INDEX

Abuse of power, 24
Acceptance approach, 147
Accountability, 125
Advanced Big Data Value Chain for Public Safety and Personal Security (AEGIS), 84
Algorithms, 23
American Society for Public Administration (ASPA), 35
Analogue surveillance in digital world, 178–179
ANOM, 184–188
Anonymity, 39, 204
Anti-apartheid Movement (AAM), 182
Anticipation, 26
Arab Spring, 2
Artificial intelligence (AI), 73–74, 189–191
Australian Federal Police (AFP), 184
Australian National Health and Medical Research Council (ANHMRC), 29–30
Autoethnography, 47
Autonomy, 24
  emerging demands for, 20–21

Being Covert, 4
Bias, embedding of persistent outliers and, 61–65
Big Data, 7, 208–209
  and 'datafication' of society, 72–73
  analytics, 62
  continuity (or not) of data science research ethics, 74–75
  divide, 81–85
  as enabler of growth, 73–74
  Governance and Legislation, 85
  and its impact on privacy, 75–81
  from public sector perspective, 84–85
  for public use, 84–85
Big Data Value Association (BDVA), 79
Black box, 63
Bottom-up approaches, 149–151
British Social Attitudes (BSA), 187
British Society of Criminology (BSC), 34
British Sociological Association (BSA), 31
Bundesverfassungsgericht (BVerfG), 122–123

Capabilities, 133
Capacity of individuals, 19
Care, 10
Care Act 2014, 101
Causation, 56–58, 64
Charter of Fundamental Rights (CFR), 120
Chemical, Biological, Radiological and Nuclear weapons (CBRN weapons), 133
Chicago sociology, 3
Citizen engagement, 26
Closed Circuit Television (CCTV), 22, 124–125, 178
Code of ethics, 42
Coercion, 11
Commercial advertising, 3
Commercial uses of surveillance, 13
Community policing, 22
Community-based approaches, 8, 147–148
Concept mapping, 168
Confidential Human Source, 185
Confidentiality, 33, 39, 97, 163, 204
Confidentiality Advisory Group (CAG), 101
Confirmability, 171
Confounding variable, 57
Confrontational, 22

Consent, 31–33, 204 (*see also* Informed consent)
research without, 36–37
Consented/consensual surveillance, 201
Consenting, 3
Consumers, 3
Context, 201–202, 207–208
Contrived methods, 168
Control, 10, 31–33
Corporate espionage, 12
Corporate practices, 11
Correlation, 58–59
of data, 56
predicting future on strength of past, 65–68
Coventry dilemma, 11
Covert
being, 4
studies, 5–6
Covert observation, 2
Covert research, 2, 36, 42
'asking for subjects' consent, 46–47
autoethnography and online research, 47
covert method most suitable way of getting into field, 45–46
covert research, 48
guidance for policymakers on, 205–209
guidance for reviewers on, 200–205
informed consent, 44
informed consent inevitably concerns only initial research design, 45
informing subjects, 43–44
learned through unintentional covert research, 44–45
lying must be exception, 43
moderate defence of grounds for, 43
overt and covert research not clearly distinguishable, 43
radical approach, 48–50
researcher chooses to hide identity, 46
risk of causing harm with qualitative research, 47
superiority of situated ethics, 48
Covert surveillance
of activist groups by undercover police, 178–184
by human beings, 178–179
COVID-19 pandemic, 2, 12, 14
Credibility, 170
Crime, 20
prevention technologies, 24
Criminal acts, 34
Criminal law, 34
Critical security studies, 146
Cross-validation, 36
Cryptography, 24
Culture of surveillance, 22

Dark Internet, 21
Data analytics, 78, 203
Data collection on people, 59–60
Data management, 23
Data ownership, 85–88
Data processing technologies, 23
Data protection, 31, 32, 120, 122–123, 125
Data slippage, 18, 23
Data sovereignty, 87
Data tracking technologies, 191
Datafication, 81
of society, 72–73
Dataveillance, 85
Deception, 2–3, 6, 206–207
Deceptive research
guidance for policymakers on, 205–209
guidance for reviewers on, 200–205
Decryption, rights and wrongs of, 186–188
Deductive reasoning, 161–162
Deductive research, 162
Deep internet, 21
Dependability, 171
Deterrents, 133
Deutsche Demokratische Republik (DDR), 121
Digital ecosystem, 20
Digital modernity, 19
Digital recording, 163
Digital revolution, 20

