1. The scope of cyberlaw

1.1 RECONSIDERING CYBERLAW

1.1.1 The Nature of Cyberlaw

Since the explosion of the Internet into our daily lives in the mid- to late 1990s, scholars have struggled with the question as to whether the omnipresence of this global communications medium has – or should be regarded as having – given rise to a new legal field. While cyberlaw courses have become a staple in law school curricula, there is little consensus as to what the subject might – or should – entail. A frequent argument against cyberlaw is that there is no “there” there: in other words, cyberlaw is merely the collation of a loosely related set of cases and principles from various fields of law that happen to involve the Internet.

Some commentators have argued that, even if this is true, cyberlaw can still teach us important lessons about the nature of legal regulation, as contrasted with other regulatory modalities. For example, Professors Lessig and Reidenberg have forcefully argued that cyberlaw is an important conceptual field within which to contrast the nature of law as a regulator of human conduct against other regulatory modalities, notably system architecture, or software code. These scholars have suggested that the latter, particularly code, are likely much more effective in terms of constraining what people can and cannot do online than legal regulation.

This book reconsiders the question of the nature of cyberlaw with the benefit of hindsight. While earlier scholars considered the questions

---


2 Easterbrook, supra note 1.

prospectively – in terms of how the Internet might impact human behavior and how courts and legislatures might respond to online problems, this book considers these questions looking back on roughly fifteen to twenty years of legal developments in response to the Internet. On the basis of existing case law and legislation, it attempts to draw common threads from situations dealing with issues as facially diverse as defamation; privacy; protection of intellectual property rights; fraud, identity theft and other forms of cyber-victimization; and questions of information ownership and access.

The knowledge we now possess about how cyberspace has in fact been regulated helps to answer questions as to what the cyberlaw field should ideally look like. The dual aims of this book are to: (a) justify the existence of cyberlaw as a legal field; and (b) describe how it might be framed as a more cohesive field of study than has previously been the case. The ability to reframe cyberlaw in light of the realities of modern regulation will aid the development of the field in more pragmatic and predictable directions.

1.1.2 Central Tenets of Cyberlaw as a Law of the Intermediated Information Exchange

This book argues that several forces can unify cyberlaw, revolving round the fact that the Internet is, at its core, an interactive global online communications system. This deceptively simple fact speaks to the heart of what is unique about regulating online conduct. Because the Internet is a communications medium, all online transactions involve the exchange of information between individuals rather than physical interactions between them. Thus the regulation of information exchange must be a central feature of Internet law. The extent to which information can be propertized – or commodified – is a very significant factor in this equation. The lack of physical interaction online means that Internet law deals entirely with intangible property.

Along with the importance of information as a central tenet of cyberlaw, all online interactions involve the participation of one or more intermediaries – organizations that enable digital information exchange. These intermediaries range from Internet Service Providers (ISPs) that enable basic access to forums for specific kinds of information exchange such as search engines, online social networks, electronic retailers/auction sites, data aggregators, blogs, educational institutions, and government departments. In many ways, cyberlaw is the law of third-party-mediated information exchanges. Thus, the central focus of a
reconceptualized cyberlaw field should be on issues involving regulation of information, and on the role of these intermediaries within information exchanges.

1.1.3 Common Themes Underlying Cyberlaw: Jurisdiction, Norms and Harms

Outside of these two key concepts – the central role of information and intermediaries – come other distinctive questions related to online conduct. These questions may not be as unique to cyberlaw as the foundational tenets of information and intermediaries. However, they are significant enough to comprise what we might think of as common themes underlying much of the field. The main common themes of cyberlaw revolve around: (a) the global reach of the Internet; (b) differing norms of behavior that occur online as compared with those in the physical world; and, (c) the kinds of harms suffered as a result of undesirable online behavior. Each of these aspects of the Internet can prove challenging for regulators and they are all somewhat interrelated.

