Cyberspace Law Cases And Materials Casebook Series

Intellectual Property and the InternetProblems and Materials on Consumer LawMass Media LawThe Twenty-Six Words That Created the InternetThe Law of Armed ConflictInternet Law & PolicyCyberethics: Morality and Law in CyberspaceCaptive AudienceCyberspace, Cybersecurity, and CybercrimeThe Law of Electronic CommerceCyberspace LawInternet LawInternet LawCodeGlobal Internet Law in a NutshellComputer Crime LawLegal EthicsTechnical, Business, and Legal Dimensions of Protecting Children from Pornography on the InternetPublic International Law of CyberspaceTallinn Manual on the International Law Applicable to Cyber WarfarePrinciples of CybercrimeCyberlawThe Handbook of Internet StudiesCyberlawCyber PrivacyInternet Co-RegulationSan Diego International Law JournalComputers and the LawInternet PredatorsInternet LawTeaching Intellectual Property LawGovernance in "Cyberspace":Access and Public Interest in Global CommunicationsInternet Law in ChinaThe EBay Seller's Tax and Legal Answer BookCybercrime and Digital ForensicsCyberlawCybersecurity LawDigital CopyrightLaw and AuthorsThe International Dimensions of Cyberspace Law

Intellectual Property and the Internet

A comprehensive, structured, and up-to-date introduction to the law governing the dissemination of information in a computer-mediated world in China, Internet Law in China stresses the practical applications of the law that are encountered by all individuals and organizations in Chinese cyberspace, but always in the light of theoretical underpinnings. Among the overarching topics treated in the Chinese context are the following: intellectual property protection in cyberspace; privacy of communication and data privacy; electronic contract forming and electronic signature; personal, domestic and international jurisdiction; and free expression in cyberspace. This book is particularly valuable to legal, business, and communication professionals, academics, and students concerned with the regulation of the Internet and related activities in China. It is the first book to focus solely on Chinese Internet law. The first book to systematically explore the legal doctrines and principles that apply to the Internet and related activities in China Broad coverage: from Internet speech to proprietary interests, privacy issues, electronic contracts, and jurisdiction Original comparative analysis of China’s Internet regulation practice in the global context

Problems and Materials on Consumer Law

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 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 exquisitely oppressive control.If we miss this point, then we will miss how cyberspace is changing. Under the influence of commerce, cyberpsace is becoming a highly regulable space, where our 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.

Mass Media Law

Global view of the fundamental legal issues raised by the advent of the Internet.

The Twenty-Six Words That Created the Internet

A comprehensive doctrinal analysis of cybercrime laws in four major common law jurisdictions: Australia, Canada, the UK and the USA.

The Law of Armed Conflict

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.

Internet Law & Policy

Computers and the Law provides readers with an introduction to the legal issues associated with computing – particularly in the massively networked context of the Internet. Assuming no previous knowledge of the law or any special knowledge of programming or computer science, this textbook offers undergraduates of all disciplines and professionals in the computing industry an understanding of basic legal principles and an awareness of the peculiarities associated with legal issues in cyberspace. This is not a law school casebook, but rather a variety of carefully chosen, relevant cases presented in redacted form. The full cases are available on

an ancillary Web site. The pervasiveness of computing in modern society has generated numerous legal ambiguities. This book introduces readers to the fundamental workings of the law in physical space and suggests the opportunity to create new types of laws with nontraditional goals.

Cyberethics: Morality and Law in Cyberspace

Newly revised and expanded, The Law of Armed Conflict, 2nd edition introduces law students and undergraduates to the law of war in an age of terrorism. What law of armed conflict (LOAC), or its civilian counterpart, international humanitarian law (IHL), applies in a particular armed conflict? Are terrorists legally bound by that law? What constitutes a war crime? What (or who) is a lawful target and how are targeting decisions made? What are 'rules of engagement' and who formulates them? How can an autonomous weapon system be bound by the law of armed conflict? Why were the Guantánamo military commissions a failure? This book takes students through these LOACIHL questions and more, employing real-world examples and legal opinions from the US and abroad. From Nuremberg to 9/11, from courts-martial to the US Supreme Court, from the nineteenth century to the twenty-first, the law of war is explained, interpreted, and applied.