Digital technologies, 21
Digitalisation, 19
Discrimination, 81–85
Distrust, 2, 208
Domestic extremists, 183–184
Dual use, 24, 133
  capacity, 133
  DURC, 139–141
  framework for defining accountability and responsibility in research, 133–139
Dual use research of concern (DURC), 133, 139–141
Due Process, 35
Duties of researchers, 37–39
Duty of confidentiality, 34

Economic and Social Research Council (ESRC), 32
Economics, 19
Education, 188–191
Educational technology (EdTech), 187, 189–191
Embedding of persistent outliers and bias, 61–65
Emotional AI, 188–191
Encryption, rights and wrongs of, 186–188
End-users, 168–169
Entitlement, 10
Equality, 35
Espionage, 11
Establishing trust, 169–171
Ethical engagement, 10
Ethical grid, 193
Ethical issues, 178
  of dual use, 24
Ethical research, 37–39
  approach, 162–165
  in sensitive security domains, 171–172
Ethical review, 37
Ethical rules, 29
Ethics
  of care, 26
  challenges, 81
  of espionage, 11
  of journalism, 13
  of monitoring, 11–12
  review committees, 7
Ethnicity of students, 59
Ethnographic methods, 167
EU Agency for Network and Information Security (ENISA), 77–78
Europe, privacy in, 119–120
European Convention on Human Rights (ECHR), 110
European Data Protection Supervisor (EDPS), 74
'European legal and ethical standards for the protection of citizens' privacy, 127–128
European Privacy Association, 80
European Union (EU), 75, 120
Evidence-gathering activity, 4
Exploitation, 11

Fabrication, 21
Face recognition in social media, 24
Facial recognition systems, 14
Fairness, 35
False positives, 23
Falsification, 21
Financial model, 13
Focus groups, 167

Gender equality in science, 26
General Data Protection Regulation (GDPR), 120
General practitioners (GPs), 60, 96
General Regulation on the Protection of Personal Data (GDPR), 76
German Census Case (1983), 122–123
German experiences of security agencies, 120–122
Germany, privacy in, 119–120
Gestapo, 120–122
Google, 38
Google Classroom, 188
Governance, 26
  of education technology in schools, 189
Government institutions, 150

Harm, 2, 4
Harmless surveillance, 10
Health and Social Care Act 2012, 102
Health and Social Care Information Centre, 102
Health data, 60
Health Protection, 99–100
Health Research Authority (HRA), 101
Health Service Regulations 2002, 98–99
Health surveillance using health data, 96–98
Health-related surveillance, 94
Helsinki Declaration, 61
Hidden bias, 62–63
Historic data processing, 60
Human agency, 20
Human behaviour, 2
Human dignity, 38, 75–77
Human factors approach, 166
Human rights, 33, 38
Humanitarian space, 146
Humanitarian workers, 146

ICTs, 19, 22–23
Immersive fieldwork, 5
Inappropriate surveillance technologies, 24
Inclusiveness, 26
Incomplete disclosure, 5
Independent advisory board, 111–113
Independent oversight, 125
'Individuals' control over personal data, 75
Inductive reasoning, 161–162
Inductive research, 162
Inequality, 2
Infiltration, 181
Inform policy, 208–209
Information privacy, 31–33
Informed consent, 36, 44, 60
  inevitably concerns, 45
Innovative methodological approaches, 3
Institutional Review Boards (IRBs), 3, 6, 42, 132, 134, 138–139
Integrity, 26
International authorship, 7
International Data Space Association (IDSA), 87
Internet, 21, 123
  environment, 20
Internet of things (IoT), 124
Intrusive threat, 160
Intrusiveness, 7