The fact that much Internet content can be accessed simultaneously in most countries raises jurisdictional challenges along with the specter of differing cultural norms that may come into conflict in terms of attitudes to appropriate regulation. What is a matter of free speech in the United States may not be protected elsewhere, either normatively or as a matter of constitutional law. Outside problems of cultural norm divergence are potential divergences of social norms between online communities: for example, what may be acceptable in an adult chatroom may not be acceptable on a child-friendly blog. Additionally, online and offline norms within similar communities may vary.

It has been well documented that people interacting online tend to be much less inhibited with a lesser tendency to self-censor than people interacting in the real world. Part of the reason for this may be the absence of physical world cues online that impact conduct in the real world, including facial expressions, tones of voice and body language. All of these subtle cues are missing from online interactions. When confronted with a computer monitor rather than a person, people tend to be disinhibited in their conduct.

---

4 See, for example, Sherry Turkle, Alone Together: Why We Expect More from Technology and Less from Each Other, 235–36 (2011) (describing the way that individuals often respond to each other in much more coarse and aggressive ways online than in physical space).
Internet-based harms also raise challenges different in scope and nature than their physical world counterparts. The harms engendered by, say, intellectual property infringement or defamation online may be much greater in scope and scale than their physical world analogs because of the global reach of Internet communications. The Internet also raises the specter of new classes of harm engendered by flame wars, global privacy or reputation damage, and widespread anonymous vigilante justice. The ability to aggregate information online quickly and easily from multiple sources and to distribute it at the push of a button can cause much more comprehensive and global damage to an individual in terms of cyber-harassment and cyber-bullying than was ever possible in the physical world.

To the extent that the Internet enables new kinds of harm, or at least harms on a more aggregated global scale, the field of cyberlaw will ultimately also be faced with new questions involving appropriate legal remedies for these harms. Injunctive relief may be more appropriate in most cases than monetary relief. Injunctive relief will tend to impact online intermediaries more significantly than perhaps those individuals who participate in harmful information exchanges. Imposing injunctions on intermediaries to stanch harmful information flows will be much more effective than seeking relief against individuals often in multiple jurisdictions. However, this approach will also raise questions about appropriate legal burdens to impose on intermediaries in terms of monitoring and controlling the conduct of those who utilize their services. This book will examine a number of case studies involving the balance of legal rights and responsibilities imposed on intermediaries in fields such as copyright infringement, trademark infringement, privacy, defamation and cyber-harassment.

1.2 WHAT MIGHT “NOT” BE CYBERLAW

An attempt to identify the boundaries and unifying themes of cyberlaw also necessitates a consideration of what might not belong within those boundaries, at least as central tenets or common themes. If cyberlaw is regarded as the law of the intermediated information exchange, some

---

5 Id. (discussing concerns about online flaming and flame wars).
6 Jacqueline Lipton, “We, the Paparazzi”: Developing a Privacy Paradigm for Digital Video, 95 IOWA LAW REVIEW 919, 921–22 (2010) (providing examples of online vigilante justice) [hereinafter, Paparazzi].
7 Id.
issues become more peripheral to the field than existing casebooks and syllabi would suggest. These issues include regulation of the hardware through which online communications take place, and some of the more procedural jurisdictional questions. This sub-section examines why these issues, while undoubtedly relevant to the study of cyberlaw, should not be regarded as a central focus of the field.

In terms of the hardware – the pipes, cables and bandwidth that enable online communications – it is true that these elements of the system will be subject to legal regulation. Nevertheless the regulation of the infrastructure is largely a separate question to regulating the content passing through the system (except perhaps in debates about network neutrality). The regulation of network infrastructure is a highly specialized and government-specific aspect of the Internet. While a content-based cyberlaw course is relatively generalized, focusing on the global regulation of online conduct and content, the regulation of telecommunications hardware is an extremely sophisticated and jurisdiction-specific endeavor. While the two are related, it is too difficult, and largely unnecessary, to include the infrastructure regulation piece as part of a cyberlaw course, except perhaps to touch on it as an issue important in its own right but not necessarily central to the basic course of study.

