2011

New First Principles? Assessing the Internet's Challenges to Jurisdiction

Teresa Scassa

Robert J. Currie

NEW FIRST PRINCIPLES? ASSESSING THE INTERNET'S CHALLENGES TO JURISDICTION

TERESA SCASSA AND ROBERT J. CURRIE*

The globalized and decentralized Internet has become the new locus for a wide range of human activity, including commerce, crime, communications and cultural production. Activities which were once at the core of domestic jurisdiction have moved onto the Internet, and in doing so, have presented numerous challenges to the ability of states to exercise jurisdiction. In writing about these challenges, some scholars have characterized the Internet as a separate "space" and many refer to state jurisdiction over Internet activities as "extraterritorial." This article examines these challenges in the context of the overall international law of jurisdiction, rather than focusing on any one substantive area. This article argues that while the Internet may push at the boundaries of traditional principles of jurisdiction in public international law, it has not supplanted them. The article explores the principles of jurisdiction, including the evolving concept of "qualified territoriality," and demonstrates how these principles continue to apply in the Internet context. The article examines how states exercise their authority with respect to Internet activities by addressing governance issues, by engaging in normative ordering for the Internet, and by extending the reach of their domestic laws to capture Internet-based activities. Lastly, the article concludes by offering a set of "first principles," in the form of policy precepts, to guide the evolution of public international law norms and to address problems particular to the context of the global Internet.

CONTENTS

---

* Teresa Scassa is Canada Research Chair in Information Law, and Professor, Faculty of Common Law, University of Ottawa. Robert J. Currie is Director of the Law & Technology Institute, and Associate Professor, Schulich School of Law, Dalhousie University. The authors gratefully acknowledge the funding of research support for this article provided by the Social Sciences and Humanities Research Council of Canada. Thanks also to Jenna Wates (J.D. Dalhousie, 2011) for her sterling research assistance, and to our colleagues Steve Coughlan and Hugh Kindred.

I. INTRODUCTION

Despite its historical origins, the Internet is far more than a communications network. In a short space of time it has become an apparently borderless marketplace, a forum for discussion and exchange of ideas, a criminal network, and a site for the uninhibited exchange of intellectual property. Its global and decentralized nature has also dramatically changed the identities and roles of traditional actors and intermediaries in a range of activities, from commerce to cultural production and information dissemination.

The variety and significance of so much Internet activity—and its impact on pressing domestic issues such as crime, national security and the economy—has necessarily compelled states toward increased engagement with matters outside their traditional spheres of legal authority. Put simply, because the Internet is borderless, states are faced with the need to regulate conduct or subject matter in contexts where the territorial nexus is only partial and in some cases uncertain. This immediately represents a challenge to the Westphalian model of exclusive territorial state sovereignty under international law. As a result, many states have grappled with defining the boundaries of traditional notions of state jurisdiction in cyberspace. This is manifest in the assumption of jurisdiction by states over a broad range of subject

matter, from the most routine financial transactions to the much-hyped need for "cyber-security" against Internet-based attacks by other governments or terrorist groups. Courts struggle with a range of increasingly pressing challenges to their very competency to hear a matter, which would have been unheard of only two decades ago.[1] Inter-state conflict is inevitable and has occurred.

Given this situation, it is imperative to attain a clear understanding of the law of jurisdiction and to examine its operation in cyberspace. However, a great deal of the attention paid to jurisdictional issues in the legal literature has been sector-based; one sees publications on jurisdiction over cyber-crime, jurisdiction over foreign torts, jurisdiction over commercial transactions, and so on. The literature has also often been limited to a consideration of jurisdiction solely in the context of a single branch of government, most often in relation to the exercise of jurisdiction by courts. What is needed, we suggest, is an approach grounded solidly on a broad understanding of both *how* states and state entities exercise their jurisdiction, and the fundamental legal norms that underpin it.

Accordingly, in this paper we will explore both the concept of state jurisdiction and the way in which this concept is being transformed in the context of the Internet. Drawing on examples from various substantive law areas that have been affected by the Internet, we will develop and illustrate the range of state actions encompassed by a broad understanding of jurisdiction. Such a multi-faceted approach to jurisdiction is required to understand the Internet's impact on the way jurisdiction is exercised by various arms of the state, whether through legislative, administrative, judicial or enforcement activity. Through this lens we will examine the manner in which states, via the various branches of government, have adapted to the challenge of the Internet. We scrutinize the extent to which these responses have already begun to shape new principles for the exercise of state jurisdiction in the Internet age and query whether new "first principles" of jurisdiction are nascent, emergent, or even required. The goal is to understand the current state of the law, to assess and forecast where the Internet has placed traditional norms and expectations under stress, and to suggest means and ways by which states, legislators, and courts must innovate.

---

1. "The growth of online activity has been matched by a corresponding growth of transnational civil disputes—a trend which is likely to continue with the further growth of Internet presence." UTA KOHL, JURISDICTION AND THE INTERNET: REGULATORY COMPETENCE OVER ONLINE ACTIVITY 7 (2007).

II. The Current State of the Law

A. *Jurisdiction Defined Generally*

It is difficult to come up with a legal term which is more overburdened than "jurisdiction"; it is a "word of many, too many, meanings."[2] Its multiple layers and meanings are driven by the context in which it is used, but there are nonetheless common threads that allow lawyers, when speaking with each other, to use the word in an intelligible way. Generally speaking, jurisdiction refers to:

> . . . the ability of the state to exercise some form of power, coercive or otherwise, over persons, places, things (including property) and events. This power may be exercised by various agencies of the state—the legislature, the executive, the courts or regulatory bodies that receive delegated power from one of those sources—and is defined and delimited by whatever the powers of those agencies happen to be.[3]

One sometimes sees the phrase "domestic jurisdiction" used in a way meant to distinguish it from "international jurisdiction," yet this is essentially shorthand for a point that is vital to examining jurisdiction and the Internet—to wit, there is a domestic law *of* jurisdiction and there is international law *about* jurisdiction. Any given state will have a law or set of laws, typically as part of its constitution, which sorts out the relative authority of any branch of the state. For example, in federal states such as Canada and the U.S., the constitution prescribes what powers each level of government (federal and provincial, federal and state, respectively) has, and implicitly or explicitly sets out limitations on those powers, whether according to subject matter, geography, or some other factor. It also sets out the areas of competence of the courts. As noted in the introduction, this domestic law is not the primary focus of this paper, apart from at a general level which will be described in part B of this section, below.

The international law of jurisdiction is our primary focus here—that is to say, the body of public international law which sets out rules for when and how the state (in its many aspects) may exercise jurisdiction over something. It is in a practical sense analogous to the international law of the sea, a field which demanded the creation of a set of rules

2. United Phosphorus Ltd. v. Angus Chemical Co., 322 F.3d 942, 948 (7th Cir. 2003).

3. Robert J. Currie, International & Transnational Criminal Law 50 (2010).

among states, as the jurisdictional actors, given that the subject matter was so vast that none could control it. Yet even this analogy breaks down when one considers the global electronic interconnectedness of the Internet, which produces the unique effect that it exists, operates and is used both in one state at a time and simultaneously in all states. Not only will any single state not wish to control the Internet, it could not possibly do so except in isolated pockets, and even then any exercise of jurisdiction over the Internet potentially has implications for something or someone outside that state.

The latter point is perhaps the most important, because it illustrates that any exercise of jurisdiction by a state in an inter-connected world has the potential to bump up against the interests of another state. This naturally implicates the international law of jurisdiction, which, as Mann noted in his seminal essay, establishes normative parameters for "a State's right under international law to regulate conduct in matters not exclusively of domestic concern."[4] That law, he wrote, "is concerned with what has been described as one of the fundamental functions of public international law, *viz.* the function of regulating and delimiting the respective competences of States."[5] Jurisdiction at international law "reflects the basic principles of state sovereignty, equality of states and non-interference in domestic affairs."[6] Quite obviously, states' sovereign interests are heavily engaged in Internet-related matters, regardless of subject matter. Accordingly, in our view, international jurisdiction is the hot topic when it comes to "law and the Internet."

The international law meaning of jurisdiction will be explored below, as well as our overall question, which is whether that body of law is adequate to offer states a meaningful framework to govern their actions in relation to Internet-based activities.

B. *Jurisdictional Actors: A Public Law Concept*

It is important to emphasize at the outset that jurisdiction is an inherently public law concept. This might seem self-evident, given the definitions for jurisdiction provided above, and yet we feel it bears explanation and emphasis if one is to gain a broad understanding of the nature of jurisdiction. It may also help to avoid the problems which

4. F.A. Mann, *The Doctrine of Jurisdiction in International Law*, 111 RECEUIL DE COURS 1, 9 (1964).

5. *Id.* at 15.

6. MALCOLM SHAW, INTERNATIONAL LAW 572 (5th ed. 2003).

often crop up in the literature, from focusing on a particular *kind* of exercise of jurisdiction, by a particular state entity, in a particular area of substantive law.

One of the building blocks of the literature regarding the law of jurisdiction has, for many decades,[7] been the division of the state into three entities for the purpose of exercising jurisdiction.[8] These familiar branches are: the *legislative* or *prescriptive* branch, which refers to the ability of the state to make and apply laws to subject matter, whether that subject matter involves wholly domestic matters or touches on matters outside the state's territory; the *enforcement* or *executive* branch, which refers to the state's ability to give effect to its laws (including the ability of police or other government actors to investigate a matter, which might be referred to as *investigative jurisdiction*); and the *judicial* or *adjudicative* branch, which refers to the ability of a state's courts to adjudicate cases, particularly for our purposes those with foreign elements.[9]

Accordingly, any action taken by a state that can be called an exercise of jurisdiction must ultimately go through one of these channels. The exercise of jurisdiction operates across a spectrum of subject matter, and jurisdiction is a function of the level of state interaction with or intrusion into the subject matter. Depending on the subject matter, there may be an exercise of legislative, executive, or judicial jurisdiction—or there may be a mixture of any two or three of them. In fact, it is rarely the actions of one branch of the state that are implicated; the law of jurisdiction changes depending upon which state entity or entities are engaged in a particular exercise of jurisdiction. It is important to understand this, not least because proposals for law

7. *See* Michael Akehurst, *Jurisdiction in International Law,* 46 BRIT. YB. INT'L L. 145, 145 (1972–73) (providing a classic exposition); *see also* Mann, *supra* note 4; Stephen Coughlan, Robert Currie, Hugh Kindred & Teresa Scassa, *Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization*, 6 CAN. J. LAW & TECH. 29 (2007) [hereinafter Coughlan et al.].

8. Though other international law writing and jurisprudence often refers to two categories, "prescriptive" and "enforcement" jurisdiction, with adjudicative jurisdiction being a sub-principle of enforcement. In our view that typology is better suited for criminal law matters.

9. While this structure looks something like the "division of powers" in government known to liberal democracy, naturally not every state subscribes to the full democratic implications of such a structure. In more totalitarian systems, for example, the executive and legislative branches may be fused, or all power may come from the executive arm and the courts and legislature may be subservient to it. There are many variations in the international community. Nonetheless, we feel that this structure continues to have explanatory power, particularly given that it fairly accurately reflects the *external* manifestations of state jurisdiction—i.e., other states observing/reacting to a state's exercise of jurisdiction are seeing a legislative, enforcement or adjudicative action.

reform should reflect a holistic idea of what kind of state action is being contemplated. It is also important for this paper because, as will be explored in section III, below, some of the challenges posed by the Internet impact the state's capacity to exercise any or all of the three forms of jurisdiction—and thus its ability to govern.

Criminal law is the domain from which the international law of jurisdiction originally emerged, and it presents a good example of the range of jurisdictional action set out above. At various stages, an exercise of criminal jurisdiction can involve all three state branches. The executive might sign a treaty with other states, agreeing to criminalize a particular act and exercise jurisdiction over it. Most such treaties are not self-executing[10] and will require an exercise of legislative jurisdiction (the passing of a law) to both criminalize the act and establish jurisdiction over it. The police, an arm of the executive branch of the state, exercise enforcement jurisdiction by investigating the crime and arresting perpetrators. The courts exercise adjudicative jurisdiction, first by determining whether they have the jurisdiction to adjudicate (either by looking to their inherent jurisdiction or determining whether the legislature has awarded them the power to adjudicate this particular matter) and then by trying and sentencing the perpetrator.[11]

Naturally, depending on the subject matter, a particular exercise of jurisdiction might involve only one branch, with little or no activity from the other two. For example, the executive, in particular, may engage in unilateral exercises of its jurisdiction, such as making diplomatic communications, imposing trade embargoes, signing treaties or memoranda of understanding, etc. The courts in common law jurisdictions, when exercising their inherent powers, sometimes administer the (court-made) common law and act to resolve a dispute between parties without any input from the legislature—though even then, attempts to enforce a civil judgment will likely involve the machinery and compulsory powers of the executive. Civil law jurisdictions would

10. They are not self-executing because, either the states themselves are dualist and require implementation of treaties into national laws (such as Canada); or, even in those states which directly incorporate treaties into the national law, the treaty provisions themselves tend to be framed on a general level, requiring some level of domestic interpretation and implementation in order to effectively translate them into domestic law. *E.g.*, Neil Boister, *Transnational Criminal Law?*, 14 EUR. J. INT'L L. 953 (2003).

11. For further explanation in the Canadian context, see Robert J. Currie, *Libman at Twenty-Five; or, Canada and Qualified Territoriality: Do We Understand Jurisdiction Yet?*, *in* IS OUR HOUSE IN ORDER?: CANADA'S IMPLEMENTATION OF INTERNATIONAL LAW (Chios Carmody ed., 2010).

see an interaction between executive-level activity, legislative creation of the civil code and judicial interpretation and enforcement of the code's provisions.

It is important, too, to recognize that an act of jurisdiction is still public, even if it is with regard to a subject matter thought of as "private." The courts may adjudicate public *law* (e.g. criminal, regulatory, privacy, etc.), but they may also preside over private law disputes between parties. Those parties bring a private right of action that they possess before the court, and the court (in an act of adjudicative jurisdiction) determines whether it can adjudicate and proceeds to resolve the dispute. However, the act of adjudication itself is public. This is true even for private international law, with courts deciding whether they have jurisdiction to hear disputes with foreign aspects or whether to enforce foreign awards.[12]

An exceptional situation may exist where private parties (including the state, when it is acting as a private litigant) agree to submit a dispute to a private arbitral body of some sort, essentially contracting out of their legal and/or constitutional rights to have the courts hear the dispute. The manner in which a private arbitral body is constituted and the powers which the parties agree it will have are often referred to as "jurisdiction," yet in our view they do not fit within that term, or at least certainly not within the conception of jurisdiction being examined here. A better term might be "competence," given the public law content and connotation of the word "jurisdiction." Moreover, it is worth noting that public law jurisdiction is in the background of even private dispute mechanisms. Governments may choose to outlaw these private mechanisms, or more realistically, may regulate access to them by statute or civil code, or pass laws regarding when arbitral awards will and will not be enforced, including the enforcement of contracts containing mandatory arbitration clauses.

Recognizing the public law nature of jurisdiction and the branches of its manifestation, then, this paper will not delve into the vagaries of the internal jurisdictional arrangements of any given state, except by illustrative example. Rather, we will proceed to analyze the impact of these exercises of jurisdiction upon the international law of jurisdiction, both customary and treaty-based.

---

12. And even here, there is a public, executive element contemplated, in so far as execution on assets goes. For example, a U.S. national is awarded a civil judgment against a Canadian national, and applies to the Canadian courts to order the award enforced (adjudicative jurisdiction). The court decides in favor of enforcement, and the litigant has the award enforced by the Sheriff executing upon the judgment debtor's assets in Canada (executive jurisdiction).

C. *The Customary International Law of Jurisdiction (and a Bit on Treaties)*

The previous section has dealt with the ways in which an exercise of jurisdiction is made manifest. This next section will dig into the substance of the law of jurisdiction.[13] While, as noted above, every state has its own domestic law about the exercise of jurisdiction, jurisdiction in the sense we mean here is primarily a creature of customary international law.[14] Like some other areas of customary international law, this body of rules is binding on all states but is not exactly "hard" law in operation; it is more a set of overarching principles that provides a legal basis for states to determine what each may do, and not do, inside and outside their borders. Given the potential for conflict between states as they exercise jurisdiction, it has been accurately stated that the purpose of this body of law "is to safeguard the international community against overreaching by individual nations."[15]

The starting point is territoriality: in the international legal system, the state is essentially a territorial entity and each state enjoys plenary jurisdiction within, and exclusive control over, its territory.[16] A state's plenary jurisdiction over its territory, and every person and thing within it, is a function of state sovereignty. As other states are equally sovereign, it follows that as soon as one state exerts power in a way that purports to regulate or actively affect matters outside its borders, it will face, at least nominally, some limitations. This is captured in the inelegant but standard phrase "extraterritorial jurisdiction."

The international law regarding the exercise of jurisdiction by states can be expressed simply: one state's exercise of sovereign power cannot infringe upon the sovereignty of another state or states. This is easy enough to assert, but nebulous and nuanced in application because judging where the line is crossed is a complex exercise. As explained below, the rules differ as between legislative and enforcement jurisdic-

---

13. Part of this section is adapted, in either condensed or amplified form, from Coughlan, *supra* note 7.

14. Customary international law refers to those rules of international law which derive from the practices of states and the formal recognition by states that this state practice is obligatory (*opinio juris*). Customary international law principles bind all states, even those which have not formally consented to be bound. This is distinguished from treaty law, under which obligations arise by way of formal agreement between states. *See generally* INTERNATIONAL LAW: CHIEFLY AS INTERPRETED AND APPLIED IN CANADA 107–82 (Hugh M. Kindred & Phillip M. Saunders eds., 7th ed. 2006) [hereinafter Kindred].

15. Hannah L. Buxbaum, *Transnational Regulatory Litigation*, 46 VA. J. INT'L L. 251, 304 (2006).

16. *See generally* Kindred, *supra* note 14, at 13–106.

tion, as well. The central point of conflict will be situations of *concurrent jurisdiction*, i.e. where two or more states have some legal claim to exercise jurisdiction over a particular matter.

It is worth noting that, as in all international legal disputes, resolution can be reached on an ad hoc basis; states can agree on where primary jurisdiction should lie on a case-by-case basis. For example, if a French citizen commits murder in the United States, France may have a claim to jurisdiction over its national. However, it is likely to defer to the U.S. since the U.S. is the state where the act occurred and probably where all of the evidence is located, as well as being the more aggrieved state of the two. Simply because a state notionally has jurisdiction over a matter does not necessarily mean that it will have any interest in exercising it.

However, regarding legislative jurisdiction, various principles have developed in international law to allow states to mitigate the conflict that may result from concurrent claims to jurisdiction. This system of "allocat[ing] competences"[17] is a direct outgrowth of the need to manage inter-state relations, and while it is normative in character it is functionalist in practice. As Brownlie has written, "the sufficiency of grounds for jurisdiction is an issue normally considered relative to the rights of other states and not as a question of basic competence."[18]

The starting point, of course, is the *territorial principle*, which renders territorial sovereignty as discussed above one of the bedrock jurisdictional notions. It is accepted that a state can assert jurisdiction over its territory, including the territorial sea, internal waters, airspace, and certain maritime zones.[19] In the context of criminal jurisdiction, it is not unusual (and increasingly typical) that a crime may take place in more than one state, either by way of elements of the crime occurring in more than one state or where the crime is completed in one state but has effects in another.[20] This has led to a sub-class of the territoriality principle developing, called *qualified territoriality*, which will be dealt with in part D, *infra*.