Journalism, 13
Journalists, 4

Knowledge communicating back to end-users and stakeholders, 168–169
Knowledge elicitation
  conducting, 165–166
  methods, 166–168
Knowledge management in security, 153–155
Knowledge of truth, 48

Language Model for Dialogue Applications (LaMDA), 189
Large-scale data analytics, 56–57
Late modernity, 19
Laundering surveillance, 185–186
Law and judicial control, 108
  judicial review, 111
  limits to ability to scrutinise merits of individual decisions, 109–111
  room for conflicting legislative purposes, 108–109
Law enforcement authorities, 21
Leaky containers, 23–24
Legality, 61
Legislation, 61
Legitimacy, 58–61
Liberal democracies, 2
4 Little Trees, 190–191

Memorandum of Understanding (MoU), 94
Metropolitan Police, 181
Micro-targeting, 13

Military, 137
Mixed methods, 162
Modern civilisation, 39
Motor insurance policies, 63
Mutual augmentation, 21

National Health Service Act 2006, 96
National Public Order Intelligence Unit (NPOIU), 179–180
National Security Agency (NSA), 178
Naturalistic observation methods, 7
Non-health surveillance using health data, 102–103
Non-health-related purposes
  law and judicial control, 108–111
  social legitimacy of health data sharing through institutional design, 105–108
  UK legal framework for use of health data, 95–105
Non-proportionate surveillance technologies, 24
Non-reactivity, 163
'Notice and consent' model, 80–81
Novelists, 4
Nuremberg Code, 36, 61

Observation, 5
Observational methods, 167
Observational studies, 5
Oligopoly, 22
Online research, 47
Open access to research data and publications, 26
Operation Trojan Shield, 184–188
Organisational approaches (*see* Systems-based approaches)
Organisational research, 31–32

Patient information, 94
Persistent outliers and bias, embedding of, 61–65
Personal data protection, 23
Personal data space (PDS), 79
Personal data store approach, 77–80
Phantom Secure, 184
Phone interception, 24
PIAG, 97–98, 101
Placebo, 3
Plagiarism, 21
Policing, 11
Policymakers, 2, 207–209
Political advertising, 13
Political angle, 13
Political threat, 161
Politics, 19
Post-academic research, 19
Post-modern society surveillance in context of, 18–20
Preferred approach, 10
Privacy, 7, 10, 24, 30–31, 120, 122–123, 126–127
  and current state of technological development, 123–125
  by design, 78
  by design and by default, 126–127
  in Germany and Europe, 119–120
  information, 31–33
  limits of, 33–35
  protection, 23
Privacy Enhancing Technologies (PETs), 78
Private investigators, 13–14
Private sector, 14
Private surveillance, 13
Proportionality, 110
ProPublica, 192
Public administrations, 19
Public interest, 105, 204–205
Public sector, 14
Public space, 178
Public sphere, 33
Purposive sampling, 163–164

Qualitative research, 7
  risk of causing harm with, 47
Quantified self practices, 22

Radical approach, 48–50
Recruitment of participants through professional networks, 164
Reflexivity, 26

Representativeness, 35
Research (*see also* Covert research)
  ANHMRC, 29–30
  approaches, 200–201
  without consent, 36–37
  ethical research, 37–39
  ethics, 26, 133–134, 136
  governance, 136–138
  information privacy, 31–33
  integrity, 135–136
  limits of privacy, 33–35
  philosophy, 49
  privacy, 30–31
  relationship, 202
  in sensitive domains, 160–161
Research Ethics Committees (RECs), 3, 6, 42, 132, 134, 138–139, 141
Researcher positionality, 208
Reserved territory, 33
Responsible Research and Innovation (RRI), 26
Responsible surveillance, 25–26
Responsiveness, 26, 35
Restricting informed consent, 5
Rights (human), 33, 38
Rights, 33
Rights of citizenship, 38
Rings of steel, 14
Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies Project (RESPECT Project), 23

