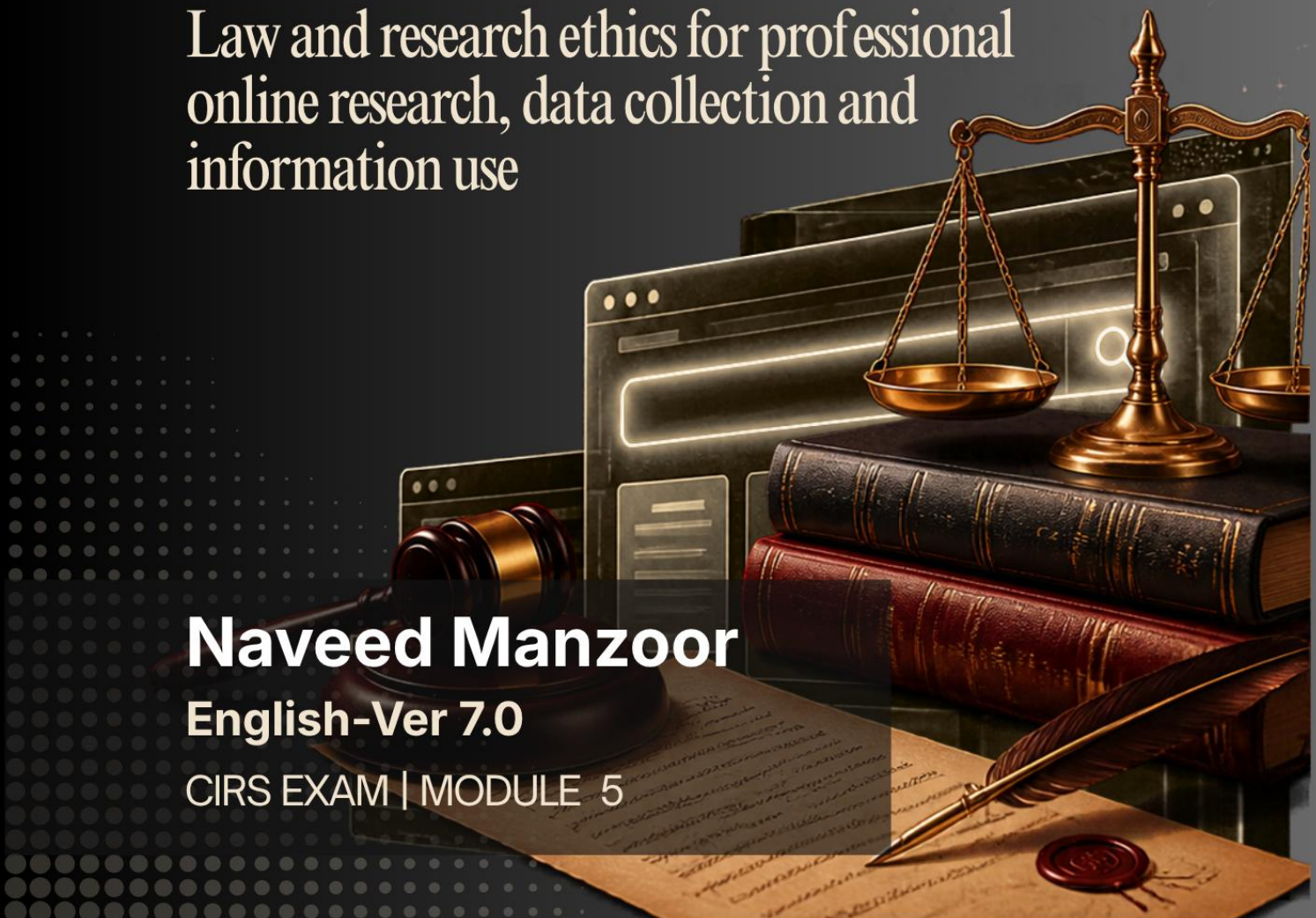
Association *of* Internet Research Specialists

Internet Law & Ethics



Law and research ethics for professional online research, data collection and information use



Naveed Manzoor

English-Ver 7.0

CIRS EXAM | MODULE 5

Internet Law and Ethics

Law and research ethics for professional online research, data collection and information use

Naveed Manzoor

Association of Internet Research Specialists
aofirs.org · Edition 7.0

Internet Law and Ethics: Law and research ethics for professional online research, data collection and information use

Edition 7.0, November 2026

Author: Naveed Manzoor

Published by the Association of Internet Research Specialists (AOFIRS), aofirs.org

Copyright © 2026 Association of Internet Research Specialists. All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, distributed or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, including use as training data for artificial intelligence systems, without the prior written permission of the Association of Internet Research Specialists, except for brief quotations in reviews and other non-commercial uses permitted by copyright law. Requests for permission should be made through aofirs.org.

