechtlich geschützte Nutzerinteressen — 226
a) Fourth Amendment — 227
aa) United States v. Jones — 228
bb) Clapper v. Amnesty International USA — 230
cc) Klayman v. Obama und ACLU v. Clapper — 231
dd) Ergebnis — 234
b) Right to Information Privacy — 234
c) First Amendment — 236
III. Gliedstaatlicher verfassungsrechtlicher Privatheitsschutz — 236
1. Kaliforniens Right to Privacy — 237
2. Anwendung auf Profile — 238
3. Rechtsdurchsetzung — 239
IV. Ergebnis — 240
C. Föderale einfachgesetzliche Regelungen — 240
I. Electronic Communications Privacy Act — 241
1. Rechtmäßigkeit der Datenerhebung — 242
a) Cookies — 243
b) Social Plugins — 244
c) Ergebnis — 244
2. Rechtmäßigkeit der Datennutzung — 245
a) Praktizierte Datennutzung — 245
b) Zukünftige Nutzungsmöglichkeiten — 246
3. Rechtsdurchsetzung — 247
4. Ergebnis — 247

II. COPPA — 248
D. Die Rolle der FTC für den Schutz von US-Privacy-Interessen — 248
I. Behördenstruktur — 249
II. Zuständigkeit — 249
III. Verfahren und weitere Befugnisse — 250
IV. Verfahren gegen Betreiber Sozialer Netzwerke — 253
V. Prüfungskriterien für Profile und ihre Anwendung — 255
1. Täuschende Geschäftspraktiken — 255
a) Prüfungskriterien — 255
b) Bewertungsfaktoren zur Bestimmung der Verbraucherperspektive — 256
c) Anwendung auf Profile: Information und Wahlmöglichkeit — 258
aa) Datenerhebung auf der Facebook-Website — 258
bb) Datenerhebung auf Drittseiten — 259
cc) Profilbildung — 260
dd) Datennutzung — 261
ee) Ergebnis — 262
2. Unlautere Geschäftspraktiken — 263
a) Dreistufentest — 263
b) Fallgruppen und ihre Anwendung auf Profile — 264
aa) Rückwirkende Änderung — 264
bb) Heimliche Sammlung sensibler Daten — 265
cc) Unfaire Gestaltung von Design und Voreinstellungen — 266
3. EU-US Safe Harbor- bzw. Privacy Shield-Prinzipien — 266
a) Informationspflicht — 267
b) Wahlmöglichkeit — 267
c) Anwendung auf Profile Sozialer Netzwerke — 268
d) Ergebnis — 268
VI. Ergebnis — 269
E. Gliedstaatliche Regelungen — 270
I. Einfachgesetzliche Regelungen ausgewählter Staaten — 270
1. California Online Privacy Protection Act — 271
2. California Shine the Light Act — 272
3. California Invasion of Privacy Act — 272
4. Unfair Competition Laws und Uniform Deceptive Trade Practices Acts — 273
5. Rechtsdurchsetzung — 273
6. Ergebnis — 274

II. Common Law Privacy Torts — 274
1. Intrusion into seclusion — 274
a) Eindringen in den Privatbereich — 274
aa) Datenerhebung — 274
bb) Profilbildung — 276
cc) Datenweitergabe — 277
dd) Ergebnis — 278
b) In hohem Maße beleidigend — 278
2. Appropriation und Right of Publicity — 279
3. Disclosure — 280
4. False light — 281
5. Einwilligung — 281
6. Rechtsdurchsetzung — 282
7. Ergebnis — 282
F. Selbstregulierung — 283
I. Gesetzlich vorgesehene Möglichkeiten — 283
II. Initiativen — 284
1. OBA-Selbstregulierungsprinzipien der FTC — 284
a) Erfasste Werbesysteme — 285
b) Erfasste Daten — 285
c) Vorgaben — 287
aa) Wahlmöglichkeit — 287
bb) Transparenz — 288
cc) Datensparsamkeit und zulässige Speicherdauer — 289
d) Ergebnis — 289
2. Wirtschaftsinitiativen — 289
a) Network Advertising Initiative (NAI) — 290
b) Digital Advertising Alliance (DAA) — 290
c) TRUSTe — 291
III. Ergebnis — 291
G. Gestaltungsbedarf — 292
I. Mängel des materiellen Rechts — 292
1. Unzureichende Regulierung der Profilbildung Sozialer Netzwerke — 293
2. Unzulänglichkeit von Transparenz und Wahlmöglichkeiten — 293
3. Keine Löschpflichten — 293
II. Durchsetzungsdefizit — 294
III. Ergebnis — 294