Captive Audience

From commerce to speech, internet companies intermediate our daily activities. At the same time, internet companies are remaking our existence. Facebook has been blamed for facilitating Russian election interference, yet credited for sparking the Jasmine Revolutions that felled dictatorships across North Africa. What laws govern the borderless domains of cyberspace? Is the internet a free speech zone protected by the U.S. Constitution's First Amendment, or does it bend to hate speech or political speech regulations from abroad? Can copyright law survive the worldwide copying machine of the internet? Is privacy dead when corporations know where you are and what you are doing nearly 24/7? Are there any limits on electronic surveillance by the government? This casebook examines the evolving law regulating internet enterprises.

Cyberspace, Cybersecurity, and Cybercrime

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.

The Law of Electronic Commerce

Even if you think of your eBay selling as a hobby rather than a business, the fact is that if you're making money, you are in business, and therefore subject to the same taxes and regulations as other real world retail businesses. Simply written and packed with stories of actual eBay sellers, The eBay Seller's Tax and Legal Answer Book takes you through the most common eBay transactions, pointing out all the legal and tax issues you're likely to encounter. Complete with sample contracts, forms, checklists, and disclaimers, this is a book no eBay seller should be without.

Cyberspace Law

Professor Litman's work stands out as well-researched, doctrinally solid, and always piercingly well-written.-JANE GINSBURG, Morton L. Janklow Professor of Literary and Artistic Property, Columbia UniversityLitman's work is distinctive in several respects: in her informed historical perspective on copyright law and its legislative policy; her remarkable ability to translate complicated copyright concepts and their implications into plain English; her willingness to study, understand, and take seriously what ordinary people think copyright law means; and her creativity in formulating alternatives to the copyright quagmire. -PAMELA

SAMUELSON, Professor of Law and Information Management; Director of the Berkeley Center for Law & Technology, University of California, BerkeleyIn 1998, copyright lobbyists succeeded in persuading Congress to enact laws greatly expanding copyright owners' control over individuals' private uses of their works. The efforts to enforce these new rights have resulted in highly publicized legal battles between established media and new upstarts.In this enlightening and well-argued book, law professor Jessica Litman questions whether copyright laws crafted by lawyers and their lobbyists really make sense for the vast majority of us. Should every interaction between ordinary consumers and copyright-protected works be restricted by law? Is it practical to enforce such laws, or expect consumers to obey them? What are the effects of such laws on the exchange of information in a free society?Litman's critique exposes the 1998 copyright law as an incoherent patchwork. She argues for reforms that reflect common sense and the way people actually behave in their daily digital interactions.This paperback edition includes an afterword that comments on recent developments, such as the end of the Napster story, the rise of peer-to-peer file sharing, the escalation of a full-fledged copyright war, the filing of lawsuits against thousands of individuals, and the June 2005 Supreme Court decision in the Grokster case.Jessica Litman (Ann Arbor, MI) is professor of law at Wayne State University and a widely recognized expert on copyright law.

Internet Law

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.

Internet Law

Written by the Director for the newly created Center for Cyberspace Law & Policy at Case Western Reserve University, the Fourth Edition of Cyberspace Law: Cases

and Materials reflects the broad knowledge and experience of a pioneer in the teaching of Cyberspace law. This was the first casebook devoted exclusively to the study of cyberspace law, and is the only one that presents it as the study of the creation, dissemination, and acquisition of human thought, creativity, and information in the digital age. Of note is the casebook's organization, which allows instructors to adapt the materials to their approaches. Features: The Supreme Court's recent decisions in J. McIntyre v Nicastro (jurisdiction), Brown v Entertainment Merchants (video games), ABC v Aereo (copyright), Bilski v Kappos (business method patents), and Riley v California (Smart phone privacy) Lower court cases including: Authors Guild v Google (Google books fair use), Lenz v Universal Music (DMCA notice), Fraley v Facebook (Misappropriation), and Verizon v FCC (net neutrality) Presentation of current Internet law as well as related policy concerns that will drive future legal analysis when new issues emerge