Many existing cyberlaw texts also devote some time to procedural conflicts of law issues which are again a highly specialized and highly jurisdiction-specific area of the law. These issues could safely be relegated to the sidelines in cyberlaw courses of the future for the following reasons. While in the early days of the Internet, questions arose as to whether cyberspace was a new jurisdictional “place” (for want of a better term) that was not amenable to existing conflicts of law principles, these questions have largely been resolved in practice in the negative. Courts have not been reticent to impose existing conflicts principles in cyberspace, particularly in the realm of personal jurisdiction.9

---


Some litigants have expressed concern that subjecting foreign defendants to an unfamiliar jurisdiction could lead to the unfair imposition of unanticipated and expensive legal consequences for an online communication published generally to the world at large. However, judges have been generally unsympathetic to these arguments, noting that defendants should know when their online conduct could raise problems in a foreign jurisdiction and should take appropriate action to avoid liability. For example, in the famous Gutnick v Dow Jones case, the High Court of Australia noted that Dow Jones knew that their online publication was available in Australia, where the plaintiff would suffer the brunt of the defamation. They affirmatively chose to make the publication available to Australian subscribers, and the Australian courts and laws were thus appropriate for the case. In the Yahoo! case involving La Ligue Contre Le Racisme, a French court granted an injunction to prevent Yahoo! customers from selling Nazi memorabilia to French customers on the basis that even though Yahoo! could not absolutely ensure that no such memorabilia was ever sold to a French customer, it could employ some relatively effective mechanisms to prevent the sales.


10 See, for example, Dow Jones v Gutnick, [2002] HCA 56, para. 165 (“The notion that those who publish defamatory material on the Internet are answerable before the courts of any nation where the damage to reputation has occurred, such as in the jurisdiction where the complaining party resides, presents difficulties: technological, legal and practical. It is true that the law of Australia provides protections against some of those difficulties which, in appropriate cases, will obviate or diminish the inconvenience of distant liability. Moreover, the spectre of ‘global’ liability should not be exaggerated. Apart from anything else, the costs and practicalities of bringing proceedings against a foreign publisher will usually be a sufficient impediment to discourage even the most intrepid of litigants. Further, in many cases of this kind, where the publisher is said to have no presence or assets in the jurisdiction, it may choose simply to ignore the proceedings. It may save its contest to the courts of its own jurisdiction until an attempt is later made to enforce there the judgment obtained in the foreign trial. It may do this especially if that judgment was secured by the application of laws, the enforcement of which would be regarded as unconstitutional or otherwise offensive to a different legal culture”).

11 Id.

12 Ligue Contre Le Racisme et L’Antisemitisme v Yahoo!, Superior Ct. of Paris (Nov. 20, 2000).

13 Id.
In other words, jurisdiction does not appear to have become the problem it was initially believed to be. Obviously, a global communications medium potentially causes a greater number of cross-border legal issues, but that fact has not prevented the application of conflicts principles to cases where Internet conduct is implicated. It is possible that a greater number of Internet-related cases are effectively resolved at the jurisdictional stage and that courts do not get a chance to rule on substantive legal issues as often as they do in non-Internet cases involving multiple jurisdictions. However, there is no empirical evidence available to decisively support this argument. As with questions relating to the regulation of the hardware, conflicts of law principles are highly specialized and jurisdiction-specific. While they are relevant to the study of cyberlaw, they should not be regarded as comprising its central focus. What we can learn from cyberlaw as a cohesive field relates to the regulation of intermediated conduct involving online content, rather than the application of specific conflicts principles in given cases.