Safeguarding participants and researchers, 164–165
Sanctions, threat of, 161
Scenarios, 167
  scenario-based modelling, 168
Science, 2
  education, 26
  and innovation, 19–20
Scientific method, 2
Security, 11, 126–127
  emerging demands for, 20–21
Security risk management, 146
  approaches to, 147–149
  conflict between procedures and experience, 151–152
  field experience, 152
  knowledge management in security, 153–155
  top-down and bottom-up approaches, 149–151
  training, 152–153
Seedhouse, 193
Self-surveillance, 22
Sensitive domains, research in, 160–161
Sensitive security domains, ethical research in, 171–172
Sensory power, 191
Sharing the wealth model, 77–80
Signals intelligence, 11
Situated ethics, 202
Smartphones, 124
Social cooling, 81–85
Social costs, 23
Social costs of surveillance, 18, 22–25
Social demands, 18, 20
Social institutions, 19
Social legitimacy, 94
  demographic information, 105–106
  of health data sharing through institutional design, 105
  legislative purpose and (social) legitimacy, 106–108
Social movements, 121
Social policy, 34–35
Social Policy Association (SPA), 33
Social profiling, 21
Social Research Association (SRA), 34
Social sorting, 18, 23, 81–85
Social subjectivity, 20–21
Social welfare, 11–12
Socialisation, lack of, 25
Socialist Workers Party (SWP), 183
Societal trust, 22–25
Sousveillance, 22, 25
Special Demonstration Squad (SDS), 179, 182–183

Spy satellites, 12
Spycops' Scandal
  analogue surveillance in digital world, 178–179
  domestic extremists, 183–184
  issues raised during UCPI, 179–180
  other harms of undercover surveillance, 181
  proportionality of political intelligence gathering by undercover police, 182–183
  undercover surveillance and human rights, 180–181
Stakeholders, 168–169
Stanford psychology, 3
Stasi, 120–122
State actors, 25
State security, 120
State surveillance, 11, 21
Stigmatisation and manipulation of civil rights, 77
Subjectivity of people, 19
Subversives, 183–184
Superiority of situated ethics, 48
Surveillance, 11, 18, 60, 121, 188–191
  commercial uses of, 13
  in context of post-modern society, 18–20
  creep, 18
  culture, 18
  design of, 20
  ethics, 10–11
  objection, 60
  of others, 22
  in private, 12
  in public places, 11
  responsible surveillance, 25–26
  social costs of, 18, 22–25
  social subjectivity and emerging demands for security and autonomy, 20–21
  surveillance/function creep, 23
  surveillance/research distinction, 101
  understandings of, 21–22
Surveillance research, 4
  guidance for reviewers on, 200–205
Surveillance society, 18
Surveillance Studies Network, 10, 18
Surveillance Study Network, 22, 27*n*2
Systems-based approaches, 8, 148–149

Targeting advertising, 13
Task analysis, 167
Tearoom Trade (Humphrey), 47
Technological surveillance, 178
Terrorism, 11, 20–21
Top-down approaches, 149–151
Training, 152–153
Transferability, 170–171
Transparency, 125
Transparency in evolving world of big data analytics, 80–81
Treaty of Lisbon, 120
Triangulation, 36
Triple helix innovation model, 19
Trust, 49
  public, 21, 24
  social, 18, 24
  social costs of surveillance and societal trust, 22–25
Trustworthiness of qualitative data, 169–171
Twitter, 38

UK legal framework for use of health data, 95
  additional requirements, 98–99
  background and legal context, 95–96
  disclosure to home office under MOU, 103–105
  Health Protection, 99–100
  health surveillance using health data, 96–98
  non-health surveillance using health data, 102–103
  surveillance/research distinction, 101
Undercover police, 178–184

Undercover Policing Inquiry (UCPI), 179
  issues raised during, 179–180
Undercover work, 181
Undisclosed research, 36
Unethical *en masse*, 57
Unethical research procedures, 2
United Kingdom (UK), 94
Universal Declaration of Human Rights states, 30
University recruitment, 62
US *National Security Agency* (NSA), 122
US Supreme Court, 14

Value, 73
Variety, 73
Velocity, 73
Veracity, 73
Verbal protocol analysis, 168
Volume, 73
Voluntary participation, 3
Vulnerability, 3

Watchdog, 112
Welfare (public/social), 11, 67
Wired, 186
Workplace surveillance, 11