Code

"A casebook that takes students through the main issues of consumer law: deceptive practices, product quality, and consumer credit. It covers the Federal Interstate Land Sales Full Disclosure Act (regulating sale of vacation home land -- not mentioned in any other book on this topic), and includes "Quotes for the Attorney's Arsenal" (statements from famous cases that eloquently encapsulate specific points)"--

Global Internet Law in a Nutshell

Global Internet Law in a Nutshell surveys the historical, technological, and cultural impacts of the Internet, applying multiple academic perspectives to the path of both U.S. and foreign cyberlaw. Subsequent chapters review the latest case law and statutory developments from the United States, European Union, China, and other countries governing the Internet. Internet-related issues for jurisdiction, contracts, consumer protection, torts, privacy, cybercrimes, content regulation, and each branch of intellectual property law are summarized. This Nutshell covers the major topics taught in Internet Law, Electronic Commerce Law, and Information Technology Law classes. Rapidly evolving topics such as the Internet of Things, Driverless Cars, Artificial Intelligence, the EU's General Data Protection Regulation, and Internet-related Intellectual Property Cases are highlighted.

Computer Crime Law

This title was first published in 2003. This text is part of the "Law of Cyberspace" series, which deals with the legal aspects of the emerging information society and corresponding ethical matters. The book examines the international dimensions of cyberspace law and the timeliness of drawing up the most appropriate international standard instrument for this environment, exploring ways and means

of achieving it and defining the organization's precise role in this respect. The text presents the framework that UNESCO is helping to develop for the international community, with the participation of all the actors in cyberspace, aiming to be ethical, flexible and technologically neutral, multiform, and universal.

Legal Ethics

Revised and updated to reflect new technologies in the field, the fourth edition of this popular text takes an in-depth look at the social costs and moral problems that have emerged by the ever expanding use of the Internet, and offers up-to-date legal and philosophical examinations of these issues. It focuses heavily on content control, free speech, intellectual property, and security while delving into new areas of blogging and social networking. Case studies throughout discuss real-world events and include coverage of numerous hot topics. In the process of exploring current issues, it identifies legal disputes that will likely set the standard for future cases.Instructor Resouces:-PowerPoint Lecture Outlines

Technical, Business, and Legal Dimensions of Protecting Children from Pornography on the Internet

`Cyberspace' is the emerging invisible, intangible world of electronic information

and processes stored at multiple interconnected sites. The digital revolution leads to `convergence' (of telecommunications, computer/Internet and broadcasting) and to dynamic multimedia value chains. Deregulation and competition are major driving forces in the new interactive electronic environment. This volume contains normative proposals for `cyber'-regulation, including self-regulation, grounded on developments in the EU, US and the Far East, in international organisations (WTO, OECD, WIPO, ITU), in business fora, in NGOs, in the `Internet community' and in academic research. The multi-actor (government, business, civil society) and multi-level analysis (subsidiarity) pertains e.g. to ex-ante and ex-post access-regulation, competition, network economics (external effects, essential facilities), public interest principles (human dignity, free speech, privacy, security), development and culture, consumer protection, cryptography, domain names and copyright. Lawyers, regulators, business executives, investment bankers, diplomats, and civil society representatives need shared essentials of plurilateral `governance' to safeguard both competition and public interest objectives, at a scale congruent to `cyberspace', in the transition to an `international law of cooperation'.

Public International Law of Cyberspace

Tallinn Manual on the International Law Applicable to Cyber

Warfare

Resource added for the Paralegal program 101101.

Principles of Cybercrime

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.

Cyberlaw

¿ CLEAR & CONCISE: Tight case editing, focused questions, and topical problems direct students' attention to the most critical issues. The book covers the full sweep of the subject, but is still short enough that the core topics can be taught in a 3-credit survey course. ¿ UP-TO-DATE COVERAGE: The seventh edition features five new principal cases, along with numerous new and revised notes and questions. New cases deal with international injunctions, free speech rights to use the Internet, compelled decryption, trademarks and search engines, and algorithmic accountability. Several sections have been tightened up and older material has been cut, resulting in a streamlined reading experience. ¿ TECHNICAL AND HISTORICAL NOTES: Mini-essays throughout the book provide the essential technical background needed to make sense of computer and Internet technologies. Where modern doctrine has important historical roots (e.g., network neutrality and telecommunications regulation), the book gives the necessary context.