---

17. ROSALYN HIGGINS, PROBLEMS AND PROCESS: INTERNATIONAL LAW AND HOW WE USE IT 56 (1994). By this phrase, Professor Higgins (as she then was) was referring to the use of principles of jurisdiction to determine which states had claims of jurisdiction over a matter and determining the relative strength of those claims. *Id.*

18. IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 297–98 (6th ed. 2003).

19. CURRIE, *supra* note 3, at 60–61.

20. *See, e.g.*, State v. Willoughby, 892 P.2d 1319 (Ariz. 1995) (where an American national was prosecuted for a first degree murder that took place in Mexico, on the basis that the element of premeditation had taken place in Arizona).

Since territoriality is the starting point, it follows that the other jurisdictional principles are extraterritorial. The four principles which have gained some acceptance in international law as supporting extraterritorial action are as follows:

(a) ***nationality principle:*** States may assert jurisdiction over the acts of their nationals, wherever the act might take place. This principle is employed more often by civil law than by common law countries, but has equal status with territoriality as a universally-accepted valid ground of jurisdiction.[21]

(b) ***protective principle:*** States may assert jurisdiction "over acts committed abroad that are prejudicial to its security, territorial integrity, and political independence."[22] Examples are treason, espionage, and counterfeiting of state currency.

(c) ***universal principle:*** States may assert jurisdiction over certain criminal acts which are deemed to be offensive to the international community at large and thus justify broad jurisdictional permissiveness. Some examples are genocide, crimes against humanity, war crimes, and piracy.[23] Certain treaty regimes oblige member states which apprehend an individual accused of the relevant crime to prosecute the individual regardless of whether there is any connection between the crime and the apprehending state. If the state does not wish to prosecute, then it is obliged to extradite the individual to a treaty partner state which indicates a willingness to prosecute. This kind of mechanism is known as *aut dedare, aut judicare* ("extradite or prosecute"),[24] and can be distinguished from the broader notion of universality both by its mandatory character and by the fact that it applies only between the parties to the relevant treaty.

(d) ***passive personality principle:*** Some states have, from time to time and controversially, asserted jurisdiction over acts which injured their nationals, regardless of territorial location.[25] It is increasingly accepted that passive personality jurisdiction can be used, though usually as a subsidiary principle, in cases of terrorist violence. The U.S. makes extensive use of this principle in anti-terrorism legislation.[26]

Exercising extraterritorial jurisdiction, then, is not necessarily illegal

---

21. CURRIE, *supra* note 3, at 66–68.

22. Kindred, *supra* note 14, at 559.

23. CURRIE, *supra* note 3, at 104–152, 281–288.

24. *Id.* at 96–99.

25. *Id.* at 68–69.

26. *See generally* Christopher L. Blakesley, *Extraterritorial Jurisdiction*, *in* 2 INTERNATIONAL CRIMINAL LAW 83 (M. Cherif Bassiouni ed., 3d ed. 2008).

under international law: it depends upon whether in exercising jurisdiction a state can be said to infringe upon the sovereignty of another. In terms of international law methodology, it is controversial whether the law is permissive, in the sense that each state is free to exercise jurisdiction unless there is a prohibitive rule to the contrary,[27] or restrictive, requiring a state to justify its assertion of jurisdiction on some recognizable legal basis. As Ryngaert has noted, "it is unclear which doctrine has the upper hand,"[28] and the question is essentially one of burden of proof. The important aspect is that each of the jurisdictional principles above has the effect of legitimizing, to a greater or lesser extent, a state's claim to exercise jurisdiction over persons, places, and things beyond its territory. They are the techniques which states use to broker conflicts, usually in situations of concurrent jurisdiction.

Recently, the principles described above have been employed as criteria within a more global test for the legality of an exercise of jurisdiction: whether there is "a substantial and bona fide connection between the subject-matter and the source of the jurisdiction."[29] Brownlie, among others, has posited that state jurisdiction over an extraterritorial act will be lawful where this primary criterion is met.[30] In a similar vein is the rule of jurisdictional "reasonableness," which is set out in the Restatement (Third) of U.S. Foreign Relations Law,[31] though the extent to which it reflects accepted international law principles is debatable.[32]

Given the state sovereignty concerns at play when actual enforcement of law is concerned, the rules regarding the exercise of enforcement jurisdiction are much more restrictive. As the Permanent Court of International Justice (PCIJ) wrote in the *Lotus* case, a state:

> . . . may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by

27. An approach which is grounded in the famous *Lotus* case. *See* SS "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A.) No. 10 (Sept. 7).

28. CEDRIC RYNGAERT, JURISDICTION IN INTERNATIONAL LAW 21 (2008).

29. BROWNLIE, *supra* note 18, at 309.

30. Also that in exercising jurisdiction, the state is not intervening in the domestic or territorial jurisdiction of another state, and that "elements of accommodation, mutuality, and proportionality" are applied. *Id.*

31. RESTATEMENT (THIRD) OF FOREIGN RELATIONS OF THE UNITED STATES § 403 (1987).

32. *See* Jordan Paust, *International Law Before the Supreme Court: A Mixed Record of Recognition,* 45 SANTA CLARA L. REV. 829, 845 (2005).

virtue of a permissive rule derived from international custom or from a convention.[33]

Accordingly, not only will states not enforce the public (particularly criminal) laws of other states,[34] but absent exceptional circumstances no state may enforce its own laws upon the territory of a second state absent some clear legal authorization to do so.[35] This extends to both investigative jurisdiction[36] (so, for example, the police of one state cannot investigate in another state without the latter's permission) and jurisdiction over the person (for example, the police of one cannot arrest an individual in another state, again without the latter's permission).[37]

These rules emerged from the criminal law stable, and as a result they are quite broad in scope and fairly permissive in nature. On the whole they are not well-developed, and certainly not as well-developed as rules relating to extraterritorial jurisdiction that have been developed by the courts of various states for use in their domestic legal systems.[38] Historically they have worked fairly well in the criminal law sphere, where the reasonably rare inter-state conflicts tended to be resolved via negotiation between prosecutorial authorities or governments; one does not see a surfeit of cases before the International Court of Justice regarding criminal jurisdiction.[39] However, they have worked less well for private law disputes. Certainly they are binding

33. SS "Lotus" (Fr. v. Turk.), 1927 P.C.I.J. (ser. A.) No. 10, at 18–19 (Sept. 7).

34. *See* The Antelope, 23 U.S. 66, 123 (1825) (opinion of Marshall, J.).

35. As the Supreme Court of Canada has written, "[t]he general rule that a state's criminal law applies only within its territory is particularly true of the legal procedures enacted to enforce it; the exercise of an enforcement jurisdiction is 'inherently territorial' . . . ." R. v. Terry, [1996] 2 S.C.R. 207, para. 17 (Can.).

36. In R. v. Hape, [2007] 2 S.C.R. 292 (Can.), the Supreme Court of Canada was dealing with a co-operative investigation between police officers of Canada and the Turks & Caicos, and identified "investigative jurisdiction" as a sub-principle of enforcement jurisdiction, involving "the ability of police or other government actors to investigate a matter." *Id.* para. 58 (citing Coughlan et al., *supra* note 7).

37. BROWNLIE, *supra* note 18, at 306; HIGGINS, *supra* note 17, at 70; JOHN DUGARD, INTERNATIONAL LAW: A SOUTH AFRICAN PERSPECTIVE 173 (2d ed., 2000).

38. Blakesley, *supra* note 26, at 94–95.

39. However, they are not unheard of. *See* Questions of Interpretation and Application of the 1971 Montreal Convention Arising from the Aerial Incident at Lockerbie (Libya v. U.S.), 1992 I.C.J. 3 (Apr. 14); Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.), 2002 I.C.J. 3 (Feb. 14); Questions Relating to the Obligation to Prosecute or Extradite (Belg. v. Sen.), 2009 I.C.J. 210 (time limits fixed July 9), *available at* http://www.icj-cij.org/docket/index.php?p1=3&p2=3&code=bs&case=144&k=5e.

upon all state exercises of jurisdiction in private international law, whether it be legislative, enforcement, or adjudicative. However, in private international law cases the interests presented are more economic than public order-oriented, and thus the major players reasonably desire and demand predictability.[40] As a result, national systems of private international law (or conflicts of law) are much more detailed and nuanced than the more indeterminate and malleable public international law rules,[41] in "recognition that civil jurisdiction is not merely an exercise of State power, but also a means of resolving private disputes."[42] Public international law principles have informed the growth and development of private international law principles, particularly in those areas where public law legislation is privately enforced, such as securities, anti-competition and intellectual property laws. There are also specific public international law treaties which facilitate inter-state cooperation in private law disputes, though these are more in the way of basic machinery[43] rather than assisting in jurisdictional selection. On the whole, however, most commentators note that there has been a commingling and confluence between the rules of jurisdiction as they apply purely to public matters and as they apply to private law matters,[44] particularly regarding the Internet.[45] Accordingly, we will discuss jurisdiction in various areas of substantive law throughout this paper, but always with an eye to their impact on the overall international law of jurisdiction.[46]

Another point to which we will return is that states often seek to

---

40. "The fundamental significance of jurisdiction is to enable the parties to foresee the extent of their liability and assess the legal and practical expense of defending a dispute in a particular jurisdiction." Lorna Gillies, *Addressing the 'Cyberspace Fallacy': Targeting the Jurisdiction of an Electronic Consumer Contract,* 16 INT'L J. L. & INFO. TECH. 242, 245 (2008) (citing ADRIAN BRIGGS, THE CONFLICT OF LAWS (2002)).

41. RYNGAERT, *supra* note 28, at 17.

42. Oren Bigos, *Jurisdiction Over Cross-Border Wrongs on the Internet,* 54 INT'L & COMP. L.Q. 585, 586 (2005).

43. *See, e.g.*, Hague Convention on the Service Abroad of Judicial and Extrajudicial Documents, Nov. 15, 1965, T.I.A.S. No. 6638, 20 U.S.T. 361, *available at* http://www.hcch.net/index_en.php?act=text.display&tid=44.

44. Christopher Kuner, *Data Protection Law and International Jurisdiction on the Internet (Part 1),* 18 INT'L J. LAW & INFO. TECH. 176, 183 (2010) (citing in particular ALEX MILLS, THE CONFLUENCE OF PUBLIC AND PRIVATE INTERNATIONAL LAW 298 (2009)).

45. KOHL, *supra* note 1, at 19.

46. It may also be worth noting that we are specifically trying to avoid the use of jurisdictional terminology which emerges from U.S. private international law jurisprudence, which is very popular in the literature—i.e. the concepts of "subject matter jurisdiction" or "personal jurisdiction." We avoid them because they have very specific meanings within that body of law, whereas we

manage the exercise of jurisdiction and head off disputes by concluding treaties, both bilateral and multilateral, on particular subject matters which contain obligations regarding the coordination of exercising jurisdiction. Again, the most prominent of these emerge from the criminal law field and are often referred to as the "suppression conventions,"[47] examples being the UN Convention on Transnational Organized Crime[48] and the Terrorist Bombing Convention.[49] These treaties typically provide that each state party will criminalize a particular act, exercise jurisdiction over it on a number of bases (including those set out above), and importantly will agree to the exercise of extraterritorial jurisdiction by other state parties over the relevant offences, even if a given state does not typically exercise such jurisdiction. States forestall conflicts and coordinate prosecutions in this way. The most important of these for present purposes is the European Cybercrime Convention,[50] which will be discussed in section IV, below.

D. *The Special Case of Qualified Territoriality*

Qualified territoriality, a subset of the territorial principle that developed in the criminal law field, accommodates a problem that is physically simple but legally immense in a legal system based on exclusive state sovereignty over territory: some acts, conduct, and transactions take place in the territory of more than one state. The classic international law textbook example is that of A, standing in state X, who fires a gun across a border into state Y, killing B. Clearly the entire crime of murder did not occur within a single state, so which state has jurisdiction to prosecute? In the modern day of transnational transactions and porous borders, this simple example has been supplanted by complex multi-state narcotics trafficking activities, money-laundering techniques that see funds running through ten banks in ten countries in as many minutes, and various kinds of terrorist acts.

Influential Anglo-American legal nomenclature describes "objective territoriality" (the act starts in one state but finishes in the forum state) and "subjective territoriality" (the offence begins in the forum state but

---

are discussing the overall international law. References to that terminology, if any, will be found only within specific discussions of U.S. private international law.

47. CURRIE, *supra* note 3, at 96–99.

48. Nov. 15, 2000, T.IA.S. No. 13127, 2225 U.N.T.S. 209.

49. Jan. 9, 1998, S. TREATY DOC. NO. 106-6, 37 I.L.M. 249.

50. Nov. 23, 2001, E.T.S. No. 185 [hereinafter Cybercrime Convention], *available at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

is completed elsewhere).[51] In antitrust law, the controversial "effects doctrine" has been asserted, imposing liability on individuals outside the United States whose activities have had economic impact within the U.S.[52] In the practice of some states, extraterritorial conspiracies can be prosecuted if any acts to complete them have been done within the foreign state,[53] or even if they have not.[54] Intriguingly, Mika Hayashi has observed that the differences between objective territoriality and the effects doctrine are disappearing in the Internet context, because the distinction between an act in one state and its effects in another state is increasingly a fine one.[55]

In any event, it is relatively clear that assertions of jurisdiction by states on the basis of qualified territoriality are uncontroversial where the act was launched in the state or where some harmful or otherwise significant effects stemming directly from the act are felt within the state. The central idea is that the forum state is asserting jurisdiction because something significant has been done on its territory, which can ground a claim that the act in question actually *happened there*. In such a case, the claim is one of territorial jurisdiction, and not extraterritorial jurisdiction. The latter would be at least slightly more controversial and involve the kinds of balancing discussed above. Qualified territoriality is an accepted jurisdictional principle in international law, even though its precise borders are vague.

The rise of the Internet has made these kinds of problems all the more acute, since a single Internet-based act may affect many jurisdictions, even simultaneously. Even as this paper was being written, a court in Minnesota heard the trial of a man charged with aiding and abetting the suicides of two people, one in Brampton, Ontario, Canada, and one in Coventry, England.[56] The evidence indicates that the accused trolled

---

51. CURRIE, *supra* note 3, at 62–64.

52. *Id.* at 64.

53. *See* D.P.P. v. Doot, [1973] A.C. 807 (H.L.) (appeal taken from Eng.) (U.K.).

54. Liangsiriprasert v. United States, [1991] 1 A.C. 225 (P.C.) 251 (appeal taken from H.K.) (U.K.); *see also* R. v. Bow St. Metro. Stipendiary Magistrate, *ex parte* Pinochet Ugarte (No. 3), [2000] 1 A.C. 147 (H.L.) 233 (Lord Hope of Craighead) (appeal taken from Eng.) (U.K.); Canada Criminal Code, R.S.C., 1985, c. C-46, § 465(4); United States v. Noriega, 746 F. Supp. 1506, 1515-19 (S.D. Fla. 1990).

55. Mika Hayashi, *The Information Revolution and the Rules of Jurisdiction in Public International Law*, *in* THE RESURGENCE OF THE STATE: TRENDS AND PROCESSES IN CYBERSPACE GOVERNMENT 59, 74–75 (Myriam Dunn et al. eds., 2007).

56. Amy Forliti, *U.S. Judge Hears Case Against Man Accused of Coaxing Canadian into Suicide*, GLOBE & MAIL (Feb. 24, 2011), http://www.theglobeandmail.com/news/world/americas/us-judge-hears-case-against-man-accused-of-coaxing-canadian-into-suicide/article1919228.

Internet chat rooms in search of vulnerable people contemplating suicide, and then counseled them as to techniques and success rates via online chats and e-mail. Assuming for the moment that the offence requires that an actual suicide took place, it is clear that that the entire crime did not take place in Minnesota, or indeed the U.S.; both Canada and the U.K. had claims to prosecute, based on both qualified territoriality and passive personality.

This is not to say that the qualified territorial principle is controversial, only to demonstrate that the criteria for its application are more easily met via the Internet than in perhaps any other setting on earth. This will be discussed further below.

E. *Distinguishing Extraterritorial Effect from Extraterritorial Jurisdiction*

As we have seen, jurisdictional conflicts can arise where more than one state is able to claim jurisdiction concurrently, which must mean that one or both claims has some extraterritorial element to it. A final but important distinction to be made is between an exercise of jurisdiction that may be properly said to be extraterritorial, and a domestic action that may have extraterritorial effects but is not an assertion of extraterritorial jurisdiction. As a matter of domestic policy, states may take actions that will have, or are even designed to have, extraterritorial effects of some kind, but cannot be said to be an exercise of extraterritorial jurisdiction.

For example, the European Union has put into place a ban on the importation of seal products from Canada, due to domestic distaste for the seal hunt.[57] This is simply a matter of closing borders to products which a state (or states) does not wish to have come into the country. As a matter of jurisdictional reach, it is a wholly domestic measure. Yet it is designed to have an impact outside the EU, specifically to pressure the Canadian government into ending or more assiduously regulating the seal hunt. Essentially, one domestic exercise of jurisdiction is being used in such a way as to convince another state to make a particular exercise of jurisdiction on its own. However, in our view this is more of a political tactic than a legal one. Were the EU to put in place directives that its member states pass laws purporting to regulate the Canadian seal hunt or prosecute Canadian sealers, that would be an exercise of extraterritorial jurisdiction (specifically legislative).

Another example of measures having extraterritorial effect is the

57. See *Trade in Seal Products*, EUR. COMMISSION (Mar. 11, 2011), http://ec.europa.eu/environment/biodiversity/animal_welfare/seals/seal_hunting.htm.

1995 passage of the EU Data Protection Directive,[58] which established norms for the protection of the processing of personal information of EU residents. One of the most controversial aspects of the Directive was the set of rules it established around the transfer of data for processing to a third country. Such transfers were only to be permitted where that country could ensure an "adequate" level of protection.[59] As a result of this Directive, third countries whose businesses wanted to continue to be able to process European data had to act to set data protection norms that would meet the standard of "adequate" as assessed by the EU. In the end a handful of countries, including Canada, Switzerland, and Argentina, enacted legislation that was found to meet the EU standards.[60] In the U.S., while new data protection legislation was not forthcoming, a "safe harbor" agreement was negotiated which permitted U.S. companies to qualify as "safe harbors" for EU data so long as they met certain standards for the processing of data.[61] Although there was nothing explicitly extraterritorial about the EU Data Protection Directive, it nevertheless had extraterritorial effect, as it compelled foreign governments either to enact new laws or to negotiate new agreements.

III. Challenges Posed by the Internet: Traditional Norms Under Stress

A. *Technology and Globalization*

The Westphalian concept of exclusive territorial sovereignty discussed above is based on notions of control over a defined territory. This ability to control activities within a physically defined space is

58. Directive 95/46/EC, of the European Parliament and of the Council of 23 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

59. *Id.* art. 25.