H. Weißbuch der Obama-Regierung: Consumer Data Privacy in a Networked World — 295
I. Diskussionsentwurf: Consumer Privacy Bill of Rights Act — 296
1. Privacy Bill of Rights und ihre Anwendung auf Profile — 296
a) Transparenz — 297
b) Individuelle Kontrolle — 298
c) Berücksichtigung des Kontexts — 298
d) Erforderlichkeitsprinzip — 299
e) Datensicherheit — 300
f) Einsichtnahme und Richtigkeit — 300
g) Verantwortlichkeit — 301
2. Durchsetzung des Consumer Privacy Bill of Rights Act — 301
3. Durchsetzbare Codes of Conduct als sicherer Hafen — 301
a) Ausarbeitungsverfahren: Verhandlungslösung und Registrierung — 302
b) Teilnahmevorteil „sicherer Hafen" — 303
c) Durchsetzung der Codes of Conduct durch private Verwalter — 303
4. Verhältnis zu sonstigen Regelungen — 303
5. Realisierungschancen des Consumer Privacy Bill of Rights Act — 303
II. Internationale Interoperabilität datenschutzrechtlicher Regulierungen — 304
1. Gegenseitige Anerkennung — 305
2. Internationale Aushandlung der Codes of Conduct — 305
3. Kooperation bei der Durchsetzung — 306
a) Multilaterale Initiativen — 306
b) Bilaterale Initiativen — 307
4. Ergebnis — 307
III. Ergebnis — 307

Teil 3: **Verbesserung des Privatheitsschutzes durch transatlantische Standards**

Kapitel 5
Chancen von Interoperabilität — 311
A. Gründe für vereinheitlichte Standards — 311
I. Aktuelle Interessenlage — 311
II. Vorteile — 314

III. Nachteile — 315
IV. Ergebnis — 316
B. Untergesetzliche Regulierungsmöglichkeiten und ihre Eignung für Profile Sozialer Netzwerke — 316
I. Verfassungs- und unionsrechtliche Vorgaben — 317
II. Vor- und Nachteile untergesetzlicher Regelungsformen — 318
III. Freiwillige oder regulierte Selbstregulierung — 319
IV. Eignung branchenweiter Regelungen für die Regulierung von Profilen Sozialer Netzwerke — 320

Kapitel 6
Formeller Rahmen transatlantischer Standards für Profile Sozialer Netzwerke — 322
A. De lege lata — 322
I. Bestehender Verfahrensrahmen — 322
II. Verbindlicher Prüfungsmaßstab — 323
1. „Common Law" der FTC? — 323
2. Angemessenheitsentscheidung der EU-Kommission — 324
3. Ergebnis — 324
III. Erfahrungen zu Verbreitung und Durchsetzung — 325
IV. Ergebnis — 325
B. De lege ferenda — 325
I. Verfahrensrahmen — 326
1. Verhandlungslösung und Registrierung — 326
2. Internationale Umsetzung — 326
a) Registrierung von Codes of Conduct — 326
b) Transatlantische Aushandlung mit Registrierung von Codes of Conduct — 327
II. Verbindlicher Prüfungsmaßstab: CPBR — 328
III. Erzielung branchenweiter Verbreitung — 328
1. Erhöhung der Anreize — 329
a) Sicherer Hafen — 329
b) Staatliche Gütesiegel — 329
2. Branchenweite verpflichtende Verbindlichkeit — 330
a) Internationale Vorbilder — 330
b) Negotiated Rulemaking Act, 5 U.S.C. §§ 561–570a — 330
3. Ergebnis — 331
IV. Verbesserung der Durchsetzung — 331
1. Kooperation der Aufsichtsbehörden — 331

2. Datenschutzaudits unabhängiger Privater — 332
a) Regelmäßige Überprüfung — 332
b) Veröffentlichung der Ergebnisse — 333
c) Transatlantisches Gütesiegel — 333
C. Ergebnis — 333

Kapitel 7
Inhalt transatlantischer Standards für Profile Sozialer Netzwerke — 335
A. Vom Regelungsbereich der CoC erfasste Daten — 335
B. Anforderungen an Profilbildung und -nutzung — 336
I. Profilbildung und -nutzung zu Werbezwecken — 336
1. Deutschland — 336
2. USA — 337
a) De lege lata — 337
b) De lege ferenda — 338
3. Transatlantische Lösung — 338
II. Profilbildung und -nutzung zu sonstigen kommerziellen Zwecken — 338
1. Deutschland — 338
2. USA — 339
a) De lege lata — 339
b) De lege ferenda — 340
3. Transatlantische Lösung — 340
III. Informationspflicht und Einholung der Einwilligung — 340
1. Allgemeine Vorgaben — 341
2. Konkrete Vorschläge — 341
a) 2-Klick-Lösung — 342
b) Informationspräsentation und Auswahlmöglichkeiten — 342
aa) Piktogramme — 342
bb) Privacy Label — 344
cc) Ergänzende Vorschläge unter Einbeziehung verhaltenswissenschaftlicher Studien — 344
dd) Präsentation von Widerspruchsmöglichkeiten — 348
ee) Ergebnis — 349
c) Regelmäßige Erneuerung der Einwilligung — 349
IV. Rechtsansprüche des Betroffenen — 350
C. Löschpflichten — 351
D. Ergebnis — 352

Kapitel 8
Schlussbetrachtungen — 353
A. Verifizierung der Arbeitshypothese — **353**
B. Mögliche Kritikpunkte an transatlantischen Standards — **355**
I. Frage der tatsächlichen Realisierbarkeit — **356**
1. Transatlantische Standards – eine Utopie? — **356**
2. Transatlantische Kooperation — **356**
II. Konsequenzen für den Einzelnen — **357**
1. Tatsächlicher Nutzen — **357**
2. Individueller Datenschutz — **358**

Literaturverzeichnis — 361

Verzeichnis sonstiger Quellen — 385

Sachregister — 405