The Handbook of Internet Studies

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.

Cyberlaw

The second edition of the definitive guide to cybersecurity law, updated to reflect recent legal developments The revised and updated second edition of Cybersecurity Law offers an authoritative guide to the key statutes, regulations,

and court rulings that pertain to cybersecurity. Written by an experienced cybersecurity lawyer and law professor, the second edition includes new and expanded information that reflects the latest changes in laws and regulations. The book includes material on recent FTC data security consent decrees and data breach litigation. Topics covered reflect new laws, regulations, and court decisions that address financial sector cybersecurity, the law of war as applied to cyberspace, and recently updated guidance for public companies' disclosure of cybersecurity risks. This important guide: Provides a new appendix, with 15 edited opinions covering a wide range of cybersecurity-related topics, for students learning via the caselaw method Includes new sections that cover topics such as: compelled access to encrypted devices, New York's financial services cybersecurity regulations, South Carolina's insurance sector cybersecurity law, the Internet of Things, bug bounty programs, the vulnerability equities process, international enforcement of computer hacking laws, the California Consumer Privacy Act, and the European Union's Network and Information Security Directive Contains a new chapter on the critical topic of law of cyberwar Presents a comprehensive guide written by a noted expert on the topic Offers a companion Instructor-only website that features discussion questions for each chapter and suggested exam questions for each chapter Written for students and professionals of cybersecurity, cyber operations, management-oriented information technology (IT), and computer science, Cybersecurity Law, Second Edition is the up-to-date guide that covers the basic principles and the most recent information on cybersecurity laws and

regulations. JEFF KOSSEFF is Assistant Professor of Cybersecurity Law at the United States Naval Academy in Annapolis, Maryland. He was a finalist for the Pulitzer Prize, and a recipient of the George Polk Award for national reporting.

Cyber Privacy

Ten years ago, the United States stood at the forefront of the Internet revolution. With some of the fastest speeds and lowest prices in the world for high-speed Internet access, the nation was poised to be the global leader in the new knowledge-based economy. Today that global competitive advantage has all but vanished because of a series of government decisions and resulting monopolies that have allowed dozens of countries, including Japan and South Korea, to pass us in both speed and price of broadband. This steady slide backward not only deprives consumers of vital services needed in a competitive employment and business market—it also threatens the economic future of the nation. This important book by leading telecommunications policy expert Susan Crawford explores why Americans are now paying much more but getting much less when it comes to high-speed Internet access. Using the 2011 merger between Comcast and NBC Universal as a lens, Crawford examines how we have created the biggest monopoly since the breakup of Standard Oil a century ago. In the clearest terms, this book explores how telecommunications monopolies have affected the daily lives of consumers and America's global economic standing.

Internet Co-Regulation

San Diego International Law Journal

Presented from a criminal justice perspective, Cyberspace, Cybersecurity, and Cybercrime introduces students to the interdisciplinary field of cybercrime by exploring the theoretical, practical, and legal framework it operates under, along with strategies to combat it. Authors Janine Kremling and Amanda M. Sharp Parker provide a straightforward overview of cybercrime, cyberthreats, and the vulnerabilities individuals, businesses, and governments face everyday in a digital environment. Highlighting the latest empirical research findings and challenges that cybercrime and cybersecurity pose for those working in the field of criminal justice, this book exposes critical issues related to privacy, terrorism, hacktivism, the dark web, and much more. Focusing on the past, present, and future impact of cybercrime and cybersecurity, it details how criminal justice professionals can be prepared to confront the changing nature of cybercrime.