60. Lilian Edwards, *Privacy and Data Protection Online: The Laws Don't Work?*, *in* Law and Internet 443, 454 (Lilian Edwards & Charlotte Waelde eds., 3rd ed. 2009).

61. Note that an EU review of safe harbour was generally dissatisfied with the level of protection offered. *See Implementation of Commission Decision 520/2000/EC on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce*, SEC (2004) 1323 final (Oct. 20, 2004), http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf. Edwards notes that data processing outside the EU in non-approved countries may still take place if the data subject consents, or if special contractual clauses are in place. She observes that the use of contractual terms in the export of data for processing is increasingly common. Edwards, *supra* note 60, at 455.

increasingly under challenge both from globalization writ large, and by technological innovations including the Internet. Taubman writes:

> The concept of sovereignty is dependent on territoriality, precisely because it concerns absolute or predominant authority of the sovereign powers within the territory of the state, exclusion of external authority and comity between states. Conventional notions of sovereignty are therefore dependent on the integrity of the capacity to exercise control within a well-defined territory.[62]

As both the definitions of territory and the capacity to exercise control are undermined,[63] traditional notions of territoriality and territorial sovereignty come under pressure. In this section we consider how the phenomena of globalization and the Internet are stressing and stretching conventional notions of territorial sovereignty.

Globalization has been identified by many as posing significant challenges to notions of territorial sovereignty.[64] Sassen argues that the concept of globalization reflects two different dynamics. The first involves the development of institutions or processes that are global in nature—supranational organizations and tribunals, for example.[65] The second dynamic involves a more organic set of processes at both the state and the non-state level. Sassen gives as examples the formation of "monetary and fiscal policies critical to the constitution of global markets,"[66] and the formation of networks of activists across borders. At the institutional or governance level we see new international and supranational organizations and the drive to harmonize legal norms and processes. In terms of the dynamics of change, we see far greater mobility of persons and of capital. There is a dramatic increase in trade

62. Antony Taubman, *International Governance and the Internet*, *in* LAW AND INTERNET, *supra* note 60, at 3, 27.

63. Notions of "territory" are undermined, for example, by the increasing engagement of a country's citizens in a wide range of activities that are carried out in "cyberspace." This in turn undermines the capacity of states to control citizen activity.

64. *See, e.g.*, STEPHEN CLARKSON & STEPAN WOOD, A PERILOUS IMBALANCE: THE GLOBALIZATION OF CANADIAN LAW AND GOVERNANCE (2010); SASKIA SASSEN, TERRITORY, AUTHORITY, RIGHTS: FROM MEDIEVAL TO GLOBAL ASSEMBLAGES (2d ed. 2006) [hereinafter SASSEN, TERRITORY]; Chris Brown, *Reimagining International Society and Global Community*, *in* GLOBALIZATION THEORY 171 (David Held & Andrew McGrew eds., 2007).

65. Saskia Sassen, *The Places and Spaces of the Global: An Expanded Analytic Terrain*, *in* GLOBALIZATION THEORY, *supra* note 64, at 79, 82.

66. *Id.*

of a global nature, including a shift in the locus of manufacturing and production. There is increasing convergence of corporate ownership, a rise in multinational corporations (often exercising significant normative power in their own right), and an increasing globalization of culture and communications.[67] All of these changes necessarily have an impact on how states exercise their jurisdiction.

At the same time, concurrent with, and often facilitating these institutional and dynamic changes,[68] we have seen breathtaking technological development. Innovations in biotechnology transform health and agriculture into industries with global economic, legal, and political dimensions. Knowledge economies breed globalized workforces, and radical transformations of communications technologies change how people interact, communicate, collaborate, and network.[69] They also change how culture is formed and communicated.[70] The Internet is perhaps the most important of these innovations in communications —not simply because of the underlying technology, but because of the way in which this technology has given rise to its own unique governance issues.

Technology facilitates the mobility of goods and persons to an extent previously inconceivable; it facilitates instantaneous and global communication, as well as new forms of creative and cultural endeavor. Nevertheless, technology—including the Internet—is only one part of the phenomenon of globalization and the stresses placed on notions of territorial sovereignty. As Taubman writes: "The classical notion of sovereignty was already under threat, well before the advent of mass Internet usage, in a direct practical sense because of the rise of global

67. David Held & Anthony McGrew, *Globalization at Risk?*, *in* GLOBALIZATION THEORY, *supra* note 64, at 1, 4.

68. Held, for example, argues that the changing infrastructure of global communications is a driver of globalization. *See* David Held, *Global Governance: Apocalypse Soon or Reform!*, *in* GLOBALIZATION THEORY, *supra* note 64, at 240, 243.

69. *See generally* CASS SUNSTEIN, INFOTOPIA: HOW MANY MINDS PRODUCE KNOWLEDGE (2006); YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM (2006).

70. There is a vast literature on this subject. We note in particular that much has been written from a copyright perspective on the impact of contemporary forces on the creation and sharing of cultural works protected by copyright. *See, e.g.*, LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (2002); KEMBREW MCLEOD, FREEDOM OF EXPRESSION: OVERZEALOUS COPYRIGHT BOZOS AND OTHER ENEMIES OF CREATIVITY (2005); BENKLER, *supra* note 69, at 59 (discussing the proliferation of non-market cultural production).

business patterns and globalized communication and cultural exchanges; as well as from a theoretical perspective."[71]

Within this broader global context, therefore, the Internet is but a case study. The Internet is both the subject of new international governance frameworks, the object of increasingly harmonized state norms regarding infrastructure and conduct, and a venue by which individuals shape and form alliances and movements that transcend national boundaries. It is a case study of the challenges to the Westphalian concept of territorial state jurisdiction, and of the ways in which states continue to define or redefine their territorial boundaries and find new ways to act within them.

B. *The Internet*

In the heady, early days of the Internet, it was seen by many as a lawless place free from the restraints of national laws.[72] That period was relatively transient, and few would share such a utopian/dystopian[73] view today.[74] Perhaps part of the perceived lawless nature of the Internet was the fact that it did not seem, at the outset, controlled by national governments.[75] The relationships between national governments and the Internet are now increasingly clear. Sassen notes that a certain degree of control over the Internet is achieved through "governmental authority through technical and operational standard setting

---

71. Taubman, *supra* note 62, at 27.

72. *See e.g.*, Alfred C. Yen, *Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 BERKELEY TECH. L.J. 1207 (2002); John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND., https://projects.eff.org/barlow/Declaration-Final.html (last visited June 14, 2011); David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN L. REV. 1367 (1996). *But see* Daniel C. Menthe, *Jurisdiction in Cyberspace: A Theory of International Spaces*, 4 MICH. TELECOMM. & TECH L. REV. 69 (1998) (arguing that rather than a truly lawless sphere, the Internet was akin to a common or shared space, like the high seas, and therefore subject to regulation in international law).

73. It could be considered either utopian or dystopian, depending on your perspective. Although many considered the unregulated nature of cyberspace to be a positive value, it quickly became clear that cyberspace could be a place of abuse, harassment, exclusion and other anti-social activities.

74. Note that at least one more contemporary author has argued that these earlier ideas might be worth revisiting at least in some limited respects. *See* Dan Jerker B. Svantesson, *Borders On, or Borders Around—The Future of the Internet*, 16 ALB. L.J. SCI. & TECH 343 (2006).

75. Milton Mueller is critical of this perspective, noting that right from its inception, the Internet implicated a growing number of national governments that "for decades if not centuries engaged in power games over resources and strategic advantage and tended to view Internet governance from within that framework." MILTON L. MUELLER, NETWORKS AND STATES: THE GLOBAL POLITICS OF INTERNET GOVERNANCE 3 (2010).

for both hardware and software."[76] As outlined below, states can and do act, through their various branches, in relation to Internet-based activity. In considering state jurisdiction and the Internet it is important to keep in mind three key dimensions. These relate to infrastructure governance issues, normative ordering for the Internet, and the reach of domestic laws onto the Internet.

The first dimension, that of infrastructure governance issues, turns on the unique distributed nature of the Internet. The Internet represents a complex decentralized and distributed infrastructure which nevertheless depends on certain norms and technological standards for its operation.[77] Internet protocol (IP) addresses are required to facilitate communications and these must be assigned and managed; further, to make the Internet user-friendly, there must be a system for cross-referencing numeric IP addresses with human-readable domain names.[78] The domain name system must in turn be one that manages, somehow, to balance competition for name resources as well as unfair competition in attempts to appropriate and misuse the trademarks or names of companies and individuals.[79] All of this requires governance bodies, and these have emerged, not without controversy, at the international level.[80] Mueller notes that the very nature of Internet protocols "decentralized and distributed participation in and authority over networking and ensured that the decision-making units over network operations are no longer closely aligned with political units."[81]

The primary Internet governance institution is the Internet Corporation for Assigned Names and Numbers (ICANN).[82] This "not for profit public benefit corporation"[83] was formed in October 1998 as the

76. TERRITORY, *supra* note 64, at 331.

77. Taubman, *supra* note 62, at 6; MUELLER, *supra* note 75, at 8–9.

78. Caroline Wilson, *Domain Names and Trade Marks: An Uncomfortable Interrelationship*, *in* LAW AND INTERNET, *supra* note 60, at 311, 313–16; Sheldon Burshtein, DOMAIN NAMES AND INTERNET TRADE-MARK ISSUES: CANADIAN LAW AND PRACTICE 2–6 (2006).

79. *See generally* Laurence R. Helfer & Graeme B. Dinwoodie, *Designing Non-National Systems: The Case Of The Uniform Domain Name Dispute Resolution Policy*, 43 WM. & MARY L. REV. 141, 154–57 (2001); Julia Hörnle, *The Uniform Domain Name Dispute Resolution Procedure: Is Too Much of a Good Thing a Bad Thing?*, 11 SMU SCI. & TECH. L. REV. 253 (2008).

80. MUELLER, *supra* note 75, at 4 (giving the examples of the Internet Engineering Task Force (IETF), the Regional Internet Address Registries, and ICANN as examples of decision-making bodies outside state structures that control key aspects of Internet infrastructure).

81. *Id.* at 4.

82. ICANN, http://www.icann.org (last visited May 3, 2011).

83. *About,* ICANN, http://www.icann.org/en/about (last visited May 3, 2011).

oversight body for domain name registrations.[84] It replaced a private sector company that was under contract with the U.S. government's National Science Foundation. ICANN's 21-member Board of Directors reflects its international constituency. ICANN has also developed a governance structure[85] that aims to involve a variety of stakeholders. Its primary role is to manage the "technical coordination, technical management and operational stability of the Internet."[86] ICANN is interesting in that it is a private corporation that performs extremely important Internet oversight functions—in this sense it could be characterized as a new international governance model.[87] The model is not without controversy.[88]

ICANN is an illustration of one of the ways in which Internet governance depends only in part on traditional normative law-making. ICANN's governance role is oriented towards technical standards and operational management of Internet infrastructure. The importance of the choices made in this respect, however, go beyond mere technical matters. Indeed, Lessig maintains that the Internet is regulated by code, i.e., by software and hardware.[89] Technical norms and specifications, their evolution, and the laws that constrain them, become part of the architecture of cyberspace that may limit and constrain it. In this

84. ICANN is a non-profit corporation incorporated under the laws of California, and with its headquarters in that state. *Bylaws*, ICANN, http://www.icann.org/en/general/bylaws (last visited May 3, 2011).

85. *Structure*, ICANN, http://www.icann.org/en/structure (last visited May 3, 2011).

86. World Intellectual Prop. Org., *The Recognition of Rights and the Use of Names in the Internet Domain System: Report of the Second WIPO Internet Domain Name Process*, ¶ 75 (2001), *available at* http://www.wipo.int/amc/en/processes/process2/report/html/report.html.

87. DelBianco and Cox argue that ICANN should be thought of as "the Internet's manager—not as its governor." Steve DelBianco & Braden Cox, *ICANN Internet Governance: Is it Working?*, 21 PAC. MCGEORGE GLOBAL BUS. & DEV. L.J. 27, 28 (2008). However, this does not stop ICANN from being considered a governance body, and from generating international debate over its composition and its role.

88. *See, e.g.*, MUELLER, *supra* note 75, at 10–11; SASSEN, TERRITORY, *supra* note 64, at 333; COMM. ON INTERNET NAVIGATION & THE DOMAIN NAME SYS., SIGNPOSTS IN CYBERSPACE: THE DOMAIN NAME SYSTEM AND INTERNET NAVIGATION 187–280 (2005), *available at* http://www.nap.edu/openbook.php?record_id=11258&page=R1; John Palfrey, *The End of the Experiment: How ICANN's Foray into Global Internet Democracy Failed*, 17 HARV. J. LAW & TECH. 409 (2004); Jay P. Kesan & Andres A. Gallo, *Pondering the Politics of Private Procedures: The Case of ICANN*, 4 J.L. & POL'Y FOR INFO. SOC'Y 345 (2008); DelBianco & Cox, *supra* note 87, at 39–40.

89. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 6 (1999) [hereinafter LESSIG, CODE].

context, states play a normative role, but so do private actors—those who control the code and architecture.[90]

The governance role of ICANN is fairly unique in international law, and has come under challenge by national governments that would prefer control over the infrastructure of the Internet in the hands of a more conventional international organization.[91] The World Summit on the Information Society, a global United Nations summit initiated in 2002 and which concluded in 2005, was the locus of significant challenges to ICANN's role in Internet governance.[92] Part of the reaction was to the perceived hegemony of the United States, as it had transferred its authority over Internet governance to ICANN, an entity incorporated under the laws of California.[93] Mueller argues that the resistance to ICANN went deeper. He describes ICANN's institutional design as one that "marked a revolutionary departure from traditional approaches to global governance."[94] As ICANN managed issues that were central to communication and information policy, it was radical indeed to have the locus of decision-making situated outside the nation-state and outside traditional international organizations.[95]

Thus ICANN is a novel governance structure not just because it is a

---

90. *Id. See generally* Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1998).

91. The threats to ICANN at the international level are discussed in DelBianco & Cox, *supra* note 87, at 39–40.

92. Although WSIS did not manage to displace ICANN, it did result in the establishment of the Internet Governance Forum (IGF). Although the IGF is more explicitly international than ICANN, it is still a novel international institution because of its structure. IGF places government representatives "on roughly equal terms with civil society and business participants." MUELLER, *supra* note 75, at 107. Indeed, it describes itself as "a new forum for multi-stakeholder policy dialogue." *About the Internet Governance Forum*, INTERNET GOVERNANCE F. ONLINE, http://www.intgovforum.org/cms/aboutigf (last visited June 16, 2011).

93. MUELLER, *supra* note 75, at 59; *see also* DelBianco & Cox, *supra* note 87, at 41–43 (highlighting a number of examples of the often heavy American influence in Domain Name Server (DNS) policy decision making).

94. MUELLER, *supra* note 75 at 60–61.

95. Under ICANN's articles of incorporation, government representatives may not sit on its board. Note that DelBianco and Cox, *supra* note 87 at 29, argue that if an intergovernmental body were to take over the functions of ICANN, its ability to act effectively to regulate Internet infrastructure would be diminished. They write: "Quarreling nations would find it impossible to agree on anything but the most trivial technical decisions. Developing nations would press for changes in Internet management to advance their economic development goals. Special interests would seek Internet-enabled social programs to address perceived disadvantages." *Id.* Perhaps ironically, in advancing their reasons why states should not involve themselves in the management of Internet infrastructure, the authors seem to be saying that it is because they would act like governments.

not-for-profit corporation not controlled by national governments, but also because the infrastructure it governs does not lend itself to control at the state level. Nevertheless, given the global importance of the Internet, it is not surprising that there is strong interest at the state level in the ability to participate in Internet governance.[96] Whether proprietary or open standards are adopted, what top-level domains are available for domain name registration and by whom, are important questions. The ability to control the infrastructure of the Internet is a matter of great state interest. Governance issues therefore represent a critical dimension with respect to state sovereignty.[97]

Sassen notes that the technological standards and infrastructure of the Internet offer a vehicle for state exercise of authority. Not only can states play a role in establishing technological standards and regulating infrastructure, their doing so can have wide-ranging effect.[98] Thus, while supranational governance issues are one dimension of the impact of the Internet on state jurisdiction, the ability of the state to exercise authority through control over technology and infrastructure remains important. Indeed, the recent examples of states limiting Internet access as a means of suppressing dissent are illustrations of this.[99] The

---

96. This is evident in the resistance to ICANN's role, as manifested at the World Summit on the Information Society, World Summit on the Information Society, Dec. 10–12, 2003, *Geneva Declaration of Principles, Building the Information Society: A Global Challenge in the New Millennium*, WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003) [hereinafter World Summit], *available at* http://www.itu.int/wsis/docs/geneva/official/dop.html.

97. Taubman, *supra* note 62 at 7 (noting that although the U.S. has tended to favour a private sector based approach to Internet governance structures, other governments have sought to play a more active role). Taubman writes that the economic, political and cultural impact of the Internet has raised "concerns that are reflected in a debate over whether the Internet should be governed through genuinely international structures with distinct legal personality and under international law, or whether the legal roots of the Internet should remain embedded in the fertile soil from where it was first cultivated, in the domestic jurisdiction of the US." *Id.*

98. Note for example, the recent furor around Internet usage-billing in Canada. The federal telecommunications regulator had issued a decision that would permit major telecommunications companies to impose usage-based billing on smaller ISPs. The decision was sent back for reconsideration by the federal government. In addition, the Minister of Industry made it clear that if the CRTC did not reverse its ruling, the government would do so. *See* Susan Krashinsky, *CRTC's Internet Decision 'Simply Wrong' Clement Says*, GLOBE & MAIL (Mar. 1, 2011, 7:56 PM), http://www.theglobeandmail.com/news/technology/tech-news/crtcs-internet-decision-simply-wrong-clement-says/article1925948/. Svantesson also argues that the technology to erect "borders" in cyberspace has evolved sufficiently to permit effective 'zoning' of the Internet. *See* Svantesson, *supra* note 74 at 353.

99. *See, e.g.*, JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 113 (2008) [hereinafter ZITTRAIN, FUTURE]; Jonathan Zittrain & Benjamin Edelman, *Documentation of Internet Filtering in Saudi Arabia*, BERKMAN CENTER FOR INTERNET & SOC'Y, HARV. L. SCH. (2002), http://

pressure brought to bear on Google by the government of China, for example, illustrates the normative power of technology, and the reality of private control over key aspects of "code" in cyberspace.[100] The example partially illustrates Lessig's view that law can operate in two different ways in relation to the Internet. Lessig argued that law can regulate the conduct of individuals by setting norms and imposing sanctions for non-compliance. It can also regulate the 'architecture' of the Internet, and in so doing, subtly change how people may act and interact.[101] In the case of services like Google, it is not the Internet itself that is the subject of regulation, but rather a popular Internet search tool. The fact that the tool belongs to and can be controlled by its corporate owner makes state-imposed limitations on its operations far more effective than broader attempts to control the Internet.[102] In general terms, though, the principle is the same. A state may choose to regulate the conduct of its citizens directly through law, or it may choose to limit the architecture of the Internet or its services in such a way that some forms of conduct are de facto restricted.

