Online Library CyberlawSA The Law Of The Internet In South Africa

2GIBWA - OSBORN MIGUEL

Social Media and Electronic Commerce Law investigates the challenges facing legal practitioners and commercial parties in this dynamic field.
Social media enables instant access to individual self-expression and the sharing of information. Social media issues are boundless, permeating distinct legal disciplines. The law has struggled to adapt and for good reason: how does the law regulate this medium over the public/private law divide? This book engages with the legal implications of social media from public and private law perspectives and outlines how the law, in various legal sub-disciplines and with varying success, has endeavoured to adapt existing tools to social media.
Nicholas Johnson and eight law students in the University of Iowa Cyberspace Law Seminar, Spring 2009, investigate everything from property rights in virtual worlds to domestic cyber attacks to K-12 students' rights with their online, off-campus speech.
Information Technology Law takes a unique socio-legal approach to examining the interaction between the law and other elements of the information society. Murray discusses relevant issues such as governance, free expression, and crime with enthusiasm, and looks forward to future challenges presented by developing technologies.

Modern business leaders need knowledge

and agility to navigate the ever-evolving legal world of e-commerce, and the third edition of CYBERLAW: TEXT & CASES, 3e, International Edition gives them both. Delivered in an entrepreneurial style, the text takes students through the complete business lifecycle—from idea to operation to dissolution—while examining the legal, managerial, and ethical issues affecting technology at each stage. Excerpted cases thoroughly explain the law in every chapter, while a running case about Google enlightens students with the real-world legal implications of running a technology company today.

The second edition of Kerrs popular computer crimes text reflects the many new caselaw and statutory developments since the publication of the first edition in 2006. It also adds a new section on encryption that covers both Fourth Amendment and Fifth Amendment issues raised by its use to conceal criminal activity. Computer crime law will be an essential area for tomorrow's criminal law practitioners, and this book offers an engaging and user-friendly introduction to the field. It is part traditional casebook, part treatise: It both straightforwardly explains the law and presents many exciting and new questions of law that courts are only now beginning to consider. The book reflects the author's practice experience, as well: Orin Kerr was a computer crime prosecutor at the Justice Department for three years, and the book combines theoretical insights with practical tips for working with actual cases. No advanced knowledge of computers and the Internet is required or assumed This book covers every aspect of crime in the digital age. Topics range from Internet surveillance law and the Fourth Amendment to computer hacking laws and international computer crimes. More and more crimes involve digital evidence, and computer crime law will be an essential area for tomorrow's criminal law practitioners. Many U.S. Attorney's Offices have started computer crime units, as have many state Attorney General offices, and any student with a background in this emerging area of law will have a leg up on the competition. This is the first law school book dedicated entirely to computer crime law. The materials are authored entirely by Orin Kerr, a new star in the area of criminal law and Internet law who has recently published articles in the Harvard Law Review, Columbia Law Review, NYU Law Review, and Michigan Law Review. The book is filled with ideas for future scholarship, including hundreds of important questions that have never been addressed in the scholarly literature. The book reflects the author's practice experience, as well: Kerr was a computer crime prosecutor at the Justice Department for three years, and the book combines theoretical insights with practical tips for working with actual cases. Students will find it easy and fun to read, and professors will find it an angaging introduction to a new world of scholarly ideas. The book is ideally suited either for a 2-credit seminar or a 3-credit course, and should appeal both to criminal law professors and those interested in cyberlaw or law and technology. No advanced knowledge of computers and the Internet is required or assumed.

The text is designed as a basic course in the legal aspects of Internet law (cyberlaw) to be taken by undergraduate and graduate students in diverse disciplines. There are no prerequisites of extensive prior legal knowledge but rather assumes only a very basic knowledge of general legal principles. The text is comprehensive and covers all of the generally recognized major areas of the subject matter. Among the subjects covered is a basic understanding of the Internet, jurisdiction, contracts, torts, crimes, intellectual property in considerable detail, privacy, antitrust, securities, and the taxation of Internet sales. The text is broad enough to be used in a law school curriculum.