Another aspect of cyberspace regulation that has also taken up significant space in cyberlaw casebooks to date – and perhaps could now be relegated to a position of lesser importance – is the question of legislative competence of domestic governments to regulate online conduct. As with conflicts questions, these issues have not proved to present major hurdles for Internet regulation despite concerns raised about lack of domestic legislative competence over “virtual places” in the early days of the Internet. Domestic governments have effectively regulated much online conduct in the ensuing years. The one exception may be laws that implicate First Amendment concerns in the United States, and perhaps some commerce clause issues.

While the debate about whether cyberspace should be subject to domestic regulation has pretty much been answered in the affirmative, the question of the most effective approaches to Internet regulation remains a significant facet of cyberlaw in terms of policy debates about regulation more generally. As noted above, Internet regulation will always involve one or more online intermediaries facilitating information transactions. Thus, an important question for cyberlaw should be the extent to which laws should be focused on intermediaries, rather than primary actors. Another important question for cyberspace regulation

---

14 See, for example, Reno v ACLU, 521 U.S. 844 (1997); Aschcroft v ACLU, 535 U.S. 564 (2002).
15 See, for example, American Libraries Association v Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997).
going forward will be identifying areas where legal regulation is important as opposed to other forms of regulation—such as software code, market forces and social norms. The interplay between these regulatory modalities is also an important question. Legal regulation does not operate in a vacuum and it is important to examine ways in which laws support other regulatory modalities and vice versa. For example, in areas where social norms are underdeveloped laws may serve a significant expressive function outside their potential for enforcement.

The global nature of the Internet also creates a need for legislatures to consider the extent to which global harmonization is desirable. Currently there are some significant global disjoints between approaches to the regulation of online privacy, defamation, and to some extent even intellectual property law. The recent Google privacy issues in the European Union are a clear example of this lack of harmonization. The European Union effectively requires Google to delete certain records about an individual from search results while the United States laws do not require similar action. Lack of harmonization can lead to confusion and expense, difficulties relating to cross-border enforcement, and the temptation of powerful countries to exert political pressure on less powerful countries to bring their laws into compliance.

1.3 DEFINING KEY TERMS: INFORMATION AND INTERMEDIARY

1.3.1 Information

As noted above, as an intermediated communications medium, the regulation of the Internet should revolve around the regulation of intermediated information or content exchanges. If this approach is taken, it is necessary to develop a working definition of the terms “information” and “intermediary” in this context. While these are each broad concepts, considering them in the context of existing cyberlaw cases and problems does suggest some commonalities as to how they might be defined for cyberlaw.

18 *Google Spain v Costeja González*, Case C-131/12, Court of Justice for the European Union (May 13, 2014).
Most dictionary definitions contemplate that the term “information” is best defined in terms of “knowledge”, “data”, “communication” or “input”. Most definitions comprise aspects of both content per se, and of communication of content. In other words, definitions tend to have a static aspect and an active/exchange aspect. The idea of information itself seems to comprise the importance of not simply compiling, learning or knowing something, but also the act of sharing or disseminating it with others. This is important for cyberlaw as it is the exchange component of information online that comes under the most regulatory scrutiny. While the development of new information is undoubtedly important, particularly in fields such as intellectual property, the dissemination of that information online is what comprises the basis of most Internet conflicts ranging from defamation and privacy incursions to intellectual property infringement.

In terms of digital technology, information also comes in more than one form. Notably, digital information can be input and output in human-readable forms, such as traditional human language. It can also be input and output in machine-readable forms, like binary code. Some information utilized online can be a combination of human-readable and machine-readable, meta-tags being an obvious example. Meta-tags can be used on a website to guide search engines to relevant content. They are input by individuals in traditional language, and converted to machine-readable code for search engines to index. Of course, search engines can also “read” digital text and images that form website content more generally, so in a sense all digital information comes in both a human-readable and machine-readable form. Even Internet domain names are effectively only alphanumeric (human-readable) versions of underlying numerical IP addresses.