The second dimension is governance-related, but rather than focusing on institutions of governance, it focuses on norms. Increasingly, states participate in international treaty-making that aims to set norms regarding the conduct of all manner of Internet-based activity, includ-

---

cyber.law.harvard.edu/filtering/saudiarabia/. Kohl discussed the willingness of some corporations to create country-specific sites to address state censorship requirements. *See* KOHL, *supra* note 1 at 29.

100. Zittrain notes that because Google's service operates from a fixed technical layer, there is no way for users to find their way around technological restrictions. As a result, Google's cooperation with the Chinese government to censor certain terms is highly effective. ZITTRAIN, FUTURE, *supra* note 99, at 113. Zittrain gives similar examples of agreements between the Chinese government and Skype and MSN Spaces regarding the censorship of certain terms. *Id.*

101. *See* LESSIG, CODE, *supra* note 89 at 93. In a recent French case, the Paris Court of Appeal held that Google was not responsible for breach of copyright when searchers used Google to obtain copies of publicly accessible but copyrighted images. *See* Cour d'appel [CA] [regional court of appeal] Paris, 1e ch., Jan. 26, 2011, R.G. n° 08/13423, *available at* http://www.juriscom.net/documents/caparis20110126.pdf. The court remarked in passing that, if the content owners did not want to have their images found through Google, they could use readily-available software (presumably robot.txt) to turn away Google's web crawlers so the sites would not be indexed. *Id.*

102. Zittrain cautions that "[t]echnologies that lend themselves to an easy and tightly coupled expression of governmental power simply will be portable from one society to the next." ZITTRAIN, FUTURE, *supra* note 99 at 113; *see also* Thomas Schultz, *Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface*, 19 EUR. J. INT'L L. 799, 825 (2008).

ing electronic commerce,[103] the downloading of copyright protected works,[104] child pornography and "child sex tourism,"[105] organized crime,[106] and terrorism.[107] These treaties may be normative (setting standards for what is legal or illegal conduct),[108] they may be process-oriented (setting standards for national administrative and legal processes to deal with issues),[109] or they may be investigation- or enforcement-oriented (designing mechanisms for inter-state cooperation on investigations and prosecutions).[110] Essentially, however, the challenges posed by the Internet are bringing states together to set norms for conduct on the Internet and to provide means of redress for offensive conduct typically through increasingly harmonized national laws. Of course, the code element should not be forgotten. Some of these international treaties specifically require technical infrastructure to facilitate surveillance

103. Through UNCITRAL, an international working group has attempted to harmonize norms relating to electronic commerce. Although the main product of these negations has been a model law, rather than a treaty, the process (along with ongoing working group meetings to refine norms and harmonize laws) is an attempt to reach an international consensus around issues in the area. *See* UNCITRAL, MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT, Sales No. E.99.V.4 (1996), *available at* http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf.

104. *See, e.g.*, World Intellectual Property Organization [WIPO], WIPO Copyright Treaty art. 5, Dec. 20, 1996, 112 Stat. 2860, 36 I.L.M. 65, *available at* http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html [hereinafter WCT]. The finalized text of the Anti-Counterfeiting Trade Agreement also contains provisions in Art. 2.18 relating to enforcement of intellectual property rights in the digital environment. *See* Anti-Counterfeiting Trade Agreement art. 2.18, Nov. 15, 2010, *available at* http://www.ustr.gov/webfm_send/2379 [hereinafter ACTA] (relating to enforcement of intellectual property rights in the digital environment) (text finalized but not yet open for signature).

105. Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, 2171 U.N.T.S. 227.

106. UN Convention on Transnational Organized Crime, *supra* note 48.

107. There are thirteen international counter-terrorism treaties, to say nothing of regional treaties and the nascent UN efforts to draft a comprehensive international treaty defining terrorism. *See* CURRIE, *supra* note 3, at 295–301, 343–70.

108. WCT, *supra* note 105, art. 12, for example, sets new copyright norms to be applicable in the case of copyright works on the Internet.

109. The ACTA, *supra* note 105, is very much process- and enforcement-oriented.

110. The Cybercrime Convention contains an extensive number of provisions dealing with mechanisms of investigation and enforcement of crimes, which are discussed further *infra* section 4. Note that while the *Cybercrime Convention* addresses criminal conduct that crosses borders through the vehicle of the Internet, the treaty is premised upon empowering states to take actions to respond to threats or harms within their own borders. *See* Susan W. Brenner, *The Council of Europe's Convention on Cybercrime*, *in* CYBERCRIME: DIGITAL COPS IN A NETWORKED ENVIRONMENT 207, 210 (Jack M. Balkin et al. eds., 2007).

and enforcement,[111] or other technological protection measures that can limit infringement, aid in detection, and permit tracking, monitoring or metering.[112] Lessig argues that cyberspace actually expands the range of tools available to governments to regulate. He writes: "by regulating code writing, the government can achieve regulatory ends, often without suffering the political consequences that the same ends, pursued directly, would yield."[113]

A distinct but related aspect of the development of consensus around new norms for the Internet relates to an emerging vision of the Internet itself as a fundamental vehicle for human rights—such that one might even speak of a right of access to the Internet. Taubman argues that there has been a growth in the number of international norms that reference the Internet as it increasingly becomes viewed as essential to goals of development, democracy, and human rights.[114] The Internet is becoming a key vehicle for education, the communication of knowledge, access to information, interpersonal communication, democratic participation, and freedom of expression. These are all values that are recognized in international law and most have the status of fundamental rights to some extent.[115] It is possible that access to the Internet may evolve into a freestanding human right because of its importance in democratic participation, self-expression, education, the dissemination of knowledge, and in

111. For example, the Cybercrime Convention address technological and infrastructure needs in relation to cybercrime. Brenner notes that the measures were incorporated to deal with the particularly fragile nature of digital evidence. *Id.* at 213.

112. The WCT, *supra* note 105, does not specifically require technical protection measures, nor does it set standards for such measures. However, it does require states to provide recourse against those who interfere with TPMs that are applied to copyright works. *Id.* art. 11. The Cybercrime Convention does contain provisions that relate to evidence gathering, surveillance and monitoring. Brenner notes that, controversially, these provisions apply not just to crimes identified as cybercrimes, but to any crime in which electronic evidence is a factor. Brenner, *supra* note 110 at 213. Lessig notes how some of the objectives of the regulator (state) can be achieved by changing technological architecture. LESSIG, CODE, *supra* note 90, at 99.

113. LESSIG, CODE, *supra* note 90 at 99. Schultz, *supra* note 102 at 802, argues that the laws of technology (code) permitted the structuring and regulation of cyberspace. He notes: "It has been shown that the Internet could be a place of exquisite control just as it used to be a place of exquisite liberty." *Id.*

114. Taubman, *supra* note 62 at 8–9. The central role of the Internet in achieving goals of education, social justice, and health was set out in the *Geneva Declaration of Principles* as part of the World Summit on the Information Society. *See* World Summit, *supra* note 96.

115. *See generally* Kindred, *supra* note 14 at 835–920. Regarding freedom of expression, see CTR. FOR DEMOCRACY & TECH., REGARDLESS OF FRONTIERS: THE INTERNATIONAL RIGHT TO FREEDOM OF EXPRESSION IN THE DIGITAL AGE (2011), *available at* http://www.cdt.org/files/pdfs/CDT-Regardless_of_Frontiers_v0.5.pdf.

other core expressive activities.[116]

The extent to which the Internet is important to democracy and human rights is only underlined by recent attempts to shut down the Internet in Iran, and during the period of unrest in Egypt leading up to the removal of Mubarak as president.[117] The Internet is greater than any individual state; it is impossible to control or suppress entirely.[118] This then is one of the central international aspects of normative ordering for the Internet. Access to the Internet is acquiring status in international law as an essential human right, and at the same time, models of governance of the physical infrastructure of the Internet are emerging.

In a third dimension, the Internet becomes an extension of each state's territory in which it may exercise its traditional sovereign jurisdiction. A state may do so through laws that seek to govern the activity of its citizens in the online environment, or through the interpretation and application of its laws to Internet-based conduct that it considers sufficiently linked to its territory. A state may also seek to impose technological limitations on Internet actors to limit citizen access to various online services. It may seek to impose these limits

116. The issue of Internet access as a human right was raised at the UN Administrative Committee on Coordination and at the 2003 World Summit on the Information Society. World Summit, *supra* note 96. France's Constitutional Court recently ruled that Internet access is, indeed, a human right when reveiwing France's new Internet copyright law. Conseil constitutionnel [CC] [Constitutional Court] decision No. 2009-580DC, June 10, 2009, Rec. 107, 110 (Fr.). *See also* Charles Bremner, *Top French Court Rips Heart Out of Sarkozy Internet Law*, SUNDAY TIMES (June 11, 2009), http://technology.timesonline.co.uk/tol/news/tech_and_web/article6478542.ece. Other countries' legislatures have explicitly declared access a fundamental right. *See* Dana Lungescu, *Tiny Estonia Leads Internet Revolution*, BBC NEWS (Apr. 7, 2004), http://news.bbc.co.uk/2/hi/europe/3603943.stm; Bobbie Johnson, *Finland Makes Broadband Access a Legal Right*, GUARDIAN (Oct. 14, 2009), http://www.guardian.co.uk/technology/2009/oct/14/finland-broadband. Finally, in a poll conducted by the BBC, 4 in 5 respondents from around the world shared the view that Internet access is a fundamental human right. *Internet Access is a Fundamental Human Right*, BBC NEWS (Mar. 8, 2010), http://news.bbc.co.uk/2/hi/technology/8548190.stm.

117. Matt Richtel, *Egypt Cuts Off Most Internet and Cell Service*, N.Y. TIMES, January 28, 2011, http://www.nytimes.com/2011/01/29/technology/internet/29cutoff.html; Larry Greenemeier, *How Was Egypt's Internet Access Shut Off?*, SCI. AM. (January 28, 2011), http://www.scientificamerican.com/article.cfm?id=egypt-internet-mubarak. There are other incidents as well where national governments have shut off Internet access in an attempt to quell unrest. *See, e.g.*, Ali Akbar Dareini, *Iran Blocks Internet on Eve of Rallies*, CBS NEWS WORLD (Dec. 6, 2009), http://www.cbsnews.com/stories/2009/12/06/world/main5915334.shtml; OPENNET INITIATIVE, WEST CENSORING EAST: THE USE OF WESTERN TECHNOLOGIES BY MIDDLE EAST CENSORS 2010–11 (2011), *available at* http://opennet.net/sites/opennet.net/files/ONI_WestCensoringEast.pdf.

118. *See* BENKLER, *supra* note 69 at 268–69.

through negotiation or ultimatums;[119] it may also do so through legal action.[120]

IV. State Jurisdiction over Internet-Based Activities

In the first part of this paper we referred to the emerging international principle of "qualified territoriality." This principle applies where an action or conduct which crosses national borders can be said to have sufficient connections to a state for that state to consider the act to have taken place substantially within its territorial jurisdiction. The principle of qualified territoriality is of some usefulness in the Internet context. Nations around the world have faced the challenge of addressing Internet-based activities. They do so as activity normally within their sphere of authority moves into online forms (the migration of commerce to the Internet, for example). They also do so as the Internet embraces roles previously played by heavily regulated industries such as telecommunications and broadcasting. Civil wrongs also find their way onto the Internet: defamation and infringement of copyright or trademarks serve as examples. Many forms of criminal conduct have also migrated to the Internet (illicit gambling, distribution of child pornography, and fraud, to give but a few examples). States also react to other crimes and threats to national security posed by the Internet, such as hacking, malware, the sabotage of systems and networks, and the use of the Internet by terrorist and criminal organizations.[121] In all of these

119. For example, the Indian government gave RIM, the maker of the Blackberry handheld device, an ultimatum requiring it to allow the Indian government access to data and email transmitted over its system or face a ban on operations in India. The Indian government expressed security concerns over the use of such devices to aid in terrorist acts, following the terrorist bombing in Mumbai. Both the United Arab Emirates and Saudi Arabia were reported to be seeking similar compliance by RIM. *See* Josh Halliday & Graeme Wearden, *India Sets Deadline for Blackberry Compliance*, Guardian, Aug. 12, 2010, http://www.guardian.co.uk/technology/2010/aug/12/blackberry-email-messaging-india.

120. An example of this is perhaps the investigation by Canada's Privacy Commissioner of Facebook's privacy practices. The Commissioner found that Facebook had violated a number of provisions of Canada's Personal Information Protection Act, S.C. 2000, c. 5. The next step would have been to take Facebook to court for a judicial ruling on the issue of breach. However, Facebook sought to reach a compromise with the Privacy Commissioner by changing or adapting some of its policies. See *infra* part IV; *cf.* Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, May 22, 2000, D. 2000 inf. rap. 172, obs. J. Gomez (Fr.), *available at:* http://www.juriscom.net/txt/jurisfr/cti/yauctions20000522.htm (ordering measures be taken to limit the access of French citizens to certain content on Yahoo!).

121. *See, e.g.*, Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474; 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C. § 1030 (2006)); Uniting and Strengthening America by

contexts, states assert the jurisdiction they have always asserted over similar activities within their borders. The difference is, of course, that these activities are no longer confined to their borders. The harmful conduct may originate outside national boundaries, or it may originate inside the country but be targeted elsewhere. States that act through an exercise of legislative, executive, or judicial authority act territorially in one sense, but their actions often have extraterritorial effects or dimensions. As Held writes, "developments at the local level—whether economic, political or social—can acquire almost instantaneous global consequences and vice versa."[122]

There is a distinction, therefore, between the second dimension discussed above, where states collaborate to set new norms to govern conduct that spans borders, and this third dimension of the problem where a state must decide whether conduct has taken place substantially within its territorial jurisdiction and is thus subject to its laws. The principle of qualified territoriality is of some use in legitimating such exercises of state jurisdiction, but it is not always easy to negotiate the boundary between traditional notions of territorial (however qualified) and extraterritorial action. In section II of this paper, we distinguished between assertions of extraterritorial jurisdiction, which ran the risk of infringing the sovereignty of other states, and domestic acts with extraterritorial effects, which generally did not. This traditional distinction is becoming blurred. If territorial action increasingly has extraterritorial effect, what is the level of impact or effect that warrants characterizing an act as extraterritorial? Is extraterritorial effect now a routine by-product of territorial action, and if so, does this embolden states to take actions within their territories that have explicit extraterritorial consequences? Clearly the notion of comity has some limiting power here, but the challenges are real.

Most discussions of state jurisdiction in the context of the Internet have focused on the exercise of adjudicative jurisdiction by the courts. While this is an important area of concern, it nevertheless offers an incomplete picture of the complexity surrounding state jurisdiction in the Internet context. In this part of the paper, adjudicative jurisdiction is considered alongside the numerous other ways in which governments exercise their territorial jurisdiction (often with extraterritorial effect) on the Internet.

Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

122. Held, *supra* note 68, at 243.

A. *Qualified Territoriality and the Courts*

It is often left to judges to decide whether a matter brought before them legitimately falls within their adjudicative jurisdiction. With the increasing frequency of Internet-based matters coming before both criminal and civil courts, we see courts struggling to come to terms with how to articulate the boundaries of their jurisdiction in a manner that is respectful of the principles of territoriality and comity.

In addressing issues around jurisdiction, courts have considered whether there is jurisdiction over both subject matter (the dispute, the act, the crime) and jurisdiction over the parties involved. Increasingly, these considerations are merged into a more globalized assessment of whether there is something like what the Supreme Court of Canada has called a "real and substantial connection" to the jurisdiction.[123] This test accepts that the Internet may present various points of connection, but it measures the strength of these connections in order to avoid an inappropriate assertion of jurisdiction.

Subject matter jurisdiction relates to the court's authority over the subject matter of the dispute. To use an illustration from the intellectual property context, jurisdiction over copyright matters is purely national in scope.[124] Thus, to have jurisdiction over a copyright dispute, the alleged act of infringement must have taken place within the country in which the court is located. There is no jurisdiction over acts that have not taken place within the country. Thus an author whose book is copied by an American citizen in the UK cannot sue for infringement in the U.S. The lawsuit must be brought in the UK under British law. Where there is no subject matter jurisdiction, a court will not hear a case. The principles are the same in the Internet context, though their application is more challenging as the locus of an act of infringement that takes place over the Internet may be more difficult to determine. The principles of subject matter jurisdiction and of national treatment between states established under international treaties remain constant; it is the relationship of the acts to state 'territory' that are contested.

With some types of activity, territorial connection may be superfi-

123. This test was first articulated by the Supreme Court of Canada in *Libman v. The Queen*, [1985] 2 S.C.R. 178 (Can.). The *Libman* formulation of the test has been influential (see, for example, R. v. Smith, [2004] EWCA (Crim) 631, [2004] QB 1418 (Eng.)), but courts in different states use varying terminology to describe essentially the same test.

124. For a useful discussion of this point, see Lee Ann W. Lockridge, *Intellectual Property in Outer Space: International Law, National Jurisdiction and Exclusive Rights in Geospatial Data,* 32 J. SPACE L. 319, 342–43 (2006).

cially obvious. For example, with the tort of defamation over the Internet, it is possible to say that a key element of the tort—publication and the ensuing harm of damage to reputation—occurred wherever the offending materials were viewed.[125] Yet this connection exists wherever there is Internet access, and courts have increasingly tended to require "something more" in order to ground a connection to a state's territory.[126] The fact that a website might be accessed by residents of one jurisdiction does not necessarily mean that it has been, or that consequences should flow if it has. Thus courts have rejected jurisdiction in cases where, in spite of the fact that the material could have been viewed from within their domestic jurisdiction, there was insufficient nexus between the parties and the jurisdiction.[127] By the same token, a company that does not target its wares or services to a particular jurisdiction does not infringe the trademarks of a trader in that jurisdiction simply because it uses the same or a similar trademark on its website.[128] Recent cases have looked at the extent to which a website targets a particular market.[129] Thus the territorial connection for subject matter must be more than simply the ability to access content from a particular location.

---

125. Although some courts require that there be genuine harm in the jurisdiction where the material was viewed. See, for example, *Jameel v. Wall Street Journal*, [2005] EWCA (Civ) 75, [68]–[71], [2005] QB 946 (Eng.), appealed to the House of Lords on a different issue, where the court found that its jurisdiction over the matter depended on the number of people who had viewed the online publication. It was established that only 5 had done so in England; this was considered insufficient and the court threw out the claim of defamation. *See also* Al Amoudi v. Brisard [2006] EWHC 1062 (QB) (Eng.).

126. Andrea Slane identifies this as an approach by courts which she labels "the internet is here, there and everywhere"; the ubiquity of the Internet is used by the courts to *restrain* their exercises of jurisdiction. "[C]ourts can claim that if the public addressed by the defendant's activity *meaningfully includes* the population of the forum jurisdiction, then the forum court may be entitled to exercise jurisdiction and to apply local law." Andrea Slane, *Tales, Techs, and Territories: Private International Law, Globalization, and the Legal Construction of Borderlessness on the Internet*, LAW & CONTEMP. PROBS., Summer 2008, at 129, 144.