Traditional Cyberlaw textbooks may not cover all you need to know. Only CYBERLAW AND E-COMMERCE REGULATION: AN ENTREPRENEURIAL APPROACH begins with the fundamentals of cyber law and e-commerce regulation in a global business context, then shows you how to make them work in your business. Whether you're an undergrad or an MBA student, this is the Cyberlaw textbook that gives you the edge in both class and the real world.

This edition of Cyberlaw@SA was written by 15 practicing experts from the legal, academic and accounting professions.

This text offers comprehensive coverage of cyberlaw and related topics using an accessible writing style, up-to-date coverage, and an entrepreneurial-process orientation and will fulfill the needs of future professional business managers for whom startups, the Internet, and innovation have continuing and increasing importance. Widely expected to become a foundational text for experiential business law courses, Cyberlaw will help prepare students for the fundamental legal challenges of startups as well as of small- and medium-sized enterprises. By following the progression of a business from idea to formation and financing to operations (including asset development and acquisition) to hiring and, finally, to the exit phase, future managers will gain insights into the kinds of decisions managers must make at every step. Students will become engaged in the topic through case analyses, examples, ethical and international perspectives, carefully constructed pedagogy, and other features, such as practice pointers, Twitter thread stories, and more. Features: The text organization observes the chronological pattern followed by a startup/entrepreneur, providing a cohesive guide to the build-out of a business. Traditional cyberlaw topics are given comprehensive coverage but always in a business context. Cutting-edge and seminal cyberlaw cases are carefully selected and edited for readability and clarity. Important topic content includes chapters on IP; social media; data privacy; and government regulation. Other up-to--date coverage includes promoting inventiveness and innovation; data security; new venture planning, fiduciary duties, and crowdfunding ; and malware, data breaches, and criminal procedure. Each chapter contains a feature focused on cyberlaw issues and dilemmas, using Twitter as a case study. Wherever appropriate and relevant, international perspectives and ethical organizational behavior are integrated into the discussion. Pedagogical features, placed strategically throughout the text, include concept summaries, case questions, exhibits and tables, hypothetical ventures to illustrate points, and dynamic end-of-chapter features such as chapter summaries, manager s checklists, key terms, short case problems or questions, and web resources. Learning objectives align with AACSB standards and Bloom s Taxonomy for assessment purposes. Cutting-edge cyberlaw cases discussed include People v. Marquan M (cyber-bullying, 2014) and Riley v. California (cell phone searches, 2014).

In today’s litigious business world, cyber-related matters could land you in court. As a computer security professional, you are protecting your data, but are you protecting your company? While you know industry standards and regulations, you may not be a legal expert. Fortunately, in a few hours of reading, rather than months of classroom study, Tari Schreider's Cybersecurity Law, Standards and Regulations (2nd Edition), lets you integrate legal issues into your security program. Tari Schreider, a board-certified information security practitioner with a criminal justice administration background, has written a much-needed book that bridges the gap between cybersecurity programs and cybersecurity law. He says, "My nearly 40 years in the fields of cybersecurity, risk management, and disaster recovery have taught me some immutable truths. One of these truths is that failure to consider the law when developing a cybersecurity program results in a protective façade or false sense of security." In a friendly style, offering real-world business examples from his own experience supported by a wealth of court cases, Schreider covers the range of practical information you will need as you explore – and prepare to apply – cybersecurity law. His practical, easy-to-understand explanations help you to: Understand your legal duty to act reasonably and responsibly to protect assets and information. Identify which cybersecurity laws have the potential to impact your cybersecurity program. Upgrade cybersecurity policies to comply with state, federal, and regulatory statutes. Communicate effectively about cybersecurity law with corporate legal department and counsel. Understand the implications of emerging legislation for your cybersecurity program. Know how to avoid losing a cybersecurity court case on procedure – and develop strategies to handle a dispute out of court. Develop an international view of cybersecurity and data privacy – and international legal frameworks. Schreider takes you beyond security standards and regulatory controls to ensure that your current or future cybersecurity program complies with all laws and legal jurisdictions. Hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. This book needs to be required reading before your next discussion with your corporate legal department. This new edition responds to the rapid changes in the cybersecurity industry, threat landscape and providers. It addresses the increasing risk of zero-day attacks, growth of state-sponsored adversaries and consolidation of cybersecurity products and services in addition to the substantial updates of standards, source links and cybersecurity products.