This book will focus on information as digital content in human readable form – including text, images, digital music and multi-media files. However, it is important to understand that at some level all of this information can be broken down into machine-readable code. Some regulatory questions confronted in cyberlaw relate to the relationship between regulating human-readable content and underlying code. In the copyright area in particular, the significance of copies of software code continually running in multiple machines to effect digital communications has been problematic in practice.

1.3.2 Intermediary

As noted above, a significant distinguishing feature of the Internet is the fact that some form of intermediary is always involved in online interactions. It is impossible for individuals to interact online without the
assistance of one or more intermediaries. For instance, in the real world I can talk to my friends face to face. But in the online world, I need to employ the services of usually multiple online service provider intermediaries to communicate with others.

The definition of intermediary is challenging, but necessary to create a conception of cyberlaw that is unified and cohesive. It is the role of intermediaries that has become the central focus of much online conduct since the inception of the Internet. Intermediaries are the most effective targets for injunctions to prevent undesirable online conduct. They are also often in the best position to monitor and control communications shared over their services. The question of balancing their liabilities, and costs of such monitoring and control, against the innovative services they provide has become a central theme in all fields of Internet law including domain name regulation, intellectual property infringement, defamation, fraud, and privacy incursions.

Additionally, it is generally easier for the individual complaining about harmful online conduct to locate and serve process on an intermediary than a defendant who may be more obviously complicit in the plaintiff’s harm but who may be operating anonymously/pseudonymously and may be difficult to locate geographically. Asserting personal jurisdiction over such a defendant may also be problematic, depending on where the defendant is located. Many individual defendants are also impecunious and cannot furnish a complainant with monetary damages, in cases where such a remedy is appropriate. Even where the complainant seeks injunctive relief, the cooperation of the intermediary that facilitated the harmful communications will most likely be required. For example, an intermediary can be called upon to terminate a defendant’s user account or to monitor the defendant’s future activities online. An injunction will also likely be more effective in practice against an intermediary that disseminates harmful information broadly even if that entity did not initially create the information in question. Again, the Google privacy decision in the Court of Justice of the European Union (CJEU) in 2014 is a good example of this dynamic. While the newspaper that wrote the story about which the defendant complained was held not to have a responsibility to delete information relating to the plaintiff, the search engine that broadly promulgated the information was liable.¹⁹

¹⁹ *Id.*, at paras. 16–17 (noting that in the prior procedural history of the case, the newspaper that initially published the information in question was legally justified in publishing it, but that did not necessarily mean that Google was legally justified in reproducing the information in search engine results).
In the modern world, there are many different kinds of online intermediaries, a number of which will be used for case studies in this book. There are search engines, content-sharing services, payments services, retail outlets, and web-hosting services/domain name registries. All of these intermediaries enable the Internet communications that many of us take for granted. The one thing that unifies them is that they are all gateways to online communications in some way or another. They are the backbone of a system that enables the rest of us to engage in meaningful online interactions. They are also arguably the entities that most risk legal liability for the wrongful conduct of others for reasons explained in the previous section – they are the obvious choke points to monitor and control wrongful online conduct.

This book conceptualizes online intermediaries as any entity that creates a platform to enable online communications. It is undoubtedly a very broad definition and is informed by case law and legislation that has grouped these entities together when regulating online conduct. Thus, intermediaries include traditional Internet service providers such as America Online (AOL) and Yahoo! The notion of an “intermediary” also includes search engines such as Google and Bing – those entities that enable us to find information online. Electronic commerce websites such as Amazon.com and iTunes are also examples of intermediaries – those entities that enable transactions in digital information.

Online social networking platforms such as Facebook, YouTube, Pinterest and Twitter are important examples of online intermediaries that may be implicated in the wrongful conduct of their users. Individuals utilizing these services may engage in a number of different kinds of online wrongs such as bullying, harassment and copyright infringement. Because these services, unlike, say, search engines, require users to register accounts with them, they are able to employ contracts – Terms of Service agreements – to minimize their legal liability and to express their views about appropriate online conduct. Many of these services, for example, utilize detailed privacy policies.