127. In *Al Amoudi*, [2006] EWHC at [37], the court found that it was insufficient simply to show that the publication could have been accessed from the U.K.; it was necessary to show that a sufficient number of people had actually accessed it.

128. Pro-C Ltd. v. Computer City, Inc. (2001), 14 C.P.R. (4th) 441, 2001 CanLII 7375 (Can. Ont. C.A.). In *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997), a U.S. court set out a "sliding scale" test for jurisdiction in Internet cases which looked at the degree of interactivity of the website. This test has been influential in many other cases, though increasingly controversial. The test distinguishes between active and passive websites, and degrees of activity and passivity in between. *Id.* at 1123–24.

129. *See* Hy Cite Corp. v. BadBusinessBureau.com, L.L.C., 297 F. Supp. 2d 1154, 1161–67 (W.D. Wis. 2004).

The case of *eBay Canada Ltd. v. Minister of National Revenue*[130] offers an interesting example of how a court reworks the notion of "territory" in the Internet age. In that case, Canada's Federal Court of Appeal considered an appeal regarding the obligation of eBay Canada to provide certain information about its Canadian PowerSellers to the Canada Revenue Agency (CRA). The CRA sought this information so as to determine whether these individuals had properly declared their income from their eBay activities. eBay Canada had resisted disclosure of this information, which was contained in electronic records stored on a server based in the United States and owned by eBay Inc., a U.S. company. eBay Canada is a wholly owned subsidiary of eBay International, which in turn is a wholly owned subsidiary of eBay U.S. eBay Canada argued that the information being sought by the CRA was "foreign-based" information that could not be disclosed to the CRA under Canada's *Income Tax Act*.[131]

A key issue was thus whether the information was properly characterized as "foreign-based." Justice Evans noted that section 231.6 of the *Income Tax Act*, which defines and addresses "foreign-based information," was enacted in 1988, a relative technological dark age. At that point in time, it might have been reasonable to conclude that a document was located where it was situated. However, the Court was of the view that technology changed the situation. Thus, Justice Evans stated:

> In order to determine the parameters of the concept of "location" on the present facts, it is helpful to consider whether the

130. eBay Can. Ltd. v. Minister of Nat'l Revenue, 2008 FCA 348, [2010] 1 F.C.R. 145 (Can.C.A.).

131. Income Tax Act, R.S.C. 1985, ch. 1 (5th Supp.) (Can.) Two provisions of the *Income Tax Act* were relevant in this dispute. The first, section 231.2(1) authorizes the Minister of National Revenue (MNR) to "require any person to produce information for any purpose related to the administration or enforcement of this Act." Section 231.2(2) governs the particular case of information relating to unnamed persons. In cases where information about unnamed persons is sought, the MNR is required to obtain judicial authorization. Judicial authorization will be forthcoming where "the person or group is ascertainable", section 231.2(3)(*a*), and where "the requirement is made to verify compliance by the person or persons in the group with any duty or obligation under this Act." Section 231.2(3)(*b*). It was under this provision that the MNR had proceeded. Section 231.6 of the Act deals specifically with "foreign-based" information or documents, which are defined as information or documents located outside Canada. This section permits the MNR to require any person resident in Canada to supply it with foreign-based information or documents. Section 231.6 notably makes no provision for obtaining foreign-based information about unnamed persons. In fact, where foreign-based information is required, it is sought by requiring the person to whom the information relates to produce it.

> rationale for a separate statutory regime governing requirements to produce "foreign-based information or document[s]" applies to information in electronic form which is accessible through computers situated far from the servers on which the information is stored.[132]

Justice Evans was of the opinion that courts should "interpret legislation in light of contemporary technology and, if necessary, should 'transpose' its terms to take into account the changed technological environment in which it is to be applied."[133] He concluded that the scheme under section 231.6 was directed at a situation where it might be "unduly onerous for a person to be required to produce material located outside Canada and in the possession of another person."[134] Justice Evans noted that there may also have been a legislative concern about the law having an unduly extraterritorial effect. From this he distinguished the set of facts before him. He declined to find that the information at issue was foreign-based. He noted that the information was accessible in Canada to employees of the appellants "with the click of a mouse."[135] In such circumstances, he ruled that it would be nonsensical "to insist that information stored on servers outside Canada is as a matter of law located outside Canada for the purpose of section 231.6 because it has not been downloaded."[136] He noted that people did not travel to the site of servers in order to read the information stored in them. Further, he noted that if eBay Canada chose to download the information it could view on its screens, the information would be located in Canada. He expressed the view that "it is formalistic in the extreme for the appellants to say that, until this simple operation is performed, the information which they lawfully retrieve in Canada from the servers and read on their computer screens in Canada is not located in Canada."[137] Essentially, as no one outside the country was compelled to act (the documents could be accessed from eBay Canada's computer system in Canada), there was no extraterritorial action; and in the court's view, any extraterritorial effect would be minimal. [138]

---

132. *eBay*, 2008 FCA 348, para. 43.

133. *Id.* para. 42.

134. *Id.* para. 47.

135. *Id.* para. 48.

136. *Id.*

137. *Id.* para. 50.

138. The Court noted as well that agreements between the appellants and PowerSellers provide that eBay may disclose "confidential 'eBay System Information.'" Thus, the agreements

There is no hard and fast rule that defines a state's territorial boundaries on the Internet. The High Court of Australia in *Dow Jones v. Gutnick* noted that a single rule has not emerged "because the rules pay insufficient regard to the different kinds of tortious claims that may be made."[139] Tortious conduct on the Internet manifests itself in different ways. Hörnle notes that

> . . . not all torts committed by information disseminated through the Internet can be located by reference to the same action (such as uploading or downloading information) or by reference to the location of the same connecting factor (such as the server hosting the information, the establishment of the person producing the information, etc.).[140]

Courts have also used jurisdiction over persons or parties as a means of determining whether to take jurisdiction over a dispute even where there is a connection to the court's territorial jurisdiction. A single act can have legal consequences in more than one country, and redress may be more appropriate in some jurisdictions than in others. While Internet-based acts may span the globe, individuals remain fairly closely and predictably tied to particular places (by residence or by operation of a business, for example). Thus, inquiries into personal jurisdiction may allow courts to limit the circumstances in which they will assume jurisdiction over a dispute. In the United States, this concept is expressed in terms of the *de minimis* principle; in other words, a defendant must meet a certain minimum threshold for contacts with the jurisdiction.[141] Thus, where the defendant has no real connection with the state, the court may decline to take jurisdiction over the matter in dispute. A defendant's place of residence and place of business may be relevant factors in establishing whether he or she has sufficient connec-

---

between eBay Canada and its top sellers contemplated that such disclosures might take place. *Id.* para. 49.

139. *Dow Jones & Co. Inc. v Gutnick* (2002) 210 CLR 575, ¶ 4 (Austl.). In *Gutnick*, the High Court found that the tort of defamation occurred in Australia when material harmful to the reputation of the Australian plaintiff was downloaded in Australia, even though it was hosted on a server located in the United States. *See id.*

140. Julia Hörnle, *The Jurisdictional Challenge of the Internet*, *in* LAW AND INTERNET, *supra* note 60, at 121, 158.

141. Int'l Shoe Co. v. Washington, 326 U.S. 310, 316 (1945); Milliken v. Meyer, 311 U.S. 457, 463 (1940); Hörnle, *supra* note 140, at 143–44.

tion to the jurisdiction.[142] Again, however, while the principles are long established, the Internet destabilizes the concept of an individual's connection to a territory. Whereas a brick and mortar store front is connected to a state in a real and physical manner, an Internet website may not be—particularly where it is not hosted on a server within the court's jurisdiction, but has merely been a site through which a few sales have been made in that jurisdiction.

Of course, at some point jurisdiction over parties and subject matter jurisdiction begin to fuse. In "locating" acts on the Internet, it is relevant to consider both physical points of contact and the relationship of the actor to the territory. It is not surprising, therefore, to view the emergence of more hybrid tests. For example, in Canada, the "real and substantial connection" test has evolved, and it requires the court to examine a range of factors before deciding to take jurisdiction. These factors blend considerations of both personal and subject matter jurisdiction.[143]

An important check to courts' exercise of adjudicative jurisdiction has always been the power of national courts to refuse (or grant) the enforcement of a court decision from another jurisdiction. This power provides an interesting buffer that allows courts to reject undue reach into their jurisdiction by the laws of another country. In other words, through this aspect of adjudicative jurisdiction in the private international law arena,[144] national courts have a means of assessing the appropriateness of a foreign state's decision that it has both personal

142. *See, e.g.*, Panavision v. Toeppen, 141 F. 3d. 1316, 1321 (9th Cir. 1998); Am. Info. Corp. v. Am. Infometrics, Inc., 139 F. Supp. 2d 696 (D. Md. 2001); Nissan Motor Co. v. Nissan Computer Corp., 89 F. Supp. 2d 1154 (C.D. Cal. 2000), *aff'd* 246 F.3d 675 (9th Cir. 2000).

143. The Ontario Court of Appeal offered a list of factors to take into account in *Muscutt v. Courcelles,* [2002] 60 O.R.3d 20 (Can. Ont. C.A.), which was later varied somewhat in *Van Breda v. Village Resorts Ltd.,* 2010 ONCA 84 (Can. Ont. C.A.). These factors were applied in the Internet defamation context in *Black v. Breeden,* 2010 ONCA 547 (Can. Ont. C.A.). Both cases are currently on appeal to the Supreme Court of Canada. The factors were distilled in the subsequent Internet defamation case of *Bangoura v. Wash. Post* (2005), 202 O.A.C. 76, 2005 CanLII 32906 (Can. On. C.A.) into the following list: (i) the connection between the forum and the plaintiff's claim; (ii) the connection between the forum and the defendant; (iii) unfairness to the defendant in assuming jurisdiction; (iv) unfairness to the plaintiff in not assuming jurisdiction; (v) the involvement of other parties to the suit; (vi) the court's willingness to recognize and enforce an extra-provincial judgment rendered on the same jurisdictional basis; (vii) whether the case is interprovincial or international in nature; and (viii) comity and the standards of jurisdiction, recognition and enforcement prevailing elsewhere. *Id.* para. 19.

144. It is well-established, indeed axiomatic, that court will not enforce the public laws of other states. S.A. Williams & J.-G. Castel, An Introduction to International Law, 2nd ed. (1987) at 125–126.

and subject matter jurisdiction regarding the acts of a defendant located in the national court's jurisdiction. A court asked to enforce such a decision will only do so if it is of the view that the deciding court properly had jurisdiction over both the subject matter and the parties. Where it is not persuaded that this was the case, it will not give effect to the judgment.[145]

Where a national court has been too quick to take personal jurisdiction over individuals, a decision not to enforce the judgment will serve as a means by which another court places a check on its extraterritorial reach. The court in the jurisdiction in which a foreign decision is sought to be enforced may decline to order its enforcement if it is of the view that the foreign court was not properly seized of the dispute.

It is thus that courts play an important role in defining the territorial boundaries of state action. They can extend those boundaries through interpretation of laws, events (by finding, for example, that an Internet communication occurs both at the point of transmission and the point of reception, instead of one or the other), or facts (finding that individuals have sufficient ties to the jurisdiction). They can restrict the boundaries by the same means. Finally, they can limit the reach of other states' laws by refusing to enforce judgments against their residents, nationals, or corporations where they are of the view that the foreign court was not properly seized of jurisdiction. Nevertheless, questions of territoriality and extraterritoriality are not limited to the judicial branch of government. Indeed, it is important to consider the diversity of ways in which states and state entities exercise jurisdiction in the Internet context.

B. *Prescriptive Jurisdiction*

In our discussion of the "second dimension" of state jurisdiction and the Internet we discussed the international norm-setting activities of states. These arise where states negotiate treaties to establish common norms for addressing certain types or categories of Internet-based activities. These treaties generally result in domestic law that is applied and enforced, but these domestic laws are enacted within a framework of international consensus. In this section we consider a somewhat different issue: the extension of existing national norms or laws, often enacted prior to the Internet, to Internet-based activity.

States regularly legislate to address matters arising within the bounds of their territorial sovereignty. Just as is the case, however, with adjudi-

145. *See, e.g.*, Lucasfilm Ltd. v. Ainsworth, [2009] EWCA (Civ) 1328 (Eng.).

cative jurisdiction, the boundaries of prescriptive jurisdiction are tested by the Internet context. Where prescriptive jurisdiction is at issue, states must consider whether the acts or conduct that they seek to control, regulate or modify are appropriately linked to their territory. The challenge is by no means a small one. In the early days of the Internet, Johnson & Post observed that this phenomenon

> . . . is destroying the link between geographical location and: (1) the power of local governments to assert control over online behaviour; (2) the effects of online behaviour on individuals and things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.[146]

These remain challenges. Not only is Internet-based activity difficult to regulate, its effects are distributed and difficult to measure, and the laws of individual nation states are unlikely to have much effect without some form of global cooperation. The consequences for states can be deeply challenging. These challenges arise in the context of, to name some key areas: cultural and linguistic policy, economic policy, social policy, criminal law, and morality.[147]

Cultural and linguistic policies are increasingly disrupted by the phenomenon of the Internet. For example, the Quebec government's legislation requiring businesses operating in Quebec to offer a French-language face to consumers encountered significant hurdles with the rise of e-commerce.[148] Businesses with premises in Quebec must ensure that they have a French language version of their website in order to comply with the law. However, there is no way to stop businesses the world over from selling their wares or services to Quebeckers over the Internet in any language they choose.[149] Cultural policies are also at

146. Johnson & Post, *supra* note 72, at 1370.

147. *See* Schultz, *supra* note 102, at 801 (arguing that one sees the strongest assertion of state jurisdiction over Internet activity in the area of protection of local values).

148. The legislation is known as the Charter of the French Language, R.S.Q., c. C-11 (Can.). It provides that the language of business in Quebec is French. Section 58 of the law requires all public signs and advertising to be in French.

149. This is effectively conceded by the fact that the Office de la Langue Française indicates that only those businesses with an address in Quebec must have a French version of their website. *See* Office de la Langue Francaise, Information and Communication Technolgies in French 4 (2010), *available at* http://www.oqlf.gouv.qc.ca/ressources/bibliotheque/depliants/20100212_depliant6fva.pdf.

risk. Federal Canadian content regulations[150] have long required radio and television undertakings to meet certain quotas for Canadian broadcast content. The federal regulator has so far hesitated to apply such rules in the Internet context.[151] In many countries, broadcasters have also had to account for certain standards of "decency," including restrictions regarding profanity, nudity, and violence.[152] These restrictions functioned so long as the state could exercise control over the broadcasters. In a decentralized, distributed system such as the Internet, consumer choice rules, and it will be increasingly difficult for states to impose cultural and other agendas.[153]

The regulation of citizen expression also becomes more challenging on the Internet. There are numerous instances of national governments attempting to transpose limits on various types of expression from traditional media to the Internet—often with great difficulty. Examples include attempts in Canada and Germany to address the dissemination of hate propaganda over the Internet,[154] attempts in

150. *See, e.g.,* Radio Regulations, SOR/1986-982 (Can.), *available at*: http://www.canlii.org/en/ca/laws/regu/sor-86-982/latest/sor-86-982.html.

151. CAN. RADIO-TELEVISION AND TELECOMMS. COMM'N, CRTC 2009-329, BROADCASTING REGULATORY POLICY (2009), *available at* http://www.crtc.gc.ca/eng/archive/2009/2009-329.htm.

152. In Canada, the CRTC may refuse to renew the licence of a broadcaster that does not comply with prescribed standards of decency. This is a system that works reasonably well in the context of a broadcasting network where licences are required in order to operate a broadcast undertaking. It does not work at all in the Internet context. The regulations relating to content standards are found in the Radio Regulations, SOR/1986-982, s. 3(c) (obscene or profane content) and s. 3(b) (hate speech), and in Television Broadcasting Regulations, SOR/1987-49, s. 5(1)(c) (obscene or profane content), and s. 5(1)(b) (hate speech). In 2011, the CRTC attracted international media attention when it ruled that Canadian radio stations could not play the Dire Straits song "Money for Nothing" unless a certain word, considered homophobic, was edited out. The decision is currently under review. Press Release, Can. Radio-television and Telecomms. Comm'n, *CRTC Asks the Canadian Broadcast Standards Council to Review Decision to Ban Dire Straits Song* (Jan. 21, 2011), http://www.crtc.gc.ca/eng/com100/2011/r110121.htm.

153. For a discussion of content regulation on the Internet in the EU, *see* Elizabeth Newman, *EC Regulation of Audio-visual Content on the Internet*, *in* LAW AND INTERNET, *supra* note 60, at 159.

154. The Canadian Human Rights Commission (CHRC), acting under Section 13 of the Canadian Human Rights Act, R.S.C. 1985, c. H-6, has struggled to address hate speech on the Internet with a great deal of controversy. A recent report commissioned by the CHRC recommend that extreme forms of hate speech be dealt with under Criminal Code provisions and not under the CHRA. *See* RICHARD MOON, REPORT TO THE CANADIAN HUMAN RIGHTS COMMISSION CONCERNING SECTION 13 OF THE CANADIAN HUMAN RIGHTS ACT AND THE REGULATION OF HATE SPEECH ON THE INTERNET (2008), *available at* http://www.chrc-ccdp.ca/pdf/moon_report_en.pdf. Moon argues that ISPs should play some role in limiting hate speech over the Internet through the application of acceptable use policies to customer activity. *Id.* at 41. In Germany, the German High Court took jurisdiction over an Australian citizen who posted holocaust denial material online. *See* Bundes-

China to limit certain types of discourse by imposing technological constraints on infrastructure,[155] and attempts to apply French law to the sale of Nazi memorabilia on eBay.[156]

Economic policy is also difficult to apply to the Internet. Governments that have sought to facilitate electronic commerce, to regulate competition, and to impose taxation on online goods and services have all quickly realized that little can be done without international cooperation.[157] Economic policy is also reflected in international trade treaties, and these have proliferated in recent years in regional, bi- and multilateral forms.[158]

Even social policy with Internet dimensions poses challenges to concepts of territoriality. A government might choose, for example, to adopt a particular educational policy that contains broad exceptions for the use of online materials in education, or for educational fair dealing. Yet these same materials which can be legitimately accessed in that country may infringe copyright when accessed or downloaded in another jurisdiction. The same can be said about states that maintain a lower term of copyright protection to serve the public domain; works that fall in the public domain in that country will infringe copyright if, once uploaded to a local website, they are accessed and downloaded in

---

gerichtshof [BGH] [Federal Court of Justice], Dec. 12, 2000, NEUE JURISTICHE WOCHENSCHRIFT [NJW] 624, 2001 (Ger.).

155. Subjects that are banned include democracy, the Dalai Lama and the Falung Gong. *See, e.g.,* Jack Linchuan Qui, *Virtual Censorship in China: Keeping the Gate Between the Cyberspaces,* INT'L J. COMM. L. & POL'Y, Winter 1999, at 1. However, Zittrain argues that these technological measures are imperfect, and work arounds are generally possible. *See* ZITTRAIN, FUTURE, *supra* note 99, at 106; *see also* BENKLER, *supra* note 69, at 268–69.

