1. Record Nr. UNINA9910465582903321

Autore	Seligmann Matthew S. <1967->
Titolo	Spies in uniform [[electronic resource]] : British military and naval intelligence on the eve of the first World War / / Matthew S. Seligmann
Pubbl/distr/stampa	Oxford ; ; New York, : Oxford University Press, 2006
ISBN	1-280-90529-8 0-19-151463-2
Descrizione fisica	1 online resource (287 p.)
Disciplina	355.3/432/094109041
Soggetti	Military intelligence - Great Britain - History - 20th century World War, 1914-1918 - Military intelligence - Great Britain Electronic books.
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references (p. [264]-268) and index.
Nota di contenuto	Contents; Abbreviations; Map; Introduction; 1. Court and Social: The Role of the Service Attache; 2. Spies in Uniform: British Service Attaches as Intelligence-Gatherers; 3. Men and Machines: Service Attaches as Procurers of Information on Personnel and Materiel; 4. Harbingers of the German Menace: The Service Attaches' Perspective on Germany; 5. Taking Centre Stage: The Influence of the Service Attaches on the British Government; Conclusion; Bibliography; Index; A; B; C; D; E; F; G; H; I; J; K; L; M; N; O; P; R; S; T; V; W; Y; Z
Sommario/riassunto	Did the British Government go to war in 1914 because of a well-founded fear of a German threat or did it, as some would now argue, send thousands to their deaths to fight against a danger, the existence of which was not even backed by any hard intelligence? To address this question, Spies in Uniform examines the information sent back from Germany by the Government's principal intelligence source, its 'men on the spot', the service attach--eacute--;s in Berlin. Using their reports, previously thought to have been lost, the book demonstrates that the intelligence picture of Germany available to

2. Record Nr. UNISA996495562603316

Titolo	Privacy symposium 2022 : data protection law international convergence and compliance with innovative technologies (DPLICIT) / / edited by Stefan Schiffner, Sebastien Ziegler, Adrian Quesada Rodriguez
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-09901-X
Descrizione fisica	1 online resource (254 pages)
Disciplina	943.005
Soggetti	Data protection - Law and legislation
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Executive Commitee -- Steering Committee -- Program Commitee -- Additional Referees -- Sponsoring Institutions -- Contents -- Part I Privacy Friendly Data Usage -- 1 An Overview of the Secondary Use of Health Data Within the European Union: EU-Driven Possibilities and Civil Society Initiatives -- 1 Introduction: The Potential of the Secondary Use of Data for Health and Care in the European Union -- 2 The Legal Framework in the European Union -- 2.1 The Secondary Use of Health Data Within the General Data Protection Regulation (GDPR) -- 2.2 The Data Governance Act: A Debated First Approach to the Secondary Use of Data -- 2.3 Artificial Intelligence and Personal Data in the EU Framework -- 3 Initiatives Towards the Use of Data Within Healthcare Research -- 3.1 Policymaker Initiatives -- 3.2 Civil Society Initiatives -- 4 Discussion -- 5 Conclusions -- References -- 2 Multi-Party Computation in the GDPR -- 1 Introduction -- 2 Multi-Party Computation -- 2.1 Introduction -- 2.2 Private Set Intersection -- 2.3 Security -- 3 GDPR: Personal Data -- 3.1 Absolute Approach -- 3.2 Relative Approach -- 3.3 Risk-Based Approach -- 3.4 Conclusion -- 4 GDPR: Data Protection by Design -- 4.1 Article 25 -- 4.2 Privacy Engineering -- 4.2.1 Privacy-Enhancing Technologies -- 4.3 EDPB Guidelines -- 4.4 Conclusion -- 5 MPC in the GDPR -- 5.1 Related Work -- 5.2 Test -- 5.2.1 Absolute vs. Relative -- 5.2.2 Input Data -- 5.2.3 Output Data -- 5.2.4 Data Minimization --