Rights of robots, a closer collaboration between law and the health sector, the relation between justice and development - these are some of the topics covered in The Law of the Future and the Future of Law: Volume II. The central question is: how will law evolve in the coming years? This book gives you a rich array of visions on current legal trends. The readable think pieces offer indications of law's cutting edge. The book brings new material that is not available in the first volume of The Law of the Future and the Future of Law, published in June 2011. Among the authors in this volume are William Twining (Emeritus Quain Professor of Jurisprudence, University College London), David Eagleman (Director, Initiative on Neuroscience and Law), Hassane Cisse (Deputy General Counsel, The World Bank), Gabrielle Marceau (Counsellor, World Trade Organisation), Benjamin

Odoki (Chief Justice, Republic of Uganda), Martijn W. Scheltema (Attorney at law, Pels Rijcken and Droogleever Fortuijn), Austin Onuoha (Founder, The Africa Centre for Corporate Responsibility), Lokke Moerel (Partner, De Brauw Blackstone Westbroek), S.I. Strong (Senior Fellow, Center for the Study of Dispute Resolution), Jan M. Smits (Chair of European Private Law, Maastricht University).

CyberLaw provides a comprehensive guide to legal issues which have arisen as a result of the growth of the Internet and World Wide Web. As well as discussing each topic in detail, the book includes extensive coverage of the relevant cases and their implications for the future. The book covers a wide range of legal issues, including copyright and trademark issues, defamation, privacy, liability, electronic contracts, taxes, and ethics. A comprehensive history of the significant legal events is also included.

The adoption of electronic commercial transactions has facilitated cross-border trade and business, but the complexity of determining the place of business and other connecting factors in cyberspace has challenged existing private international law. This comparison of the rules of internet jurisdiction and choice of law as well as online dispute resolution (ODR) covers both B2B and B2C contracts in the EU, USA and China. It highlights the achievement of the Rome I Regulation in the EU, evaluates the merits of the Hague Convention on Choice of Court Agreement at the international level and gives an insight into the current developments in CIDIP. The in-depth research allows for solutions to be proposed relating to the problems of the legal uncertainty of internet conflict of law and the validity and enforceability of ODR agreements and decisions.

With the expansion of the internet and the world wide web, comes the very real potential for loss of control of intellectual property of all kinds, whether text or graphic, whether copyrighted or trademarked. In addition, business and financial issues, as well as social issues such as privacy and obscenity are also covered. Through the use of case studies and analysis, Cyberlaw presents a wide variety of legal and ethical issues relating to internet law and intellectual property protection.

The internet has transformed the world of work in ways that could not have been imagined even a decade ago. Almost anything we do is intimately connected to information creation, retrieval, processing or management. Regardless of perceived ethical or enforcement limitations, laws have become increasingly significant, from the protection of copyright to the enforcement of online contracts. Cyberlaw@SA III: the law of the internet in South Africa provides specialist insight into the myriad legal issues generated by the convergence of tecnologies and the rise of the internet. The third edition of Cyberlaw@SA is a comprehensive and updated version of the original text and covers a wide range of topics and new areas of discussion in the field of cyberlaw, including going more in-depth on issues of e-taxation, cybercrime laws, and the processing of e-evidence and its value in civil and criminal proceedings.