156. See the discussion of the litigation arising in this matter *infra.*

157. In fact, there is a great deal of effort at the international level to harmonize norms in order to facilitate electronic commerce. *See, e.g.,* Charles H. Martin, *The Electronic Contracts Convention, the CISG and New Sources of E-Commerce Law,* 16 TULANE J. OF INT'L & COMP. LAW 467 (2008). For a discussion of the challenges of taxation of the Internet, see Ken Griffen, Mark McMurtrey & LeeAnn Smith, *To Tax or Not to Tax? Foreign and Domestic Taxation of the Internet, in* PROCEEDINGS OF THE ACADEMY OF LEGAL, ETHICAL AND REGULATORY ISSUES (2008), *available at* http://www.alliedacademies.com/Public/Proceedings/Proceedings22/ALERI%20Proceedings.pdf#page=5; Daniel D. Sokol, *International Antitrust Institutions, in* COOPERATION, COMITY, AND COMPETITION POLICY 186–213 (Andrew T. Guzman ed., 2010), *available at* http://www.ingentaconnect.com/content/oso/7636688/2010 (discussing the competition or antitrust context).

158. Perhaps the most notable of these have been the Final Act Embodying the Results of the Uruguay Round of Multinational Trade Agreements, Apr. 15 1994, 108 Stat. 4809, 1867 U.N.T.S 14, and the Marrakesh Agreement Establishing the World Trade Organization, Apr. 15, 1994, 1108 Stat. 4809, 1867 U.N.T.S 154.

countries where the term of protection has not expired.[159]

The now-infamous sale of Nazi memorabilia on the Yahoo.com website offers an illustration of another challenge posed by the Internet to state jurisdiction that manifests itself in many ways and across a range of subject matter. In the Yahoo! case, advocacy groups in France brought a complaint against both Yahoo! and the Yahoo! France website (which served to provide access to Yahoo.com) over the sale of hundreds of objects of Nazi memorabilia through the auctions page. A French court found that Yahoo! had violated French law as both the illegal objects and related hate propaganda materials could be accessed and viewed in France. The court was of the view that as the auction site could identify French visitors to the site well enough to display French language banner advertisements to them, it was clearly targeting them. One part of the court's order was that Yahoo! limit both the hosting of and the access to offensive content in France.[160] The court found that since it was technologically possible to block access to certain content to visitors from France, Yahoo! was required to adopt such measures to avoid breaching the law.[161] This interim ruling was confirmed by a second decision rendered after the court considered a study by a team of Internet experts who assessed the technological feasibility of blocking French users from accessing the disputed content.[162]

Following the French court order, Yahoo! sought declaratory relief from the U.S. District Court for the Northern District of California, asking that the court decline to recognize or enforce the French court orders. Judge Fogel essentially found that the French court's decision could not be reconciled with the First Amendment protection for freedom of speech.[163] A U.S. based company could not be forced to

159. This has proven to be a significant challenge, for example, for those who have tried to create online archives of public domain works. *See, e.g.*, Hannibal Travis, *Building Universal Digital Libraries: An Agenda for Copyright Reform*, 33 PEPPERDINE L. REV. 761, 792 (2005).

160. Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, May 22, 2000, D. 2000 inf. rap. 172, obs. J. Gomez (Fr.).

161. Note that Kohl is critical of this decision and argues that it was not evident that the Yahoo! content had "a substantial effect on French territory so as to make an assertion of regulatory competence reasonable." KOHL, *supra* note 1, at 100.

162. Tribunal de grande instance [T.G.I.] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000, obs. J. Gomez (Fr.), *available at* http://www.lapres.net/ya2011.html, and *at* http://www.lapres.net/yahen11.html (providing an unoffical English translation). Schultz argues that using filtering as a means of restricting the liability of companies online has consequences for a free and open flow of information on the Internet. *See* Schultz, *supra* note 103, at 821.

163. Yahoo, Inc. v. La Ligue Contra le Racisme et l'Antisemitism, 169 F. Supp. 2d 1181 (N.D. Cal. 2001); *see also* Evan Scheffel, Yahoo, Inc. v. La Ligue Contre Le Racisme et L'Antisemitism:

comply with the regulation by another country of speech protected under the First Amendment in the U.S. Thus the ruling turned on this difference in values between the two countries. In France, the goals of fighting racism and anti-Semitism justified restrictions on speech, whereas such restrictions would not be justifiable in the U.S. The decision underlines a fundamental challenge with the exercise of state jurisdiction in relation to the Internet.

The decision was appealed to the Ninth Circuit Court of Appeals.[164] The en banc court decided to reverse the decision and remand it with directions to dismiss the action, although the court was not united as to the reasons for this. A majority of judges found that the District Court had personal jurisdiction over the defendants, but that the matter was not ripe for decision. A minority of the judges found that the matter was ripe but that the court below lacked personal jurisdiction. The U.S. Supreme Court did not grant certiorari in the case.

In ruling that the decision was not yet ripe, the majority of the Ninth Circuit Court of Appeals noted that it was not clear from the facts whether Yahoo!, in changing its practices, had already substantially complied with the French court's orders. If there was substantial compliance, there might be no attempt to enforce the judgment in the U.S. In addition, if Yahoo! was already in substantial compliance, the argument that the enforcement of the French court's orders would violate the First Amendment would be difficult to assess. The Court noted that there did remain an issue of whether the First Amendment had extraterritorial effect, and thus whether denying access to certain content to French users amounted to a violation of the First Amendment even if U.S.-based users were not affected by any changes. However, the majority noted that without knowing if Yahoo!'s policy changes brought it into substantial compliance, there was no way to know whether there would actually be a First Amendment issue, and without knowing what further steps would need to be taken it would be impossible to tell whether any such argument would be based on the

---

Court Refuses to Enforce French Order Attempting to Regulate Speech Occurring Simultaneously in the U.S. and in France, 19 SANTA CLARA COMPUTER & HIGH TECH L.J. 549 (2003); Sakura Mizuno, *When Free Speech and the Internet Collide: Yahoo!—Nazi—Paraphernalia Case,* 10 CURRENTS INT'L L.J. 69 (2001).

164. Yahoo, Inc. v. La Ligue Contra le Racisme et l'Antisemitism, 433 F. 3d 1199 (9th Cir. 2006). Multiple commentaries have been made on the appellate court decision. *See e.g.*, Andrew M. Pickett, *Much Yahoo! about Nothing: The Ninth Circuit, Jurisprudential Schizophrenia, and the Road Not Taken in Yahoo! v. La Ligue Contre le Racisme et l'Antisemitisme*, 8 TUL. J. TECH. & INTELL. PROP. 231 (2006); Robert T. Razzano, *Error 404 Jurisdiction Not Found: The Ninth Circuit Frustrates the Efforts of Yahoo Inc. to Declare a Speech-Restrictive Foreign Judgment Unenforceable*, 73 U. CIN. L. REV. 1743 (2005).

infringement of rights in the U.S. and France, or simply in the U.S. alone. The majority concluded that "First Amendment issues arising out of international Internet use are new, important and difficult. We should not rush to decide such issues based on an inadequate, incomplete or unclear record."[165]

It has always been the case that some activities may be regulated differently in some jurisdictions than in others. This is particularly the case with so-called moral questions—those involving gambling and pornography, for instance. It is also the case with speech-related activities: hate crimes, sedition, and other forms of subversive speech are treated quite differently in different jurisdictions, as the Yahoo! case illustrates. A state seeking to control or restrict these forms of speech within its own borders, may wish to target those engaging in these forms of speech in other countries.[166] Conduct may be perfectly legal in the jurisdiction where a site is hosted, even though it is not legal in all of the jurisdictions where the particular wares or services offered are consumed. Where this is the case, a country may seek to assert jurisdiction over offshore Internet hosts or actors on the basis that their activities spill over into its jurisdiction, where they are illegal.[167] Or, countries may seek various compromise solutions which reflect the limitations on their ability to enforce their laws; so, the EU regulates foreign gambling only where there is "equipment" in place in the particular member state, while Australia essentially concedes and pro-

165. *Yahoo,* 433 F. 3d at 1223.

166. Bundesgerichtshof [BGH] [Federal Court of Justice], Dec. 12, 2000, NEUE JURISTICHE WOCHENSCHRIFT [NJW] 624, 2001 (Ger.). In *Citron v. Zündel, (*2002) 41 C.H.R.R. D/274, the Canadian Human Rights Commission found Canadian citizen Ernst Zündel to have violated the Canadian Human Rights Act, R.S.C. 1985, c. H-6 by ordering an employee based in California to upload hate propaganda to a website hosted on a server also located in California. Here the national jurisdiction was exercised not by pursuit of offshore actors, but by pursuing someone in Canada for directing certain activities in another country.

167. *See, e.g.*, People v. World Interactive Gaming Corp., 714 N.Y.S.2d 844 (Sup. Ct. N.Y. 1999). In this case, a company based in Antigua (but with a Delaware incorporated parent company) operated an online gambling website from Antigua. *Id.* at 846-47. The New York court took criminal jurisdiction over the matter because the gambling site was accessed by many residents of New York. *Id.* at 850. The court stated that a "computer server cannot be permitted to function as a shield against liability, particularly in this case where respondent's activity targeted New York as the location where they conducted many of their allegedly illegal activities." *Id.* Note, however, that in this case the location of the company in Antigua may have been done deliberately so as to evade the reach of U.S. authorities. For other offshore gambling cases in which U.S. courts have taken jurisdiction, see *United States v. Am. Sports Ltd.*, 286 F.3d 641 (3d Cir. 2002), and *United States v. Ross*, 1999 WL 782749 (S.D.N.Y. Sept. 16, 1999).

hibits unlicensed gambling only by Australian residents.[168] A state may also seek to have its own national law limitations (such as a minimum age requirement for participation in the activity) implemented by the offshore site.[169]

Significant challenges may arise where a state sets norms of conduct within its own jurisdiction that can be infringed by Internet based companies located elsewhere, whose services are nonetheless available to its citizens. The recent battle between Facebook and the Privacy Commissioner of Canada offers an interesting illustration of the extent to which Canadian law can reach, however informally, outside the boundaries of the state. Facebook, which operates a hugely popular social networking site internationally, was the subject of a complaint to the Privacy Commissioner.[170] The complaint alleged that the site operators violated Canadian data protection laws by not ensuring the collection, use, and disclosure of personal information was in accordance with those laws. The Privacy Commissioner, emboldened by a court decision which found that she had jurisdiction to investigate complaints involving foreign companies as long as the collection, use, or disclosure of information took place in Canada,[171] investigated and found that Facebook was not compliant.[172] Interestingly, Facebook chose to work with the Commissioner to attempt to change its system to

168. *See* Joseph J. McBurney, *To Regulate or to Prohibit: An Analysis of the Internet Gambling Industry and the Need for a Decision on the Industry's Future in the United States*, 21 CONN. J. INT'L L. 337, 355 (2006).

169. As the Yahoo! cases illustrate, in some cases, the limitations required may be achievable through the use of technology. The French Court in Yahoo!, for example, looked at ways in which Yahoo! could modify its system so as to block access to offensive content to French users without affecting access by U.S. users. Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, May 22, 2000, D. 2000 inf. rap. 172, obs. J. Gomez (Fr.).

170. *See* Letter from Phillipa Lawson, Dir., Can. Internet Policy & Public Interest Clinic, to the Privacy Comm'r of Can., Re: PIPEDA Complaint: Facebook (May, 30 2008), http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf [hereinafter Letter to Privacy Commissioner] (providing the original complaint made against Facebook to the Privacy Commissioner).

171. Lawson v. Accusearch Inc., [2007] 4 F.C.R. 314 (Can.). In *Lawson*, the federal court ruled that while the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, did not have extraterritorial effect, the Office of the Privacy Commissioner of Canada did have the power to investigate the collection, use and disclosure of personal information by a U.S.-based company where the collection, use or disclosure was linked to Canada, essentially on the basis of qualified territoriality. *Id.*; *see also* Donna L. Davis, *Tracking Cross-Border Data Flows: A Comment on* Lawson v. Accusearch, 6 CAN. J. L. & TECH. 119 (2007).

172. ELIZABETH DENHAM, REPORT OF FINDINGS INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC AGAINST FACEBOOK INC. UNDER THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (2009), *available at* http://www.priv.gc.ca/cf-dc/

her satisfaction.[173] The alternative was to face an enforcement action in Canadian Federal Court. It is not clear what effect any decision of the Federal Court could or would have had on Facebook, which is based in California.

The case may offer interesting insights into the effect that a national law setting data protection norms can have on the practices adopted by a foreign company. Similar issues arise in the EU in the case of the data protection regime and some Internet companies. For example, Google (like other search engines) may retain IP addresses associated with search data. Google had the practice of retaining this data indefinitely. However, if the data qualified as personal information, the retention of the data indefinitely was not permitted under EU data protection norms governing the retention and reuse of personal information.[174] Google did agree to reduce its period of data retention under pressure from the EU,[175] however the reduced retention period is still controversially high. Like the Facebook case, the issue is one of national norms or standards pushing multinational Internet-based companies to make changes to how they operate. However, the changes are voluntary, and may only meet the regulator half way. Enforcement beyond this point remains problematic, as the jurisdictional complexities will be challenging for any court that is asked to render a decision on the violation of domestic norms that can be enforced without limiting or denying its nationals access to a global site or service.

It is to be noted that states have clearly not abdicated their territorial jurisdiction when it comes to Internet-based activities that touch on social, cultural, or 'public order' issues. Indeed, Schultz argues that "[t]he protection of such local values lies at the heart of modern

---

2009/2009_008_0716_e.pdf (providing the Privacy Commissioner's findings with respect to the complaint).

173. The Commissioner later reviewed the changes made by Facebook in response to the complaint, and ruled that the matter was resolved. *See* Press Release, Officer of the Privacy Comm'r of Can., Privacy Commissioner Completes Facebook Review (Sept. 22, 2010), http://www.priv.gc.ca/media/nr-c/2010/nr-c_100922_e.cfm.

174. Directive 2006/24, of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58, 2006 O.J. (L 105) 54–63 [hereinafter Data Retention Directive], *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

175. Edwards, *supra* note 60, at 458; *see also* Christopher Kuner, *International Data Protection Law and Jurisdiction on the Internet (Part 1)*, 18 INT'L J. L. & INFO. TECH. 176, 177 n.12 (2010).

conceptions of political sovereignty."[176] More specifically he argues that the principles of jurisdiction arose to ensure that one state, in the regulation of matters within its borders, does not unduly encroach on the sovereignty of another.[177] It is not surprising, therefore, that it is in this soft area of values that we find some of the more contentious exercise of jurisdiction, as well as a rising tide of regulatory approaches that mandate technological boundaries to online activities.

C. *The Erosion of Jurisdiction*

Not only does the Internet pose new challenges for states in terms of how to determine when and how they should exercise their jurisdiction, the Internet and the related phenomenon of globalization also have an eroding effect on jurisdiction. An essential element of jurisdiction is state sovereignty—the ability of states to govern that which concerns their territory. Yet there are a number of forces and factors which undermine both the concept of territory, and the ability of the state to truly regulate what occurs within its borders. Sassen notes that "globalization has brought strong pressures for the deregulation of a broad range of markets, economic sectors, and national borders and, furthermore, for the privatization of public sector firms and operations."[178] These are clearly phenomena that erode state jurisdiction by removing certain subject matter from state authority.[179]

The globalization of commerce—first between businesses, and more recently with the rise of e-commerce, between business and individuals—has also given rise to two other phenomena that erode state jurisdiction through the choices of private actors.[180] The first is the ubiquity of choice of law clauses that see parties to contracts agreeing to settle disputes in one jurisdiction over all others with connections to the agreement. These choice of law clauses thus limit state jurisdiction over

176. Schultz, *supra* note 102, at 807.

177. *Id.* at 808 ("To reconcile these two imperatives—to protect local values without encroaching on the territory of other states—is the fundamental problem of state intervention on the Internet.").

178. SASSEN, TERRITORY, *supra* note 64, at 222.

179. Schultz, *supra* note 102, at 801 (commenting on the rise of transnationalism as a phenomenon that contributes to the undermining of national jurisdictions).

180. Schultz, *supra* note 102, at 805. Schultz argues that "online communities of various kinds, albeit primarily of a commercial nature, will further the development of their social norms into private legal systems." *Id.*

a wide range of transactions that might otherwise have been considered to fall within the jurisdiction of their national courts.[181]

In addition to choice of law clauses, mandatory arbitration clauses have found their way into business and consumer contracts. By agreeing to mandatory arbitration of disputes, the parties move any potential disputes over the agreement to a private dispute resolution provider instead of the national courts of any one country. Schultz describes these regimes as causing "their normative environments to be largely divorced from public legal systems: a private dispute resolution mechanism applies privately developed norms and the outcome of the procedure is enforced through private means."[182] In some cases, such as with domain name registrations, the arbitration clause does not necessarily remove the jurisdiction of the courts. Yet the arbitration mechanism, while not definitively moving all disputes out of the courts, still moves the vast number of them out of national courts.

Domain name disputes center on the issue of bad faith registration of domain names, the notional "addresses" of Internet websites. Yet implicit in domain name disputes is the protection of trademark rights —something that normally falls within the domestic law of the state in which the trademark is registered. Domain name registrants agree to submit to arbitration of any disputes, and these arbitrations are carried out by panels appointed by private corporations.[183] These arbitration exercises have been controversial for a number of reasons.[184] One of

181. *E.g.*, Dell Computer Corp. v. Union des Consommateurs, [2007] 2 S.C.R. 801 (Can.) (upholding the validity of an arbitration clause in an online consumer contract that provided that any disputes should be resolved by arbitration provided by a U.S.-based arbitration company).

182. Shultz, *supra* note 102, at 831. Schultz notes that there are real advantages to this practice, and that numerous online alternative dispute resolution systems have emerged. He defines these mechanisms broadly, ranging from online mediation or arbitration to credit card chargebacks and trustmaks. (at 830).

183. The domain name dispute resolution system for the Top Level Domains is administered by ICANN but dispute resolution is contracted out to private dispute resolution providers. *See List of Approved Dispute Resolution Providers*, ICANN (Aug. 13, 2010), http://www.icann.org/en/dndr/udrp/approved-providers.htm.

184. Criticisms of the UDRP have included allegations that panelists show a bias towards trademark owners. *See, e.g.*, MICHAEL GEIST, FAIR.COM? AN EXAMINATION OF THE ALLEGATIONS OF SYSTEMIC UNFAIRNESS IN THE ICANN UDRP (2001), *available at* http://aix1.uottawa.ca/geist/geistudrp.pdf; MICHAEL GEIST, FUNDAMENTALLY FAIR.COM? AN UPDATE ON BIAS ALLEGATIONS AND THE ICANN UDRP (2002), *available at* http://aix1.uottawa.ca/geist/fairupdate.pdf; MILTON MUELLER, ROUGH JUSTICE: AN ANALYSIS OF ICANN'S UNIFORM DISPUTE RESOLUTION POLICY, *available at* http://dcc.syr.edu/PDF/roughjustice.pdf (last visited June 3, 2011). The following articles provide additional comprehensive critical studies. *See* ANNETTE KUR, UDRP: A STUDY BY THE MAX PLANCK INSTITUTE FOR FOREIGN AND INTERNATIONAL PATENT, COPYRIGHT AND COMPETITION LAW 65

these is related to jurisdiction at least to some extent. While such systems move disputes out of any one country's jurisdiction, the panelists nevertheless apply legal principles that derive from trademark law. While there are commonalities in the trademark law of many countries, the accusation leveled at these dispute resolution panels is that they have allowed U.S. trademark law principles to dominate.[185] This presents an interesting illustration both of the erosion of national jurisdiction and also of concerns about the internationalization of the legal principles of a single state.