5.3 Security Model and Trust Assumption -- 5.3.1 GDPR Avoidance -- 5.3.2 Data Protection by Design -- 6 Scenarios -- 6.1 Private Set Intersection -- 6.1.1 Solution 1 -- 6.1.2 Solution 2 -- 6.1.3 Solution 3 -- 6.2 Outsourcing -- 6.2.1 Solution -- 6.2.2 Variant -- 7 Conclusion -- References -- 3 A Critique of the Google Apple Exposure Notification (GAEN) Framework.
1 Introduction -- 2 How Contact Tracing and Exposure Notification Works -- 3 The GAEN Framework -- 4 How the GAEN Framework Differs from a Purely App-Based Approach -- 5 A Critique of the GAEN Framework -- 5.1 GAEN Creates a Dormant Mass Surveillance Tool -- 5.2 Google and Apple Control the Exposure Notification Microdata -- 5.3 Distributed Can Be Made Centralised -- 5.4 Google and Apple Dictate How Contact Tracing Works -- 5.5 Function Creep -- 6 Conclusion -- References -- Part II Implications of Regulatory Framework in the European Union -- 4 Global Data Processing Identifiers and Registry (DP-ID) -- 1 Introduction -- 2 Global Data Processing Identifier Registry Concept -- 3 Facilitating GDPR Compliance -- 3.1 Obligation to Inform Art. 12, 13, 14 -- 3.2 Data Protection by Design and Default Art. 25 -- 4 Data Processing-Identified Requirements -- 5 DP-ID Implementation -- 6 Data Processing Identifier Format -- 7 Enabling Data Processing Mapping -- 8 Demonstrating Integrability and Portability -- 9 Demonstrating Interoperability -- 10 Demonstrating Cross-Organization Data Protection Compliance Management -- 11 Use Cases -- 12 Conclusion and Future Work -- References -- 5 Europrivacy Paradigm Shift in Certification Models for Privacy and Data Protection Compliance -- 1 Introduction -- 1.1 Europrivacy Genesis -- 1.2 Purpose and Scope of the Chapter -- 2 GDPR Certification -- 3 Certification Scheme Model Dilemma -- 3.1 Partial Certification Schemes Limits -- 3.2 Universal Certification Schemes Limits -- 3.3 Specialised Certification Schemes Limits -- 4 The Europrivacy Hybrid Model -- 5 Supporting Multi-jurisdictional Requirements -- 6 Addressing a Fast-Changing Normative Environment -- 7 Reducing the Risk of Subjectivity in Certification Processes -- 8 Conclusion and Future Work -- References.
Part III What is Beyond Brussels? International Norms and Their Interactions with the EU -- 6 Untying the Gordian Knot: Legally Compliant Sound Data Collection and Processing for TTS Systems in China -- 1 Introduction -- 2 Sample Project Description -- 2.1 Project Frame and Objectives -- 2.2 Focus on Data Collection and Processing -- 3 Legal Impacts on the Collection of Data -- 3.1 Legal Basis for Transnational Research -- 3.2 Applicability of GDPR and PIPL -- 3.3 Addressees of the Legal Provisions -- 3.4 Data Processing in the EU and China -- 3.5 Data Minimization, Anonymization, and Pseudonymization -- 3.6 Retention or Deletion Period -- 3.7 Data Transmission from China to the EU -- 3.8 Data Implementation -- 3.9 Formalities -- 3.10 Supervisory Authorities -- 4 Final Comparison -- 5 Conclusion -- References -- 7 Regulating Cross-Border Data Flow Between EU and India Using Digital Trade Agreement: An Explorative Analysis -- 1 Introduction -- 2 Regulatory Landscape of Cross-Border Data Transfer -- 2.1 Current Regulatory Landscape for Cross-Border Data Transfer in the EU -- 2.2 Current Regulatory Landscape for Cross-Border Data Transfer in India -- 3 Regulation Acting as Trade Barrier -- 3.1 GDPR and Its ``Brussels Effect''-Limitation on Cross-Border Data Flow and Challenges of Implementation -- 3.2 India and Its Data Localization Measure-Protectionist Measures and Challenges to Digital Trade -- 3.3 Analyzing Restrictive Data Transfer Mechanisms Acting as a Barrier Under Trade Law-GATS -- 3.3.1 GATS and Its Relevance to Cross-Border Data Flows -- 3.3.2 Possibility of Data Protection Laws of