It is important to note that the ability to utilize contracts is inherently limited to services that are in a position to require users to enter into contracts to accept their services. Some intermediaries – such as search engines – typically do not work on a “member sign-up” model, so do not utilize contracts in this way. Other intermediaries require sign-up for posting information, but, once posted, the information is generally available to the public. YouTube is an example of this model. Thus, YouTube is able to enter into contractual agreements with those who post content with it, but not with those who access content. The role of contracts in managing the liability of online intermediaries is discussed in
more detail later in this book. Electronic payments systems – such as PayPal, Visa and Mastercard – are arguably also part of the intermediary framework for supporting the commercial aspects of online transactions.

Because of the central role played by intermediaries in enabling all online conduct, a cyberlaw field needs to focus significantly on appropriate approaches to regulating the conduct of those intermediaries. A strategy that places significant burdens of potential liability on these intermediaries runs the risk of chilling online innovation and communication generally, while an approach that avoids imposing any duties on intermediaries runs the risk of inadvertently condoning wrongful online conduct. The ill-fated Stop Online Piracy Act (SOPA) was perhaps an example of the former approach, while the implementation of § 230 of the Communications Decency Act (CDA) in the United States is arguably an example of the latter.

A reconceptualized cyberlaw field could serve to organize the judicial and legislative developments from disparate areas of law that relate to intermediaries into a more cohesive framework. Currently, online service providers within the United States face completely different approaches to liability in fields such as copyright, trademark and defamation law. Even within those fields, questions of primary versus secondary liability for online service providers remain largely unanswered. There is no uniform approach as to when and whether an intermediary should be sued in primary versus secondary liability in fields such as copyright or trademark law. The picture is even more confusing for such service providers across national borders.

The remainder of this book comprises detailed examination, drawing heavily from existing case law and legislation, of the central role played by online intermediaries in Internet-based transactions. It attempts to draw common threads between intermediary issues that have arisen across distinct legal fields. Focusing on recent developments in the digital content marketplace, along with case law and legislation from the United States and other jurisdictions involving online conduct, the author attempts to create a more cohesive approach to cyberlaw going forward. Many of the case studies revolve around attempts to balance interests in intellectual property and privacy against free speech and other public interests in the online context. These questions go to the heart of Internet regulation because cyberlaw is all about content regulation and the balance between access to, and control of, digital information. The key point is that because intermediaries are essential to all online conduct they are in a unique position as a focal point of Internet regulation.

The following chapters focus respectively on the role of intermediaries in online information exchanges in the context of digital copyright law,
1.4 CHAPTER SUMMARY: THE CONTOURS OF CYBERLAW

While no book can answer every possible question about future directions for the development of the cyberlaw field, the aim of this book is to reconceptualize the basic tenets of the field so debates about future regulation of the Internet can be more cohesive and pragmatic. In particular, it is important to move the debate away from questions about whether cyberlaw is a distinct field toward what the field actually comprises. The subject has endured in law school curricula and does have something important to contribute to law reform efforts provided that it is conceptualized in a more unified manner with a focus on intermediated information exchange. The central tenets of the field are therefore: information and intermediaries.

Related themes include jurisdictional questions, the relationship between legal rules and other regulatory modalities, the role of law as a regulatory force online (as compared with other modalities of regulation), and appropriate remedies for online harm. It is obvious from this description that the discussions in this book will consciously focus on “law” as regulator of online conduct, as contrasted with these other modalities. While it is not possible to consider law in a vacuum, much existing cyberlaw literature has argued that law becomes less relevant in the digital age and other forces may be more effective as regulators.20

It is important to focus back on the appropriate role for legal regulation online, rather than making the assumption that law should take a back seat to system architecture and social norms. While it may be true that law is less important online as a regulator than in the physical world, the law does have something to contribute to Internet regulation, and it would be inadvisable to overlook its importance.

20 See, for example, notes 1 and 3, supra, and accompanying text.