Computers and the Law

In response to a mandate from Congress in conjunction with the Protection of

Children from Sexual Predators Act of 1998, the Computer Science and Telecommunications Board (CSTB) and the Board on Children, Youth, and Families of the National Research Council (NRC) and the Institute of Medicine established the Committee to Study Tools and Strategies for Protecting Kids from Pornography and Their Applicability to Other Inappropriate Internet Content. To collect input and to disseminate useful information to the nation on this question, the committee held two public workshops. On December 13, 2000, in Washington, D.C., the committee convened a workshop to focus on nontechnical strategies that could be effective in a broad range of settings (e.g., home, school, libraries) in which young people might be online. This workshop brought together researchers, educators, policy makers, and other key stakeholders to consider and discuss these approaches and to identify some of the benefits and limitations of various nontechnical strategies. The December workshop is summarized in Nontechnical Strategies to Reduce Children's Exposure to Inappropriate Material on the Internet: Summary of a Workshop. The second workshop was held on March 7, 2001, in Redwood City, California. This second workshop focused on some of the technical, business, and legal factors that affect how one might choose to protect kids from pornography on the Internet. The present report provides, in the form of edited transcripts, the presentations at that workshop.

Internet Predators

The Handbook of Internet Studies brings together scholars from a variety of fields to explore the profound shift that has occurred in how we communicate and experience our world as we have moved from the industrial era into the age of digital media. Presents a wide range of original essays by established scholars in everything from online ethics to ways in which indigenous peoples now use the Internet Looks at the role of the internet in modern societies, and the continuing development of internet studies as an academic field Explores Internet studies through history, society, culture, and the future of online media Provides introductory frameworks to ground and orientate the student, while also providing more experienced scholars with a convenient and comprehensive overview of the latest trends and critical directions in the many areas of Internet research

Internet Law

This law school text is an in-depth survey of the emerging legal framework for the protection of intellectual property on the Internet, with particular emphasis on issues that have not yet become well known, such as protection of databases, and trademark-based disputes over domain names. It is designed to be used either in a traditional survey course in intellectual property, or as the basis for a course or seminar focusing on intellectual property in cyberspace. The authors assume familiarity with first-year legal courses, but no further specialized knowledge is required.

Teaching Intellectual Property Law

The emergence of the World Wide Web, smartphones, and Computer-Mediated Communications (CMCs) profoundly affect the way in which people interact online and offline. Individuals who engage in socially unacceptable or outright criminal acts increasingly utilize technology to connect with one another in ways that are not otherwise possible in the real world due to shame, social stigma, or risk of detection. As a consequence, there are now myriad opportunities for wrongdoing and abuse through technology. This book offers a comprehensive and integrative introduction to cybercrime. It is the first to connect the disparate literature on the various types of cybercrime, the investigation and detection of cybercrime and the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of: key theoretical and methodological perspectives, computer hacking and digital piracy, economic crime and online fraud, pornography and online sex crime, cyber-bulling and cyber-stalking, cyber-terrorism and extremism, digital forensic investigation and its legal context, cybercrime policy. This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders and a full glossary of terms. It is supplemented by a companion website that includes further students exercises and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation

and the sociology of technology.

Governance in "Cyberspace":Access and Public Interest in Global Communications

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.

Internet Law in China

“Chilling, eye-opening, and timely, Cyber Privacy makes a strong case for the urgent need to reform the laws and policies that protect our personal data. If your

reaction to that statement is to shrug your shoulders, think again. As April Falcon Doss expertly explains, data tracking is a real problem that affects every single one of us on a daily basis." —General Michael V. Hayden, USAF, Ret., former Director of CIA and NSA and former Principal Deputy Director of National Intelligence You're being tracked. Amazon, Google, Facebook, governments. No matter who we are or where we go, someone is collecting our data: to profile us, target us, assess us; to predict our behavior and analyze our attitudes; to influence the things we do and buy—even to impact our vote. If this makes you uneasy, it should. We live in an era of unprecedented data aggregation, and it's never been more difficult to navigate the trade-offs between individual privacy, personal convenience, national security, and corporate profits. Technology is evolving quickly, while laws and policies are changing slowly. You shouldn't have to be a privacy expert to understand what happens to your data. April Falcon Doss, a privacy expert and former NSA and Senate lawyer, has seen this imbalance in action. She wants to empower individuals and see policy catch up. In Cyber Privacy, Doss demystifies the digital footprints we leave in our daily lives and reveals how our data is being used—sometimes against us—by the private sector, the government, and even our employers and schools. She explains the trends in data science, technology, and the law that impact our everyday privacy. She tackles big questions: how data aggregation undermines personal autonomy, how to measure what privacy is worth, and how society can benefit from big data while managing its risks and being clear-eyed about its cost. It's high time to rethink

notions of privacy and what, if anything, limits the power of those who are constantly watching, listening, and learning about us. This book is for readers who want answers to three questions: Who has your data? Why should you care? And most important, what can you do about it?