EU and India Being in Contravention of GATS -- 4 Need for Harmonization -- 4.1 Free-Trade Agreements as an Alternative? -- 4.2 Analyzing Proposed EU Horizontal Provisions -- 5 Conclusion and Proposed Way Forward -- References.
8 When Regulatory Power and Industrial Ambitions Collide: The "Brussels Effect," Lead Markets, and the GDPR -- 1 Introduction -- 2 The "Brussels Effect" and Regulation-Induced Lead Markets -- 2.1 "Unilateral Regulatory Globalization": The "Brussels Effect" -- 2.2 Regulation-Induced Lead Markets -- 3 The GDPR and "Privacy Tech" -- 3.1 The GDPR: Setting Rules for Foreign Technology Companies -- 3.2 Regulatory Diffusion -- 3.3 Compliance Tools: "Privacy Tech" -- 4 Creating Lead Markets Abroad: The GDPR and the Development of a "Privacy Tech" Market and Industry -- 4.1 Research Strategy -- 4.2 Industry Growth -- 4.3 Geographical Distribution of Privacy Tech Firms -- 4.4 Explaining the Privacy Tech Industry's Evolution -- 5 Conclusion: Regulation and the Preconditions for the Emergence of Lead Markets -- References -- Part IV The Ethics of Privacy and Sociotechnical Systems -- 9 Nobody Wants My Stuff and It Is Just DNA Data, Why Should I Be Worried -- 1 Introduction -- 2 Background and Related Work -- 2.1 Public Genealogy Database: GEDmatch -- 2.2 Genetic Data Sharing Risks -- 2.3 Users' Motivation and Privacy Perception -- 3 Methodology -- 3.1 Recruitment and Demographics -- 3.2 Method and Analysis -- 4 Results -- 4.1 Pre-introduction of DNA Testing: Non-experienced Group Only -- 4.1.1 Foreknowledge about DNA Testing and Procedure -- 4.1.2 Expected Benefits and Concerns -- 4.2 Post-introduction of DNA Testing: Non-experienced Group -- 4.2.1 Interest and Motivations -- 4.2.2 No Interest and Concerns -- 4.3 Users' Experience: Experienced Group Only -- 4.3.1 Background -- 4.3.2 Concerns and Benefits After Taking Test -- 4.4 Post GEDmatch Demo -- 4.4.1 Benefits and Concerns -- 4.4.2 Expected use of DNA Data -- 4.4.3 Expected Data Access and Data Handling -- 4.4.4 Opt-in or Opt-out -- 4.5 DTC-GT VS GEDmatch -- 4.6 Scenarios: DNA Data Sharing. 4.6.1 Subpoenas and Sharing: Law Enforcement -- 4.6.2 Perceptions about Sharing Data in Health Research -- 4.6.3 Hereditary Diseases -- 4.6.4 DNA Data Access by Insurance Company -- 4.7 Scenarios Effects -- 4.7.1 Helplessness and Resignation -- 4.7.2 Fear and Attitude Change -- 4.7.3 Regret and Realization -- 4.7.4 Defensive and Low Expectation of Privacy -- 4.7.5 Consent and Victimize -- 4.8 Lack of Knowledge -- 4.9 Race and Nation: DNA Data Sharing -- 4.10 Future Expectation DNA Sharing/ Future Motivation -- 4.11 Users' Suggestions (Privacy Preserving) -- 5 Discussion -- 5.1 Privacy Perceptions -- 5.2 Privacy Trade-off -- 5.3 Attitude Differences -- 5.4 Limitations and Future Work -- 6 Conclusion -- References -- 10 Unwinding a Legal and Ethical Ariadne's Thread Out of the Twitter Scraping Maze -- 1 Introduction -- 2 Methodology and Research Questions -- 3 Research Scenario: Dark Patterns, Twitter, and Accountability -- 4 Protecting Users' Data and Identity -- 4.1 Personal Data in Social Media Research -- 4.2 Confidentiality -- 4.2.1 Anonymization and Pseudonymization -- 4.2.2 Encryption, Secure Authentication, and Access Control -- 4.3 Purpose Limitation -- 4.4 Data Minimization -- 4.5 Storage Limitation -- 4.6 Legal Basis -- 4.7 Transparency -- 4.8 Data Subjects' Rights -- 5 Ethics of Using Social Media Data for Research Purposes -- 5.1 Respect for the Autonomy, Privacy, and Dignity -- 5.1.1 Public vs. Private Information -- 5.1.2 Anonymity and Confidentiality -- 5.1.3 Informed Consent and Opt-out of Unwitting Participants -- 5.2 Scientific Integrity -- 5.2.1 Data Quality -- 5.2.2 Minors -- 5.3 Social Responsibility -- 5.3.1 Reputation Damage -- 5.3.2 Dual Use -- 5.3.3 Risks for Researchers -- 5.4 Maximize Benefits and Minimize Harm --

6 Discussion -- 6.1 The Question of Time and Expertise -- 6.2 The Question of Motivation -- 6.3 Incentives.
7 Limitations and Future Work.