Written specifically for legal practitioners and students, this book examines the concerns, laws and regulations involved in Electronic Commerce. In just a few years, commerce via the World Wide Web and other online platforms has boomed, and a new field of legal theory and practice has emerged. Legislation has been enacted to keep pace with commercial realities, cyber-criminals and unforeseen social consequences, but the ever-evolving nature of new technologies has challenged the capacity of the courts to respond effectively. This book addresses the legal issues relating to the introduction and adoption of various forms of electronic commerce. From intellectual property, to issues of security and privacy, Alan Davidson looks at the practical changes for lawyers and commercial parties whilst providing a rationale for the underlying legal theory.

This accessible, reader-friendly handbook will be an invaluable resource for authors, agents, and editors in navigating the legal landscape of the contemporary publishing industry. Drawing on a wealth of experience in legal scholarship and publishing, Jacqueline D. Lipton provides a useful legal guide for writers whatever their levels of expertise or categories of work (fiction, nonfiction, or academic). Through case studies and hypothetical examples, Law and Authors addresses issues of copyright law, including explanations of fair use and the public domain; trademark and branding concerns for those embarking on a publishing career; laws that impact the ways that authors might use social media and marketing promotions; and privacy and defamation questions that writers may face. Although the book focuses on American law, it highlights key areas where laws in other countries differ from those in the United States. Law and Authors will prepare every writer for the inevitable and the unexpected.

This law school casebook starts from the premise that cyberlaw is not simply a set of legal rules governing online interaction, but a lens through which to re-examine general problems of policy, jurisprudence, and culture. The book goes beyond simply plugging Internet-related cases into a series of doctrinal categories, instead emphasizing conceptual issues that extend across the spectrum of cyberspace legal dilemmas. While the book addresses all of the "traditional" subject matter areas of cyberlaw, it asks readers to consider both how traditional legal doctrines can be applied to cyberspace conduct, and how the special problems encountered in that application can teach us something about those traditional legal doctrines. The fifth edition has been updated, shortened, and reconceptualized to make the book even more effective as a teaching tool and to illuminate new debates at the heart of this evolving field. The book groups the material into units addressing the who, how, and what of governance/regulation--fundamental questions that pertain to any legal system, in cyberspace or elsewhere. The fifth edition also includes updated treatment throughout, as well as a more stream-lined approach that should make an already effective casebook even more unified and teachable.

The rapid increase in Internet usage over the past several decades has led to the development of new and essential areas of legislation and legal study. Jacqueline Lipton takes on the thorny question of how to define the field that has come to be known

Presenting an emerging area of law, this book explores the legal doctrines and principles that apply to the operation and development of computer technology and the Internet. It discusses the rapid legislative and judicial responses, demanded by the creation of the new technology, to resolve legal problems of the emerging technology, covering: jurisdiction, constitutional issues, e-business, property rights, and cybercrime. For individuals interested in an introduction to constitutional and business law, as well as intellectual property.

Cyber Law is a comprehensive guide for navigating all legal aspects of the Internet. This book is a crucial asset for online businesses and entrepreneurs. Whether you're doing business online as a company or a consumer, you need to understand your rights. Trout successfully places legal complexities into digital perspective with his latest book. -- Chris Pirillo - Founder of Lockergnome CyberLaw is a must-read for anyone doing business-or just chatting or socializing - on the Internet. Without us realizing it, more and more laws are being passed each year, laws and restrictions that significantly increase the likelihood that you're skirting, or even breaking some laws when you post that restaurant review, write about the bad date you had last week, or complain about a previous employer. Your choices are easy: read CyberLaw or suffer the potential consequences. -- Dave Taylor, Entrepreneur and Strategic Business Consultant, Intuitive.com Brett Trout has the bottom-line, honest, insightful, straightfowardest, most clear-headed take on intellectual property issues you could want. He's your way out of the maze. -- John Shirley, scriptwriter and author