The EBay Seller's Tax and Legal Answer Book

Cybercrime and Digital Forensics

Digital media law is now the dynamic legal territory. &ltl>Mass Media Law: The Printing Press to the Internet is a textbook designed to introduce students to the panoply of legal theories raised by the Internet revolution as well as those supporting traditional media. The book takes a historical approach beginning with the printing press and the telegraph and proceeding to the digital technologies of today, such as social media and search engines. Concepts such as defamation, broadcast regulation, privacy, and free expression are covered along with new media legal theories including Internet exceptionalism, cyber libertarianism, and digital speech and democratic culture. These are introduced to explain why traditional theories such as First Amendment medium-specific analysis, common carriage, and network neutrality are just as relevant today as they were in the

early twentieth century. In order to help readers develop critical reasoning skills, each chapter opens with a highly readable realworld vignette and goes on to identify and explain legal doctrines and tests. Key passages from court opinions are highlighted, and each chapter closes with a list of online media law resources and thought-provoking questions, including legal hypotheticals, to give readers a solid understanding of the area in question. &ltI>Mass Media Law is designed to be the main text and a valuable resource for undergraduate and graduate courses covering media, mass communication, free expression, and journalism law.

Cyberlaw

"No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." Did you know that these twenty-six words are responsible for much of America's multibillion-dollar online industry? What we can and cannot write, say, and do online is based on just one law—a law that protects online services from lawsuits based on user content. Jeff Kosseff exposes the workings of Section 230 of the Communications Decency Act, which has lived mostly in the shadows since its enshrinement in 1996. Because many segments of American society now exist largely online, Kosseff argues that we need to understand and pay attention to what Section 230 really means and how it affects what we like, share, and comment upon every day. The Twenty-Six Words That Created the Internet tells

the story of the institutions that flourished as a result of this powerful statute. It introduces us to those who created the law, those who advocated for it, and those involved in some of the most prominent cases decided under the law. Kosseff assesses the law that has facilitated freedom of online speech, trolling, and much more. His keen eye for the law, combined with his background as an award-winning journalist, demystifies a statute that affects all our lives –for good and for ill. While Section 230 may be imperfect and in need of refinement, Kosseff maintains that it is necessary to foster free speech and innovation. For filings from many of the cases discussed in the book and updates about Section 230, visit jeffkosseff.com

Cybersecurity Law

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.

Digital Copyright

Chris Marsden argues that co-regulation is the defining feature of the Internet in Europe. Co-regulation offers the state a route back into questions of legitimacy, governance and human rights, thereby opening up more interesting conversations than a static no-regulation versus state regulation binary choice. The basis for the argument is empirical investigation, based on a multi-year, European Commission-funded study and is further reinforced by the direction of travel in European and English law and policy, including the Digital Economy Act 2010. He places Internet regulation within the regulatory mainstream, as an advanced technocratic form of self- and co-regulation which requires governance reform to address a growing constitutional legitimacy gap. The literature review, case studies and analysis shed a welcome light on policymaking at the centre of Internet regulation in Brussels, London and Washington, revealing the extent to which states, firms and, increasingly, citizens are developing a new type of regulatory bargain.

Law and Authors

The result of a three-year project, this manual addresses the entire spectrum of international legal issues raised by cyber warfare.

The International Dimensions of Cyberspace Law

Provides an overview of issues related to criminal and antisocial activity that occurs online, including history, terminology, biographical information on important individuals, and a complete annotated bibliography.

ROMANCE ACTION & ADVENTURE MYSTERY & THRILLER BIOGRAPHIES & HISTORY CHILDREN'S YOUNG ADULT FANTASY HISTORICAL FICTION HORROR LITERARY FICTION NON-FICTION SCIENCE FICTION