Another eroding effect relates to the role of transnational corporations.[186] These powerful entities lead supranational existences, prompting some to comment on their lack of real accountability to the laws of any particular jurisdiction.[187] Multinational actors may wield enormous power in terms of dictating the norms by which they are governed. Earlier we discussed the case of Facebook and privacy norms. While Facebook has been responsive to some of the privacy concerns raised by national regulators, it is not clear whether it has stopped short of what the law might require.[188] Google offers another interesting ex-

---

(2002), *available at* http://141.3.20.1/admin/get_data.php?resID=95; A. Michael Froomkin, *ICANN's 'Uniform Dispute Resolution Policy'—Causes and (Partial) Cures*, 67 BROOK. L. REV. 608 (2002); Laurence R. Helfer, *Whither the UDRP: Autonomous, Americanized or Cosmopolitan?*, 12 CARDOZO J. INT'L & COMP. L. 493 (2004); Kenneth L. Port, *Trademark Monopolies in the Blue Nowhere*, 28 WM. MITCHELL L. REV. 1091 (2002).

185. *See, e.g.*, Helfer, *supra* note 184, at 496.

186. Sassen speaks of "the power of private corporate interests in shaping the activity space of the Internet." SASSEN, TERRITORY, *supra* note 64, at 331.

187. *See, e.g.*, Malcolm J. Rogge, *Towards Transnational Corporate Accountability in the Global Economy: Challenging the Doctrine of Forum Non Conveniens in* In Re: Union Carbide, Alfaro, Sequihua, and Aguinda, 36 TEX. INT'L L. J. 299 (2001); Alison Lindsay Shinsato, *Increasing the Accountability of Transnational Corporations for Environmental Harms: The Petroleum Industry in Nigeria*, 4 NW. UNIV. J. INT'L HUM. RTS. 186 (2005); Magdalena Bexell, Jonas Tallberg & Anders Uhlin, *Democracy in Global Governance: The Promises and Pitfalls of Transnational Actors*, *in* GLOBAL GOVERNANCE 81 (2010).

188. The Canadian Internet Policy and Public Interest Clinic (CIPPIC) launched the initial complaint against Facebook to the Office of the Privacy Commissioner of Canada. *See* Letter to Privacy Commissioner, *supra* note 170. Although the Office of the Privacy Commissioner ultimately declared itself satisfied with the changes made by Facebook, *see* Letter from Elizabeth Denham, Assistant Privacy Comm'r, Office of the Privacy Comm'r of Can., to David Fewer, Professor, Univ. of Ottawa, (Aug. 25, 2009), http://www.priv.gc.ca/media/nr-c/2009/let_090827_e.cfm (letter from OPC to CIPPIC outlining its resolution with Facebook), CIPPIC continues to express concerns that Facebook is not compliant with privacy norms. *See* Letter from Tamir Israel, Staff Attorney CIPPIC, to Facebook (May 28, 2010), http://www.cippic.ca/uploads/LT_Facebook-Re_Privacy_Response-FINAL-05282010.pdf.

ample. When faced with the European Directive on data retention,[189] which imposes limits on its retention of user data, it negotiated a compromise that it was prepared to accept, but that was still in excess of the limits sought by the EU.

Aside from resisting or shaping the normative rules governing Internet activity, corporations also develop and introduce technological layers which may have a significant effect on how the Internet is accessed and used. Sassen refers to the developments in "firewalled intranets for firms, firewalled tunnels for firm-to-firm transactions, identity verification, trademark protection and billing"[190] as examples of technological layers that shift the open and public nature of the Internet towards a private and commercial one. The combination of the power of multinational corporations and the growing global dependence on access, not just to the Internet but to certain ubiquitous tools and services, has an eroding effect on a state's capacity to exercise its jurisdiction.

The Internet may have other effects on the ways in which governments seek to control their own domestic policy and even their own state "assets." Here, the Internet must be considered both in terms of its architecture, and in terms of the global mass communication vehicle that it has become. Increasingly governments are aware of the potential of the Internet to drive innovation. Both citizens and corporations put pressure on governments to facilitate, rather than impede, activities that encourage collaboration, cross-pollination, and innovation in all fields of endeavor.[191] To do so requires changes to national laws and policies relating to technology and infrastructure, competition, and innovation. These changes are, in a sense, driven from below—it is the architecture of the Internet, the way that it functions, and the way that it has been embraced by citizens and businesses, that push governments to adapt and change how they regulate and govern. They are also driven from multiple points globally. Sassen notes that the Internet provides a mechanism by which localized movements "can become part of cross-border networks and move from being subject to specific national/local laws to a global scale where these laws almost cease to be operative."[192] This globalized network can in turn "function as a

189. Data Retention Directive, *supra* note 174.

190. SASSEN, TERRITORY, *supra* note 64, at 331.

191. *Id.* (noting, for example, the "strengthening of civic and political groups concerned with the extent to which private corporate interests are shaping Internet access and development").

192. *Id.* at 338.

political support and resources for the localities that constitute that network."[193]

The open government data movement offers an illustration of this phenomenon. Driven in part by a popular push towards greater transparency in government and in part by arguments of economic necessity—to fuel the information economy by making government data sets freely available in increasingly standardized digital formats—more and more states are now moving in this direction. Although some have initially tried to retain control over the formats in which information is disseminated, and the uses to which it can be put, these efforts are fading in the face of a growing push towards harmonization of standards, interoperability, and open access.[194] As Taubman puts it: "The growth of the Internet increasingly fuels a practical expectation, and bolsters a normative claim, that digital information should flow freely regardless of physical location."[195]

Other forms of grassroots Internet movements include the organization of major protests that actually take place in specific geographic locations (and that may involve the movement of individuals across borders). Those rallying around a particular cause may network so as to stage protests in major cities around the globe, or they may organize a convergence on a particular point for a particular purpose. This has notably been the case, for example, with the coordination of protests against G-20 summits.[196] Sassen writes that activism of this kind contributes "to an incipient unbundling of the exclusive authority, including symbolic authority, over territory and people we have long associated with the national state."[197]

Of course, in another fairly simple way the Internet erodes state jurisdiction by loosening the control a state may have over its citizens. While this is going to be felt more acutely under authoritarian govern-

193. *Id.* at 339.

194. For example, both Australia and New Zealand have very recently adopted policies on open government data. *See* Press Release, Lindsay Tanner, Dep't of Fin. & Deregulation, Gov't of Austl., Declaration of Open Government (July 16, 2010), http://agimo.govspace.gov.au/2010/07/16/declaration-of-open-government/; *New Zealand Government Open Access and Licensing (NZGOAL) Framework*, E-GOV'T N.Z. (Aug. 6, 2010), http://www.e.govt.nz/policy/nzgoal. The UK has also adopted an open government policy. NAT'L ARCHIVE, UK GOVERNMENT LICENSING FRAMEWORK FOR PUBLIC SECTOR INFORMATION (2010), *available at* http://www.nationalarchives.gov.uk/documents/information-management/uk-government-licensing-framework.pdf.

195. Taubman, *supra* note 62, at 27.

196. Trevor C.W. Farrow, *Negotiation, Mediation, Globalization Protests, and Police: Right Processes; Wrong System, Issues, Parties, and Time*, 28 QUEEN'S L.J. 665 (2003).

197. SASSEN, TERRITORY, *supra* note 64, at 340.

ments, there is a message here as well for all governments in the decentralization of sources of information. Benkler notes that "the introduction of Internet communications makes it harder and more costly for governments to control the public sphere."[198] Indeed, he goes on to argue that the Internet provides "avenues of discourse around the bottle necks of older media, whether these are held by authoritarian governments or by media owners."[199] While a state's jurisdiction is not formally removed in such circumstances, its ability to act effectively to control certain types of communication within its borders is dramatically reduced.

V. STATE RESPONSES

The preceding section highlighted the various challenges that the Internet, in the context of globalization, has posed for the exercise of jurisdiction by states. Recall that we are writing of jurisdiction in a very broad sense, and thus we conceive of the challenges as being not just to the ability of states to regulate this or that area, but rather to jurisdiction as the practical exercise of a state's sovereign capacity to govern. This section will distill, highlight, and further expand upon state responses to these challenges.

To restate generally, we described how the Internet has begun to erode the ability of the state to exercise jurisdiction. While the Internet is global, jurisdiction is not. Enforcement jurisdiction, in particular, is territorially limited unless states agree otherwise. Accordingly, the various apparatuses of the state have been faced with events, fields, and subject matters over which they desired to exercise jurisdiction, in no small part because they impacted the state's territory. However, to the extent that the effective exercise of jurisdiction meant being able to control extraterritorial actors, it was often frustrated or at least impeded by the need to accommodate the interests of other states. This is not new in and of itself, but the Internet has both multiplied the frequency and created new venues for this frustration to occur. Erosion also occurs as private parties, particularly corporations involved in international e-commerce transactions, opt for private arbitration and exclude the exercise of adjudicative jurisdiction by the courts. Large Internet-based companies such as Facebook and Google display inordinate bargaining power in their relationships with states, due to their globalized penetration into markets and the difficulties of regulating

198. BENKLER, *supra* note 69, at 270.

199. *Id.* at 271.

them. Moreover, the Internet has loosened the hold of governments on individuals generally, as information flow increases citizen empowerment and resistance to the state in both authoritarian and liberal-democratic manifestations.

We also noted three themes of state response to the Internet's challenges to jurisdiction: 1) state participation in governance regarding Internet architecture; 2) state facilitation of normative ordering for the Internet; and 3) state engagement with the reach of domestic laws onto the Internet. Specific manifestations along the lines of each theme are addressed and reflected upon below.

A. *Unilateral Territorial Measures*

As noted earlier, despite earlier romanticized notions of the Internet as a separate, self-regulating frontier, states quickly moved to take what actions they could in response to Internet activities which were conducted or felt on their territories.[200] Sometimes such actions have been problematic because of the interconnectedness of the medium. The various problems associated with state jurisdiction over Internet activities are often presented as being those primarily of extraterritorial jurisdiction. This is only accurate to a point. First, as explained in section II, *supra*, there is a distinction between an actual assertion of extraterritorial jurisdiction, and an assertion of territorial jurisdiction that has extraterritorial impacts. The former can present legal problems, while the latter typically only causes political problems. This is not to say that such political problems are not significant, or more frequent in the Internet era, or that they do not sometimes require legal solutions—of course they are, and do. However, despite any potential stretching effect the Internet's global connectedness has on the law of jurisdiction, states are nonetheless on fairly solid ground when trying to regulate and enforce matters that touch their own soil. Schultz writes instructively about an example of this, the imposition of filtering upon Yahoo! by the government of France:

> Filtering information that originated abroad certainly has extra-territoriality effects, as it influences and regulates the foreign actors' activities, typically increasing their costs of providing information into this territory. But these are 'extraterritorial spillover effects' of national regulations, as Jack Goldsmith

200. *See generally* THE RESURGENCE OF THE STATE: TRENDS AND PROCESSES IN CYBERSPACE GOVERNMENT (Myriam Dunn et al. eds., 2007).

> argues. And they are 'both inevitable and legitimate', and actually also very common. In the language of the distinctions drawn above, indirect extraterritoriality caused by obstacles is less objectionable than direct extraterritoriality involving sanctions. From a jurisdictional perspective, it is doubtless less objectionable for state *X* to make it impossible for residents of state *Y* to send certain information into the territory of state *X* than to impose economic penalties for the residents of state *Y* trying to send information into state *X*. As Jonathan Zittrain writes, '[i]mposing control on destination ISPs has been the approach of governments that wish to control the flow of content over the Internet but who cannot project that control beyond their boundaries'. This applies not only to governments that *cannot* project their regulatory actions beyond their boundaries but also those that *do not wish* to project such actions onto the territories of other states, seeking to avoid or limit the extraterritorial effects of their laws.[201]

Accordingly, states are competent to regulate activities that touch their soil as a matter of qualified territoriality, i.e. they have territorial legislative and enforcement jurisdiction. The extraterritorial spillover effects of their territorial actions may cause problems and engage the comity principle, causing a state to stand down or a court to refuse to enforce the judgment of a foreign court felt to be overreaching.[202] Indeed, this even works as a doctrine of law on the domestic level, as it is what the body of private international law regarding the assumption of jurisdiction over a case and enforcement of judgments is geared towards. Moreover, we share Goldsmith's view that "these spillovers do not affect the legitimacy of unilateral regulation, but they might argue for public and private harmonization strategies to eliminate the spillovers."[203] But this is not extraterritorial jurisdiction, i.e. not an assumption of jurisdiction over an event entirely outside the state's territory.

---

201. Schultz, *supra* note 102, at 825 (citations omitted).

202. For example, a New York court refused to enforce a judgment of a French court, an award of damages for copyright violation to a French company whose pictures were posted on an American website by a U.S. company. Louis Feraud Int'l SARL v. Viewfinder Inc., 406 F. Supp. 2d 274 (S.D.N.Y. 2005). Even though the pictures were the intellectual property of the French company and their publication on the website had a territorial link to France, the U.S. court held that the publication, which was done in the U.S., was protected by the First Amendment. *Id.* at 281–85.

203. Jack Goldsmith, *Unilateral Regulation of the Internet: A Modest Defence*, 11 EUR. J. INT'L L. 135, 136 (2000).

Second, and following the first, extraterritorial jurisdiction is essentially a problem of enforcement. As Goldsmith wrote, "the true scope and power of a nation's regulation is measured by its enforcement jurisdiction, not by its [legislative] jurisdiction."[204] For all the talk of extraterritoriality in the Internet context, states have for the most part been very wary of exercises of actual extraterritorial jurisdiction, both legislatively (in terms of passing laws that purport to regulate matters entirely outside their territories) and particularly in terms of enforcement jurisdiction. This makes sense intuitively, since as with most other policy areas, states tend to prescribe and enforce only in areas that affect their interests fairly directly. Accordingly, most of the problem areas have been in dealing with qualified territorial jurisdiction claims, since they inevitably involve concurrent jurisdiction with the legislatures and courts of other states, whether in private or public law areas. Exertions of extraterritorial legislative jurisdiction tend to be grounded on the existing principles, such as nationality[205] or, even at the outer reaches, protective jurisdiction over extraterritorial terrorist conspiracies such as is exerted by the U.S.[206] Instances of extraterritorial enforcement are rare, though they do cause conflict when they occur, and it is to conflict that we now turn.

B. *Conflict*

Jurisdictional matters have always caused conflict between states, and it is for this reason that both customary and treaty-based international law of jurisdiction, with its attendant principles, developed. It is hardly surprising that Internet-based activities would increase the points of conflict, since the chance of them occurring has expanded dramatically. Since enforcement issues can be felt quite keenly, it is also no surprise that states have clashed over the exercise of enforcement jurisdiction, particularly regarding cybercrime. For all the interconnectedness of the World Wide Web and other aspects of the Internet, territorial borders are still sacrosanct in international law, and this aspect of sovereignty is closely and jealously guarded. Despite years of negotiation and discussion,[207] little progress has been made on this point.

---

204. *Id.* at 139.

205. *See* Yulia A. Timofeeva, *Worldwide Prescriptive Jurisdiction in Internet Content Controversies: A Comparative Analysis*, 20 CONN J. INT'L L. 199, 201 (2005).

206. *See* Blakesley, *supra* note 26.

207. Most recently in the negotiations towards the formation of the Council of Europe Cybercrime Convention. *See* Henrik W.K. Kaspersen, *Jurisdiction in the Cybercrime Convention*, *in*

This is illustrated by the now-famous case of Gorshkov and Ivanov,[208] two Russian hackers who stole large amounts of personal information, including credit card numbers, from American Internet Service Providers (ISPs), online banks and e-commerce dealers. The hackers used this information for various acts of online theft and fraud. FBI investigators enticed the two to travel to Seattle, Washington using phony job interviews as a pretext, and monitored Gorshkov when he accessed his computer back in Russia, obtaining his login and password information. The investigators then arrested the two and used the information obtained to download the entire contents of Gorshkov's computer remotely. Russian authorities protested this investigation as an intrusion on their sovereignty, but were faced with U.S. denials on the basis that the agents had never left U.S. soil. The agents were later charged with hacking by the Russian government.[209]

Apart from outright illegality, enforcement barriers can lead to other kinds of inter-state conflict. Unable to effectively enforce laws against unlicensed online gambling on sites originating from Antigua and Barbuda, the U.S. began to enforce various federal laws against being involved in cross-border gambling enterprises and blocked American banks and financial companies from allowing funds to flow through to the gambling companies. In 2003 this led to Antigua and Barbuda bringing proceedings against the U.S. before the World Trade Organization, on the basis that this enforcement, while not impermissibly extraterritorial, constituted an unfair trade practice.[210] Antigua was successful at many turns of the case, at one point receiving an award of compensation in the form of a WTO-granted right to distribute copyrighted American materials in violation of licenses thereon.[211] In the Yahoo! case discussed above, the court of the Northern District of

---

CYBERCRIME AND JURISDICTION: A GLOBAL SURVEY 9, 19–21 (Bert-Jaap Koops & Susan Brenner eds., 2006); *infra* Section (c).

208. *See* Susan Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH TECH. L. 1, 21–23 (2004) (discussing this case); Press Release, U.S. Dep't of Justice, Russian Computer Hacker Convicted by Jury (Oct. 10, 2001), http://www.justice.gov/criminal/cybercrime/gorshkovconvict.htm.

209. John Leyden, *Russians Accuse FBI Agent of Hacking*, REGISTER (Aug. 16, 2002, 10:30 PM), http://www.theregister.co.uk/2002/08/16/russians_accuse_fbi_agent/.

210. ISAAC WOHL, INT'L TRADE COMM'N, THE ANTIGUA-UNITED STATES ONLINE GAMBLING DISPUTE (2009), *available at* http://www.usitc.gov/publications/332/journals/online_gambling_dispute.pdf.

211. *See* James Kanter & Gary Rivlin, *WTO Gives Antigua Right to Violate U.S. Copyrights in Gambling Dispute*, N.Y. TIMES, Dec. 21, 2007, http://www.nytimes.com/2007/12/21/business/worldbusiness/21iht-wto.html.

California would have refused to enforce the French order against Yahoo! Inc. because of the incompatibility of the order with the First Amendment's protection on freedom of speech. This straight jurisdictional conflict also represents a more passive kind of inter-state conflict, but one based on differing values that underpin public laws and how they are to be enforced.