The world of Internet law is constantly changing and is difficult to follow, even for those for whom doing so is a full-time job. This updated, everything-you-need-to--know reference removes the uncertainty. Internet and the Law: Technology, Society, and Compromises, Second Edition is the go-to source for anyone who needs clear explanations of complex legal concepts related to online practices and content. This wide-ranging, alphabetical reference explores diverse areas of law, including territorial jurisdiction and taxation, that are relevant to or affected by advances in information technology and the rise of the Internet. Particular emphasis is placed on intellectual property law and laws regarding freedom of expression. The Internet, as this book shows, raises questions not only about how to protect intellectual creations, but about what should be protected. Entries also discuss how the Web has brought First Amendment rights and free expression into question as society grapples with attempts to control "leaks" and to restrict content such as pornography, spam, defamation, and criminal speech. Explains complex legal and technical concepts clearly and understandably through entries that range from 500 to 5,000 words Covers a wide range of topics, including censorship, copyright, domain name disputes, file-sharing, hacking, patents, spam, malware, international law, tax issues, trademarks, and viruses Features an introductory guide to the U.S. legal system, including how to find, read, and understand sources of law Includes cases, statutes, and international treaties relevant to the law of information technology and the Internet

Modern business leaders need knowledge and agility to navigate the ever-evolving legal world of e-commerce, and the third edition of CYBERLAW: TEXT & CASES gives them both. Delivered in an entrepreneurial style, the text takes students through the complete business lifecycle from idea to operation to dissolution while examining the legal, managerial, and ethical issues affecting technology at each stage. Excerpted cases thoroughly explain the law in every chapter, while a running case about Google enlightens students with the real-world legal implications of running a technology company today. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

In light of the overwhelming impact of technology on modern life, this thought-provoking book critically analyses the interaction of innovation, technology and corporate law. It highlights the impact of artificial intelligence and distributed ledgers on corporate governance and form, examining the extent to which technology may enhance or displace conventional theories and practices concerning corporate governance and regulation. Expert contributors from multiple jurisdictions identify themes and challenges that transcend national boundaries and confront the international community as a whole.

A primer on legal issues relating to cyberspace, this textbook introduces business, policy and ethical considerations raised by our use of information technology. With a focus on the most significant issues impacting internet users and businesses in the United States of America, the book provides coverage of key topics such as social media, online privacy, artificial intelligence and cybercrime as well as emerging themes such as doxing, ransomware, revenge porn, data-mining, e-sports and fake news. The authors, experienced in journalism, technology and legal practice, provide readers with expert insights into the nuts and bolts of cyber law. Cyber Law and Ethics: Regulation of the Connected World provides a practical presentation of legal principles, and is essential reading for non-specialist students dealing with the intersection of the internet and the law.

This compact, highly engaging book examines the international legal regulation of both the conduct of States among themselves and conduct towards individuals, in relation to the use of cyberspace. Chapters introduce the perspectives of various stakeholders and the challenges for international law. The author discusses State responsibility and key cyberspace rights issues, and takes a detailed look at cyber warfare, espionage, crime and terrorism. The work also covers the situation of non-State actors and quasi-State actors (such as IS, or ISIS, or ISIL) and concludes with a consideration of future prospects for the international law of cyberspace. Readers may explore international rules in the areas of jurisdiction of States in cyberspace, responsibility of States for cyber activities, human rights in the cyber world, permissible responses to cyber attacks, and more. Other topics addressed include the rules of engagement in cyber warfare, suppression of cyber crimes, permissible limits of cyber espionage, and suppression of cyber-related terrorism. Chapters feature explanations of case law from various jurisdictions, against the background of real-life cyber-related incidents across the globe. Written by an internationally recognized practitioner in the field, the book objectively guides readers through on-going debates on cyber-related issues against the background of international law. This book is very accessibly written and is an enlightening read. It will appeal to a wide audience, from international lawyers to students of international law, military strategists, law enforcement officers, policy makers and the lay person.