CIRS™ (Certified Internet Research Specialist) is a trademark of the Association of Internet Research Specialists. Product, platform and company names mentioned in this book are trademarks of their respective owners. Their use is for identification and teaching only and does not imply any affiliation with, or endorsement by, those owners.

Statutes, treaties, regulations and court decisions are cited from official sources where available. Use cases and scenarios are fictional unless a source is given, and their names are placeholders. Illustrations are original diagrams drawn for teaching.

This edition supersedes all earlier editions. Treaty status, enforcement dates, court decisions and web sources cited were checked in October and November 2026.

Legal Disclaimer

This book is published for education and professional training. It explains internet law, intellectual property law and research ethics as they stood when it was written, and the author and publisher have taken care to check its statements against official and reliable sources.

Not legal advice. Nothing in this book is legal advice, and reading it does not create a lawyer–client relationship. Internet law differs between countries, states and provinces, and it changes quickly: treaties gain parties, regulations take effect in stages, and courts reverse or refine earlier decisions. Summaries of laws, cases and regulations in this book are simplified for teaching and are current only as of the date stated. Before acting on any question with legal consequences, consult a qualified lawyer in the relevant jurisdiction.

International scope. The book teaches generally accepted principles and uses the laws of particular countries as examples. It does not set out the complete law of any country. The absence of a law in one country does not remove obligations owed under the laws of other countries where data subjects live, where content owners are protected or where your client or servers are located.

Ethics guidance. The ethical frameworks and professional codes described are guidance for professional judgment. They do not replace the requirements of your employer, client, ethics review board or professional body, which may be stricter.

Your responsibilities. You are responsible for collecting, using and publishing information lawfully and ethically; for complying with the terms of service of websites, platforms and APIs; for protecting personal and confidential data; for respecting intellectual property; and for documenting your decisions.

Third-party content. This book refers to many websites, organisations, courts and regulators that the author and publisher do not control. References to them are not endorsements, and the author and publisher are not responsible for their content or availability.

No warranty. The content is provided "as is", without warranty of any kind, express or implied, including warranties of accuracy, completeness or fitness for a particular purpose. To the fullest extent permitted by law, the author and the Association of Internet Research Specialists accept no liability for any loss or damage arising from the use of, or reliance on, the information in this book.

Contents

LEGAL DISCLAIMER III

PREFACE II

ABOUT THE AUTHOR III

HOW TO USE THIS BOOK IV
What you will be able to do iv
Study plan v

CHAPTER 1 INTERNET LAW ESSENTIALS FOR ONLINE RESEARCHERS 2
Objective 2
What you will learn 2
Lessons in this chapter 2

LESSON 1 Foundations of Internet Law for Researchers 3
Why internet law is needed 3
Legal issues in emerging technology 4
Sources of internet law and their authority 4
What generally accepted means: four layers 5
The international landscape in November 2026 6
Emerging issues and where the law now stands 9
Use case: which layer answers the question? 9

LESSON 2 Jurisdiction and Conflict of Laws 11
How courts decide they have jurisdiction 11
Personal jurisdiction online 11
Subject-matter jurisdiction 12
Choice-of-law and forum-selection clauses 12
Territorial and extraterritorial reach: GDPR Article 3 12
Case: Google v CNIL and the limits of reach 13
Your legal role on a project 13
Conflict of laws and the most protective rule 14
Use case: mapping a five-country project 14

LESSON 3 Lawful Access and Cybercrime Law 17
International harmonisation 17
How national laws define illegal access 17
Case: Van Buren v. United States (2021) 18
Applying authorisation to common barriers 19
Pretexting, fake personas and social engineering 20
Breached and leaked data 21
Use case: the closed employee group 21