One of the more chilling examples in this context is the exercise of enforcement jurisdiction by executive branches of governments to launch cyber-attacks against foreign targets, in violation of the laws of the receiving states and conceivably the laws of war.[212] This is an extreme example of jurisdictional overreach that is nonetheless empowered by the Internet, which could ultimately contribute to global catastrophe.[213]

C. *Formal Cooperation and Harmonization*

The entire premise of modern international law is that inter-state cooperation can preclude, resolve, or at least help to manage conflict between states, and the international community has made attempts to rise to the jurisdictional challenges described in sections III and IV above, by way of collaboration and mutual aid. The cybercrime arena again provides some of the most illustrative examples since, as this is the area where national sovereignty and public values are guarded most closely, the need for cooperation is that much greater. States have, of course, relied upon the traditional architecture of international criminal cooperation, such as extradition and the provision of mutual legal assistance. It is becoming more common to see fugitives extradited for computer-based crime that began in the requested state but was completed or caused effects in the requesting state, as states recognize the propriety of other states asserting criminal jurisdiction on a qualified territoriality basis. A good example is the case of Gary McKinnon, a UK national who is alleged to have hacked U.S. Defense Department computers and caused extensive damage, and who has been embroiled in extradition proceedings in the UK since 2002.[214] McKinnon's case

212. *See* Nasser Karimi, *Iran Revolutionary Guard Launches Cyber Attack: Report*, HUFFPOST WORLD, March 14, 2011, http://www.huffingtonpost.com/2011/03/14/iran-revolutionary-guard-cyber-attack_n_835489.html.

213. *See* PETER SOMMER & IAN BROWN, OECD, REDUCING SYSTEMIC CYBERSECURITY RISK (2011), *available at* http://www.oecd.org/dataoecd/57/44/46889922.pdf.

214. *See* Michael Goldfarb, *The Case of a Hacker with Asperger's Threatens the US-UK Relationship*, GLOBAL POST (Dec. 3, 2010), http://www.globalpost.com/dispatch/united-kingdom/101202/gary-mckinnon-extradition.

has, in fact, become something of a *cause celebre* in the UK, due in part to the fact that portions of the British public have objected to the breadth of the U.S.-UK 2003 extradition treaty (which imposes only modest burdens on the requesting state for establishing its case to justify extradition), and because many feel it is unfair for McKinnon to face the harsh U.S. sentencing regime when he could easily be prosecuted in the UK.[215] The case has led to a government inquiry into a potential overhaul of all of the UK's extradition arrangements.[216]

One of the most important efforts at addressing jurisdictional challenges in the public law arena has been the Council of Europe Convention on Cybercrime,[217] to which Canada and the U.S. are both signatories. The Convention has a twofold goal: to harmonize state laws relating to certain forms of computer crime (crimes against computers, crimes using computers, and crimes relating to child pornography and intellectual property infringement), and to provide mechanisms for inter-state cooperation in exercising investigative and enforcement jurisdiction in such cases.

Perhaps the most interesting aspect of the Cybercrime Convention is that, in working out how to manage inter-state cooperation in crimes with many jurisdictional touch points, states fell back on traditional jurisdictional principles, and quite conservatively so.[218] The convention requires parties to assert only territorial jurisdiction, and even modest extraterritorial jurisdiction is optional. There are quite developed mechanisms for cooperation and provision of mutual legal assistance, but these have all the hallmarks of inter-state cooperation between sovereign authorities. A negotiating effort to allow transborder investigation by state authorities, particularly access to computer data located abroad via computers in the investigating state, attracted little agreement during the negotiations which led to the treaty.[219] The only result was article 32, which allows state authorities to access extraterritorial data where the data is "publicly available (open source)"

---

215. *See* FREE GARY MCKINNON, http://freegary.org.uk/ (last visited May 28, 2011) (providing a great deal of information on the case, including links to media coverage and Parliamentary hearings).

216. *See* Tom Whitehead et al., *New Powers to Block Britons from Extradition*, TELEGRAPH (Sept. 6, 2010, 9:59 PM), http://www.telegraph.co.uk/news/politics/7985764/New-powers-to-block-Britons-from-extradition.html?utm_source=twitterfeed&utm_medium=twitter.

217. Cybercrime Convention, *supra* note 50; *see generally* Mike Keyser, *The Council of Europe Convention on Cybercrime*, 12 J. TRANSNAT'L L. & POL'Y 287 (2003).

218. *See* CURRIE, *supra* note 3, at 396–402 (providing a more detailed analysis).

219. COUNCIL OF EUR., CONVENTION ON CYBERCRIME: EXPLANATORY REPORT ¶¶ 293–94, http://conventions.coe.int/treaty/en/reports/html/185.htm (last visited May 28, 2011).

or if the state obtains the lawful and voluntary consent of a person who is legally entitled to disclose the data. As Brenner and Koops have noted, "territoriality still turns out to be a prime factor; apparently, cyberspace is not considered so a-territorial after all."[220]

In private international law areas, as discussed above, states have quickly discovered that the prospects for successful regulation are dependent upon cooperation. The approach has generally been to attempt to harmonize law, on the one hand, and harmonize the law of jurisdiction, on the other. Typically efforts have been channeled into negotiations via international or inter-governmental institutions, such as UNCITRAL and the Hague Conference on Private International Law. In neither branch has there been much success as yet. The Hague Conference made sustained efforts to lay a foundation for a treaty on jurisdiction, recognition, and enforcement of judgments, but in the end has only been able to reach sustained agreement on the more modest Convention on Choice of Court Agreements.[221] UNCITRAL's Model Law on E-Commerce has been influential, but the jurisdictional problems remain.

In the arena of the courts, moreover, the battle for clarity and for workable and commonly-shared principles still rages. The significant case law and enormous literature on Internet defamation strikes us, in particular, as emblematic of just how overplayed the rhetoric of the Internet as a globalized, borderless medium truly is. While the Internet has changed our modes of communication and the ease thereof, it has not truly globalized values to any great extent. These still emerge largely from national legal and cultural frameworks. To be sure, there are large swaths of the international community that share values, at least on a conceptual level (e.g. defamation is bad, contracts should be honored), but even on this plane the Internet has simply exposed their diversity. That is to say, even if a social or legal value is shared between two systems, the specifics may differ profoundly, or even the procedural laws, which are meant to allow for the vindication of those values, may vary widely.[222] This is not to deny the gathering strength of some globalized values which may shape the Internet in the future—the right to Internet access, the right to freedom of expression, the right to free

220. Brenner & Koops, *supra* note 208, at 6.

221. Convention on Choice of Court Agreements, E.U.-Mexico-U.S., June 30, 2005, 44 I.L.M. 1294, *available at* http://www.hcch.net/index_en.php?act=conventions.text&cid=98; *see* Bernhard Maier, *How Has the Law Attempted to Tackle the Borderless Nature of the Internet?*, 18 INT'L J.L. & INFO. TECH. 142, 171 n.199 (2010).

222. *See* KOHL, *supra* note 1, at 263–64.

flow of information—only to say that the impact of these on the law of jurisdiction is thus far nascent.

Interestingly, states are also engaged, alongside the business community, in efforts to remove e-commerce from the usual public sphere altogether, or at least as far as can comfortably be achieved. UNCITRAL has founded a working group that is examining globalized online dispute resolution (ODR) for cross-border electronic commerce transactions.[223] The rationale is expressed as follows:

> [T]raditional judicial mechanisms for legal recourse did not offer an adequate solution for cross-border e-commerce disputes, and that the solution—providing a quick resolution and enforcement of disputes across borders—might reside in a global online dispute-resolution system for small-value, high-volume business-to-business and business-to-consumer disputes. E-commerce cross-border disputes required tailored mechanisms that did not impose costs, delays and burdens that were disproportionate to the economic value at stake.[224]

In this model, then, law is harmonized in the sense that a generic code for online transactions (both "business-to-business and business-to-consumer"[225]) is formulated, and administered by private mediators. In essence, both prescriptive and adjudicative jurisdiction are ceded by states to the international institutional level; only enforcement jurisdiction remains local, since dispute resolution decisions would still need local execution.

VI. RECOMMENDATIONS

We are driven to the conclusion that, thus far in the history of the law of jurisdiction and the Internet, there is nothing new under the sun. That is to say, no new first principles have emerged in the international law of jurisdiction, and there is moreover no particular will on the part of states to create any. To be sure, refinement is both necessary and ongoing, particularly on the pernicious issue of what states are to do in

223. WORKING GROUP III, U.N. COMMISSION ON INT'L TRADE LAW, http://www.uncitral.org/uncitral/commission/working_groups/3Online_Dispute_Resolution.html (last visited May 28, 2011).

224. UNCITRAL, *Report of the United Nations Commission on International Trade Law*, ¶ 254, U.N. Doc. A/65/17 (June 21–July 9, 2010).

225. *Id.*

situations of concurrent territorial jurisdiction over public or private law matters, and it strikes us that the qualified territorial principle is ripe for expansion and clarification. Thus far, however, states—the primary actors in creating international law—are choosing to regulate, and if they wish to they will, despite such unflattering descriptions of this as "the new virtual 'land-grab.'"[226] Technology, the force that spawned the Internet, is now being used to erect cyber-borders along the lines of geographical ones, via ISP filtering and geolocation, *inter alia*. More such use is predicted[227] since, ironically, technology allows for more perfect realization of the traditional modes of asserting jurisdiction. To date, states have answered Geist's oft-quoted question[228] negatively—there is no "there" there, there is only here.

On the other hand, it seems clear that cracks are showing in the dam of state-exclusive Internet jurisdiction. As we said in section II, *supra*, the Internet is both the subject of new international governance frameworks, the object of increasingly harmonized state norms regarding infrastructure and conduct, and a venue by which individuals shape and form alliances and movements that transcend national boundaries. This is all in recognition of the fact that, as a driver of globalization itself, globalized communication of the kind allowed by the Internet both amplifies existing legal problems and creates others. If those problems can be summed up at all neatly, it might be by the word "uncertainty." Individuals who use the Internet are uncertain as to whether their actions might expose them to another state's law, which might be unknown to them and/or might conflict with the law of the state in which they are acting. Wronged consumers of e-commerce products are uncertain whether they will be able to obtain remedies by court process or arbitration, or whether their state's consumer protection laws will extend to, or be enforceable against, the other parties to their transaction. Conflict of state laws means commercial actors are uncertain whether they can enforce judgments obtained in one state before the courts of another. Prosecutors are uncertain of whether they have jurisdiction to prosecute particular cases, or whether the authorities of other states will agree with their jurisdictional claims.

---

226. Lillian Edwards, *Caveat Uploader? Recent Developments in Cyberspace Jurisdiction*, SCRIPTED, http://www.law.ed.ac.uk/ahrc/script-ed/elaw/caveat.asp (last visited May 28, 2011).

227. Schultz, *supra* note 102; *see* Svantesson, *supra* note 74, at 353; *see also* Andrea M. Matwyshyn, *Of Nodes and Power Laws: A Network Theory Approach to Internet Jurisdiction Through Data Privacy*, 98 NW. U.L. REV. 493 (2004).

228. Michael Geist, *Is There a There There? Towards Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345 (2002).

Uncertainty, of course, is undesirable. It creates economic inefficiency and sometimes unwieldy cost. It suppresses freedom of action in any number of sectors. Can the law of jurisdiction be utilized or evolve in such a way as to mitigate this uncertainty in the Internet context?

We feel it is important to keep in mind that, ultimately, jurisdiction is just a tool of substantive law, and substantive law in turn is simply a tool of policy. As this paper has been about the concept of jurisdiction writ large, so too must our solutions be writ large. We cannot hope to propose how, why or if some particular development in the laws relating to jurisdiction and the Internet will be salutary or successful in any of the various areas of law we have used as specific examples. That said, in light of our conclusion above that no new "first principles" in the law of jurisdiction are emerging, we offer two sets of conclusions: first, a set of "first principles" about jurisdiction, in the form of policy precepts; and second, a set of forecasts about how states may, can, and should innovate.

A. *New First Principles*

Our new first principles about jurisdiction in the Internet age are founded upon two main premises. The first is that the Westphalian model of sovereign states is certainly evolving, but will remain extant for the foreseeable future. The international community will evolve towards more global governance via supranational institutions, but the state will remain a viable entity. It not only provides most efficiently and effectively for localized law-making and law-enforcing, but is still one of the primary vehicles for the legitimate expression of values by its citizens.

The second premise is that the legal regime surrounding enforcement jurisdiction is unlikely to see any significant change. There will continue to be some coordination of enforcement, as with article 32 of the European Cybercrime Convention, but enforcement will still be mostly territorially limited. There will remain a need for a domestic local machinery (police, sheriff, courts) to enforce. In private international law, where public authorities do enforce the judgments of other states (unlike public law areas, for the most part), local procedural values are quite diverse. This will remain a perennial problem for private international law, likely to be addressed only by international harmonization of both substantive law and the law of recognition and enforcement.

With these premises in mind, we offer the following first principles:

- Individuals are entitled to notice, in the sense of knowledge of what law pertains to their Internet activities. They need notice of the law

of jurisdiction (when the state is going to regulate their actions) and they need notice of the substance of that law. This is a general principle of international law, and applies across both private and public law.

- The Internet is fast becoming a major part of the architecture of the globalized world. Accordingly, its status under international law requires reconceptualizing. It is, of course, a set of interconnected computer networks linked to state territory and thus is liable to the exercise of sovereign jurisdiction on a territorial basis. However, the interconnectedness means that, while states will continue to control various aspects of the Internet, it will never totally be in their grasp, either individually or collectively. Accordingly, the Internet is a new kind of *res communis*, as has been touched upon in the literature.[229] Alternatively, it may be more analogous to the principle of "common heritage of mankind" as that phrase has been used in the law of the sea context. The Internet is different from those other areas of the earth deemed to be *res communis*, because rather than being in the jurisdiction of no state, it is within the territorial jurisdiction of every state. Accordingly, collective action is required for its governance, to the extent governance is possible and desirable.
- The collective governance referred to above should not exclusively be driven by states. Naturally, states will be primary players. However, what is needed is more civil engagement, more public-private partnership on technology development, and more co-ordination of state activity, particularly in the rationalization of private international law rules regarding the Internet.
- While this may be more of an ideological stance, in our view some form of democratic accountability is required, regarding both the architecture of the Internet and its regulation.
- As the law grows more specialized, so too must the law of jurisdiction. The customary international law of jurisdiction is unlikely to see more explicit or active development. Instead, coordination and harmonization will go on a sector-by-sector basis, indirectly causing the evolution of customary international law principles.
- In e-commerce, both consumers and vendors should have, and ultimately will require, both stable and secure architecture and a fair and equitable dispute resolution system. The decisions of the

229. *See* Svantesson, *supra* note 74, at 362–64.

dispute resolution system should be enforceable, as necessary, within national legal systems.

B. *Forecasts and Suggestions*

Our thinking on the future of Internet jurisdiction is driven, in the first instance, by proposals put forth in two very interesting recent pieces of scholarship. The first is Kohl's book, *Jurisdiction and the Internet: Regulatory Competence Over Online Activity*.[230] In her final chapter, Kohl expresses the view that resolving the conundrums of Internet jurisdiction comes down to a choice of tools, which she places under the umbrellas of "more global law" or "a less global Internet." The former comprises harmonization of rules regarding jurisdictional competence, and harmonization of substantive law, by treaty, by deregulation (private imposition of code, user self-help) or by default (courts adopting country of origin/destination approaches). The latter category, "less global Internet," presents the assertion of state jurisdiction over the Internet on a territorial basis, using technology (particularly "zoning") to focus Internet activities on either the state of origin or of destination. She notes the tension embodied in this bifurcated approach—recognition that there is much in local law, culture and social values that is worth retaining, but also appreciating the value of unfettered Internet communication and its potential to positively advance the causes of humanity.

In "Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface,"[231] Schultz posits that the Internet will essentially be "carved up" into two streams. The first is the "vertical" stream, where in public affairs, states will regulate most everything that is within their policy precepts, because technology will develop in such a way as to allow them to do so.[232] The second "horizontal" stream will be observed where online commercial "communities" (i.e. electronic marketplaces) will generate their own normative orders, buttressed by increasingly shared values and technological solutions. These new "normative environments" will become "largely divorced from public legal systems," producing "a patchwork of private

230. KOHL *supra* note 1, at 253–87.

231. Schultz, *supra* note 102.

232. Schultz fears the "impoverishment" of the Internet that could result from this, and proposes a combination of the targeting principle and a modified effects doctrine to maintain order. *Id.*

legal orders each specific to an online marketplace or to an equivalent context of Internet activities."[233]

Both authors are predictive, though Schultz is more prescriptive. However, we feel that their writing accurately captures the forward movement on this issue of Internet jurisdiction, which can be encapsulated by the word "lurching." Perhaps it was ever thus with the forward march of human progress. However, ideally at least, the Internet itself and the values that are growing up around it present an opportunity for a more truly globalized exploration and confluence of norms than was ever present before. It is increasingly clear that states cannot dominate the discourse, nor should they. The Internet is an ideal forum for the concretization of deliberative democracy, the idea that binding, collective, and legitimate decisions can only be made by deliberation, a public exchange of views between equal participants that creates binding agreements on form, substance, procedure, and enforcement.[234] Although they may not map perfectly onto the Internet setting, the foundational ideas behind deliberative democracy are *a propos* to the Internet.[235]

VII. CONCLUSION

Whether the international community is up to the challenge of using deliberative democracy to shape both Internet governance and the way in which state jurisdiction maps onto Internet activity is an open question. It is true that the Internet Governance Forum, discussed in section III above, was given a composition that is far more inclusive of a broader set of stakeholders than traditional international institutions. The potential for the creation of a more inclusive forum exists, and there may be more to work with today in terms of precedent and

233. *Id.* at 831–37 (using the eBay dispute resolution system as an example of such a "normative system which is autonomous").

234. *See generally* Joshua Cohen, *Deliberation and Democratic Legitimacy*, *in* THE GOOD POLITY: NORMATIVE ANALYSIS OF THE STATE 17 (Alan Hamlin & Philip Pettit eds., 1989). Of course, the potential for active deliberation and participatory democracy by electronic means has its own rich literature and schools of adherents and critics. *See, e.g.*, DEMOCRACY ONLINE: THE PROSPECTS FOR POLITICAL RENEWAL THROUGH THE INTERNET (Peter M. Shane ed., 2004).

235. Andrew Chadwick, *Web 2.0: New Challenges for the Study of E-Democracy in an Era of Informational Exuberance*, 5 I/S: J. L. & POL'Y for INFO. SOC'Y 9, 1 (2009). *See generally* JOHN PARKINSON, DELIBERATING IN THE REAL WORLD: PROBLEMS OF LEGITIMACY IN DELIBERATIVE DEMOCRACY (2006); JOHN DRYZEK, DELIBERATIVE DEMOCRACY AND BEYOND: LIBERALS, CRITICS, AND CONTESTATIONS (2000); AMY GUTMANN & DENNIS THOMPSON, WHY DELIBERATIVE DEMOCRACY? (2004); DELIBERATION, PARTICIPATION, AND DEMOCRACY: CAN THE PEOPLE GOVERN? (Shawn Rosenberg ed., 2007).

willingness than there has ever been before. The Internet itself is a tool to address the lack of resources to spend on participation, which might otherwise be a bar to having a more inclusionary governance structure. This remains the promise and challenge of the Internet: an opportunity to rethink fundamental principles of state sovereignty, citizen engagement, and international governance in a time of significant technological change and social transformation.