Featuring the most current exploration of cyberlaw, CYBERLAW helps students understand the legal and policy issues associated with the Internet. Tackling a full range of legal topics, it includes discussion of jurisdiction, intellectual property, contracts, taxation, torts, computer crimes, online speech, defamation and privacy. Chapters include recent, relevant cases, discussion questions and exercises at the end of each chapter. Using a consistent voice and clear explanations, the author covers the latest developments in cyberlaw–from cases to legislation to regulations.

This book introduces law to computer scientists and other folk. Computer scientists develop, protect, and maintain computing systems in the broad sense of that term, whether hardware (a smartphone, a driverless car, a smart energy meter, a laptop, or a server), software (a program, an application programming interface or API, a module, code), or data (captured via cookies, sensors, APIs, or manual input). Computer scientists may be focused on security (e.g. cryptography), or on embedded systems (e.g. the Internet of Things), or on data science (e.g. machine learning). They may be closer to mathematicians or to electrical or electronic engineers, or they may work on the cusp of hardware and software, mathematical proofs and empirical testing. This book conveys the internal logic of legal practice, offering a hands-on introduction to the relevant domains of law, while firmly grounded in legal theory. It bridges the gap between two scientific practices, by presenting a coherent picture of the grammar and vocabulary of law and the rule of law, geared to those with no wish to become lawyers but nevertheless required to consider the salience of legal rights and obligations. Simultaneously, this book will help lawyers to review their own trade. It is a volume on law in an onlife world, presenting a grounded argument of what law does (speech act theory), how it emerged in the context of printed text (philosophy of technology), and how it confronts its new, data-driven environment. Book jacket.

This fresh and insightful Research Handbook delivers global perspectives on information law and governance, delving into principles of information law in the areas of trade secrecy, privacy, data protection and cybersecurity.

This book provides a comprehensive guide to legal issues which have arisen as a result of the growth of the internet and the worldwide web. As well as discussing each topic in detail, Jonathan Rosenoer includes extensive coverage of the relevant cases and their implications for the future. Topics covered include: copyright and trademark issues, defamation, privacy, liability, electronic contracts, tax issues, and ethics. A potted history of the significant legal events is included which runs from the founding of the Electronic Frontier Foundation to the 1996 Telecommunications Act. About the author:Jonathan Rosenoer has been general counsel for the Haft Corporation, Executive Editor for Lexis Counsel Connect, and is best known for his CyberLaw column which has a distribution list of over four million.

Legal environment is changing in the 21st century, and Cyberlaw and E-Commerce has been created to address the legal issues surrounding the Internet and Electronic Commerce in light of technological changes that have radically altered the legal realities that confront business managers. The text is designed, among other things, to prepare students to manage intellectual property. Cyberlaw and E-commerce is intended for the Legal Environment of Business course for faculty interested in additional material on e-commerce. It could also fit into courses entitled Computers, Law and Society, Internet Law, Intellectual Property Law, or Issues in E-Commerce.

There's a common belief that cyberspace cannot be regulated-that it is, in its very essence, immune from the government's (or anyone else's) control. Code, first published in 2000, argues that this belief is wrong. It is not in the nature of cyberspace to be unregulable; cyberspace has no "nature." It only has code-the software and hardware that make cyberspace what it is. That code can create a place of freedom-as the original architecture of the Net did-or a place of oppressive control. Under the influence of commerce, cyberspace is becoming a highly regulable space, where behavior is much more tightly controlled than in real space. But that's not inevitable either. We can-we must-choose what kind of cyberspace we want and what freedoms we will guarantee. These choices are all about architecture: about what kind of code will govern cyberspace, and who will control it. In this realm, code is the most significant form of law, and it is up to lawyers, policymakers, and especially citizens to decide what values that code embodies. Since its original publication, this seminal book has earned the status of a minor classic. This second edition, or Version 2.0, has been prepared through the author's wiki, a web site that allows readers to edit the text, making this the first reader-edited revision of a popular book.

Examines cyberlaw topics such as cybercrime and risk management, electronic trading systems of securities, digital currency regulation, jurisdiction and consumer protection in cross-border markets, and international bank transfers.