LESSON 4 Automated Collection, Web Scraping and APIs 23
The four-layer analysis 23
Case: hiQ Labs v. LinkedIn, from start to finish 24
Clickwrap, browsewrap and API terms 25

The Robots Exclusion Protocol (RFC 9309) 25
Public personal data is still personal data 26
Case: Clearview AI 26
Server load, rate limits and identifying your agent 27
Use case: job advertisements for a labour-market study 27

LESSON 5 Data Protection Principles Shared Worldwide 29
What counts as personal data 29
The OECD principles 30
Convention 108 and 108+ 30
The GDPR principles 30
Choosing and documenting a legal basis 31
The legitimate-interests balancing test 31
Special categories and criminal-offence data 32
Research and journalism exemptions 32
The rights of the people in the data 33
Use case: sentiment about a new medicine 33

LESSON 6 Comparative Privacy Regimes and Cross-Border Transfers 35
The regimes compared 36
United States: a patchwork 36
India: the DPDP Act and Rules 37
Moving data across borders 37
The EU-US Data Privacy Framework 38
Other transfer regimes and localisation 38
Breach notification 39
Retention and secure deletion 39
Use case: a multinational due-diligence project 39

LESSON 7 Contracts, Terms of Service and Research Agreements 41
The research services agreement 41
Terms of service: reading them like a contract 43
Public use of information: laws and licences 43
Obtaining permission 44
Protecting research work from legal liability 44
Use case: an engagement letter that protects both sides 45

LESSON 8 Publishing Research: Defamation, Platforms and Evidence 46
Defamation across jurisdictions 46
Privacy torts and misuse of private information 47
Case: Google Spain and the right to be delisted 47
Intermediary liability and takedown 48
Evidence: capture, hashing, chain of custody and verification 48
Use case: pre-publication review of a due-diligence report 49

LESSON 9 AI Regulation and Legal Risk Management 51
The EU AI Act 51
The timeline after the Digital Omnibus 51
Labelling AI-generated content and deepfakes 52
The Council of Europe Framework Convention on AI 53
Building a legal risk register 53
When and how to escalate to counsel 54
Staying current 55
The pre-collection legal due-diligence checklist 55

Use case: an AI-assisted brand-risk monitor 55

CHAPTER 1 Knowledge Check 57
Answer key 59

CHAPTER 2 INTELLECTUAL PROPERTY LAW FOR ONLINE RESEARCH 60
Objective 60
What you will learn 60
Lessons in this chapter 61

LESSON 1 IP for Researchers and the International Framework 62
IP is territorial 63
The Berne Convention 63
TRIPS and the WTO 64
The WIPO Internet treaties 64
Which law applies, and the most protective rule 65
Use case: one report, four countries 65

LESSON 2 Copyright Fundamentals and Owners' Rights 67
The exclusive rights 67
Some straight facts about copyright 67
Originality, facts and data 68
How long copyright lasts 69
Moral rights 70
Use case: is this table protected? 70

LESSON 3 Infringement, Linking, Embedding and Online Uses 72
Three forms of infringement 72
Examples of infringement 73
Infringement online 73
Piracy 73
Caching and browsing 73
Linking, deep linking, embedding and framing 74
Screenshots, images and video 75
Archiving web pages 76
Detecting infringement online 76
Use case: a video in a client report 77

LESSON 4 Exceptions, Public Domain and Rights Clearance 78
The three-step test 78
Fair use in the United States 78
Fair dealing and other closed exceptions 79
The quotation right 80
The public domain 81
Checking public domain status in the United States 81
Checking public domain status elsewhere 81
Orphan works 82
The permission process 82
A rights-clearance decision tree 83
Use case: ten items for a client report 83

LESSON 5 Text and Data Mining, AI Training and AI Outputs 85
European Union: two exceptions and the opt-out 85

Japan: Article 30-4 and its limits 86
United Kingdom: no change yet 86
United States: fair use, case by case 87
Other jurisdictions 87
The EU AI Act: copyright duties for model providers 88
How rights are reserved in practice 89
Using AI tools in research 89
Use case: mining news for a classifier 90

LESSON 6 Databases, Licences and Open Content 92
Databases and compilations 92
Creative Commons licences 93
Licence compatibility 93
Open data licences 94
Commercial data and API licences 94
When contracts override exceptions 95
Use case: combining four datasets 95

LESSON 7 Trademarks and Domain Names Online 97
The international framework and national law 97
Infringement: likelihood of confusion 97
Dilution: blurring and tarnishment 98
Trademarks in research reports 98
Trademark infringement on the internet 99
Domain names, typosquatting and cybersquatting 99
Pagejacking, linking and framing 100
Meta tags, hidden text and keyword advertising 100
Use case: brand-protection research 100

LESSON 8 Patents and Patent Research 102
Requirements for patentability 102
Patent infringement 103
How to perform patent research 103
1. Establish your goals 104
2. Determine keywords and classifications 104
3. Pick the search tools 104
4. Find what you need 105
5. Examine findings and adjust 105
6. Consider consulting an expert 106
Use case: a worked patent search 106

LESSON 9 Trade Secrets, Leaked Material and an IP Checklist 108
Trade secrets and confidential information 108
Leaked and confidential documents 109
Use case: a competitor's price list 109
An IP checklist for research reports 110

CHAPTER 2 Knowledge Check 112
Answer key 114

CHAPTER 3 RESEARCH ETHICS ESSENTIALS: DATA, PRIVACY AND INTELLECTUAL PROPERTY 116
Objective 116

What you will learn 116
Lessons in this chapter 116

LESSON 1 Foundations: Law Is the Floor, Not the Ceiling 118
What ethics is 119
Law, ethics and professional obligations 119
Internet research ethics 120
Key guiding principles 121
The Menlo Report: four principles for ICT research 121
Four ways of reasoning about right and wrong 122
International reference points 123
Case: the 2016 dating-profile data release 125
Use case: lawful, but is it right? 125
Ten essentials of ethical online research 126

LESSON 2 Ethical Data Collection 128
Tool or venue, observer or participant 128
Purpose first 129
Honesty about who you are 129
Case: research on volunteers who did not know they were subjects 130
Honouring robots.txt, opt-outs and expressed wishes 130
Courtesy to site owners 131
Ethics across the research lifecycle 131
Use case: a review-collection plan, minimised 132

LESSON 3 Respecting Privacy Beyond Compliance 134
Public is not permission 134
Reading a site's privacy level 135
Privacy, anonymity and confidentiality 136
Aggregation and the mosaic effect 136
Re-identification: anonymised is not anonymous 137
Case: AOL search logs, 2006 137
Case: the Netflix Prize dataset, 2006–2010 137
Vulnerable groups 138
Doxxing, harassment and the duty not to expose 138
Minimising harm: the Berkeley Protocol 138
Use case: a supplier check that stops at the right place 139

LESSON 4 Consent, Online Communities and Human Participants 141
Does the research involve human participants? 141
Ethics review around the world 142
Informed consent 143
Consent online in practice 144
Consent and minors 144
The limits of consent in big-data research 145
Case: the emotional contagion experiment, 2014 145
Online community norms 145
Quoting posts 146
Ethical recruitment 146
Use case: recruiting gig workers for online interviews 147

LESSON 5 Respecting Intellectual Property and Creators 149
Plagiarism and infringement are different wrongs 149
Accurate, complete attribution 150

Keeping licence promises 150
Respecting creators' opt-outs 150
Legitimate sources 151
Participant agreements and disclaimers 151
Use case: images in a client report 152

LESSON 6 Information Integrity and Responsible Use 154
Provenance and verification 154
Misinformation and disinformation 155
Honest selection and presentation 155
Saying how sure you are 155
Corrections and retractions 156
Use case: a viral video before a client briefing 156

LESSON 7 Ethical Use of AI in Research 158
Principles that apply to researchers 158
Hallucinations and fabricated citations 159
Bias 159
Confidentiality 159
Disclosure and accountability 159
AI agents, synthetic personas and deception 160
What AoIR says about AI 160
An AI-use policy for a research team 160
Use case: summarising a foreign-language forum with AI 161

LESSON 8 Ethical Decision-Making and Professional Conduct 163
The seven-step ethical decision framework 163
Use case: a worked decision record 164
Confidentiality, conflicts of interest and client pressure 164
Security, retention and secure deletion 165
Researcher wellbeing and safety 166
Professional codes and a personal code of conduct 166

CHAPTER 3 Knowledge Check 168
Answer key 170

CAPSTONE A: CROSS-BORDER LEGAL RISK ASSESSMENT 171

CAPSTONE B: ETHICS CASE PORTFOLIO 173

GLOSSARY 174

REFERENCES 179

INDEX OF TERMS 189

Preface

A single online research project can involve a researcher in one country, a website hosted in a second, a client in a third and the people described in the data living in several more. Each of those places has its own law on access to computers, on personal data, on copyright and on what may be published about whom. There is no single world internet law, and the absence of a rule in your own country does not protect you from the rules of the others. Much of what researchers do is also perfectly legal and still capable of harming people.

This book is written to give online research professionals a working command of both. It brings together three lessons from the AOFIRS CIRS curriculum, *Introduction to Cyber Law*, *Intellectual Property Law* and *Internet Ethics*, each rewritten, checked and extended for Edition 7.0, and organises them according to the AOFIRS course outline *Internet Law and Research Ethics: Course Outlines for Professional Online Research, Data Collection, and Information Use*. Part I, *Internet Law Essentials*, asks what the law allows, requires and prohibits. Part II, *Research Ethics Essentials*, is a separate course in its own right: it asks what is right, fair and respectful even where the law is silent.

The emphasis throughout is on generally accepted law and ethics as applied internationally. Each topic starts from international treaties and widely adopted principles, such as the Berne Convention, the Budapest Convention, Council of Europe Convention 108, the OECD Privacy Guidelines and the UNESCO Recommendation on the Ethics of AI, then shows how influential regimes such as the EU General Data Protection Regulation and the EU AI Act reach beyond their borders, and how the United States, the United Kingdom, Canada, India, China, Brazil, Japan, South Africa and others compare. The practical rule the book teaches is simple: identify every regime that may apply, and plan to the most protective of them.

Much has changed since the earlier lessons were written. Courts have ruled on web scraping, on training AI systems with copyrighted works and on what counts as unauthorized access; regulators have fined companies for scraping personal data; the EU AI Act has begun to apply in stages; new treaties on cybercrime and artificial intelligence have opened for signature. Where the earlier lessons had been overtaken by events, or were wrong, the chapters say so in **What has changed** boxes. Every chapter includes use cases that show how a researcher works through a real legal or ethical question, step by step. Claims about treaties, statutes, cases and regulations are cited to official sources wherever possible and collected in a single list of references. Treat every date, ratification count and enforcement status as a snapshot from November 2026. The book is written for internet research specialists, OSINT and due-diligence analysts, investigators, market and social researchers, paralegals and compliance staff, librarians, journalists, students and candidates preparing for the CIRS™ certification. No prior legal training is needed.

Thank you to the AOFIRS members, students and instructors whose questions over many years shaped these chapters.

Naveed Manzoor-Florida, November 2026

Association of Internet Research Specialists

Know the law. Do what is right.

Online research crosses borders in a single click: a researcher in one country, a website in a second, a client in a third and the people in the data somewhere else again. Internet Law and Ethics gives research professionals the working command of internet law and research ethics that this demands.

Part I explains generally accepted internet law as it applies internationally: jurisdiction, lawful access and cybercrime, web scraping and APIs, data protection and cross-border transfers, copyright, text and data mining and AI training, licences, trademarks and patents, defamation and evidence, and the new law on artificial intelligence. Part II, a self-contained course in research ethics, shows how to collect data, respect privacy, handle consent and credit creators when the law is only the minimum.

Fully revised for Edition 7.0, with use cases, real court decisions, checklists, a seven-step ethical decision framework, two capstone projects, a glossary and a knowledge check in every chapter.

Naveed Manzoor is the founder of the Association of Internet Research Specialists (AOFIRS) and creator of the Certified Internet Research Specialist (CIRS™) program. With twenty-five years of experience teaching online research to investigators, legal professionals and analysts in more than 80 countries, and nine technical books, he brings a practitioner's view of where law and ethics meet everyday research.

For researchers, OSINT and due-diligence analysts, investigators, paralegals, librarians, journalists, students and CIRS™ candidates.

ASSOCIATION OF INTERNET RESEARCH SPECIALISTS
aofirs.org· Edition 7.0 · © 2026 AOFIRS

