> jurisdiction by reference to the place where the offence is committed; second, the nationality principle, determining jurisdiction by reference to the nationality or national character of the person committing the offence; third, the protective principle, determining jurisdiction by reference to the national interest injured by the offence; fourth, the universality principle, determining jurisdiction by reference to the custody of the person committing the offence; and fifth, the passive personality principle, determining jurisdiction by reference to the nationality of national character of the person injured by the offence. Of these five principles, the first is everywhere regarded as of primary importance and of fundamental character. The second is universally accepted, though there are striking differences in the extent to which it is used in the different national systems. The third is claimed by most states, regarded with misgivings by a few, and generally ranked as the basis of an auxiliary competence. The fourth is widely, though by no means universally accepted as the basis of an auxiliary competence, except for the offence of piracy, with respect to which it is the generally recognised principle of jurisdiction. The fifth, asserted in some form by a considerable number of states and contested by others, is admittedly auxiliary in character and is probably not essential for any state if the ends served are adequately provided for by another principle.[13]

The commentary to the Harvard Research Draft Convention on Jurisdiction with Respect to Crime 1935 identified five general principles, namely:

(a) the territorial principle;

(b) the passive personality principle;

(c) the nationality principle;

(d) the protective principle; and

(e) the universality principle.

Discussion of the application of these principles will form the main part of this chapter. Before looking at them in detail, it is necessary to consider some issues raised by the assertion of civil jurisdiction. One final introductory point needs to be made: this chapter is concerned with the exercise of jurisdiction by states on the municipal plane. Questions of jurisdiction also arise on the international plane and the subject of international criminal jurisdiction will be discussed in Chapter 9.

8.2 Civil jurisdiction

The rules relating to the exercise of civil jurisdiction have tended to be more flexible than those relating to criminal jurisdiction. Some writers have argued that there in fact exist no clear rules of customary international law governing the exercise of civil jurisdiction, although there are an increasing number of treaties dealing with the matter. The traditional rule in the common law countries was that courts would have jurisdiction over civil disputes if the defendant was present in the territory, no matter for how short a period. Civil law countries have tended to operate on the basis that the defendant is habitually resident within the territory where jurisdiction is to be assumed. The position within the European Union is governed by the Brussels Convention on

13 Dickinson, 'Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime 1935' (1935) 29 *AJIL*, Supp 443.

Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters 1968. This provides the general rule that persons domiciled in a contracting state must be sued in the courts of that state alone, although there are two main exceptions to this rule. The Brussels Convention is incorporated into English law by the Civil Jurisdiction and Judgments Act 1982. The 1982 Act has since been amended to incorporate the Lugano Convention 1989, which extends the Brussels Convention regime to those states which are members of the European Free Trade Association.

As far as matrimonial cases are concerned, the generally accepted ground for exercising jurisdiction is the domicile or habitual residence of the party bringing the action, and this rule is reflected in the Hague Convention on the Recognition of Divorces and Legal Separations 1970.

For a full discussion of the rules relating to the exercise of civil jurisdiction reference should be made to a textbook on private international law. As far as public international law is concerned, disputes about jurisdiction have usually arisen when a state has attempted to exercise criminal jurisdiction over non-nationals or in respect of actions that have occurred outside the state's own territory.

8.3 Territorial principle

The ability of a state to exercise jurisdiction over crimes committed within its territory is an essential attribute of sovereignty, and the territorial principle has received universal recognition.

According to the territorial principle, events occurring within a state's territorial boundaries and persons within that territory, albeit temporarily, are subject to local law and the jurisdiction of the local courts. The principle has practical advantages in terms of availability of witnesses.

Application of the territorial principle will usually be straightforward where the crime has been committed wholly within the territory. However, it is not always possible to decide on the exact location of the crime. The activities constituting the offence may have taken place in more than one state, for example, suppose X fires a gun in state A killing someone in state B. Which state can claim territorial jurisdiction? Under what is known the 'subjective territoriality principle', state A has jurisdiction, since that is where the offence was commenced. Under the 'objective territoriality principle', state B has jurisdiction, since that is where the offence was completed and had its effect. Both principles are recognised by international law and thus, in the example, both state A and state B would have concurrent jurisdiction.

An example of the subjective territorial principle is found in *Treacey v DPP* (1971).[14] The appellant had written and posted in the Isle of Wight a letter addressed to Mrs X in Germany which demanded money with menaces. Mrs X received the letter in Germany but informed the British police. Treacey was convicted of blackmail and his conviction was upheld by a majority in the House of Lords. Lord Diplock stated that:

14 [1971] AC 537.

> There was no principle of international comity to prevent Parliament from prohibiting under pain of punishment persons who are present in the United Kingdom, and so owe local obedience to our law, from doing physical acts in England, notwithstanding that the consequences of those acts take effect outside the United Kingdom.

In *DPP v Doot* (1973),[15] the respondents were convicted of conspiracy to import cannabis into the UK. The House of Lords held that the English courts had jurisdiction over the case, even though the actual conspiracy took place abroad, since the offence continued to occur in England when the conspiracy was carried out. Lord Wilberforce stated:

> The present case involves 'international elements' – the accused are aliens and the conspiracy was initiated abroad – but there can be no question here of any breach of any rules of international law if they are prosecuted in this country. Under the objective territorial principle ... or the principle of universality (for the prevention of narcotics falls within this description) or both, the courts of this country have a clear right, if not a duty, to prosecute in accordance with our municipal law.'

It should be noted that recently, the English courts have moved away from a strict application of the subjective or objective territorial principle. Thus in *Somchai Liangsiriprasert v Government of the USA* (1990)[16] Lord Griffiths commented:

> The English courts have decisively begun to move away from definitional obsessions and technical formulations aimed at finding a single *situs* of a crime by locating where the gist of the crime occurred or where it was completed. Rather, they now seem by an examination of relevant policies to apply the English criminal law where a substantial measure of the activities constituting a crime take place in England, and restrict its application in such circumstances solely in cases where it can seriously be argued on a reasonable view that these activities should, on the basis of international comity, be dealt with by another country.

A controversial example of the application of the objective territorial principle is provided by the *Lotus* case (1927). The case arose following a collision on the high seas between a Turkish and a French ship. As a result of the collision the Turkish vessel sank and a number of crew members and passengers drowned. The French ship put into port in Turkey and a number of French crew members were arrested and subsequently tried and convicted of manslaughter. France raised objections to the exercise of jurisdiction by Turkey and the dispute was submitted to the PCIJ. Turkey argued that ships on the high seas formed part of the territory of the state whose flag they fly. They therefore argued that jurisdiction could be exercised on the basis of the objective territorial principle, since the consequences of the French act had occurred on Turkish territory. The PCIJ found in favour of Turkey by the casting vote of the President of the Court. The decision has been criticised for the suggestion it makes that states have a wide measure of discretion to exercise jurisdiction which is only limited to the extent that there are specific prohibitive rules. In other words, the onus is on the

15 [1973] AC 807.

16 [1990] 3 WLR 606.

one disputing jurisdiction to provide evidence of a rule restricting jurisdiction. The better view today seems to be that it is the one asserting jurisdiction that must show a relevant permissive rule of international law. It is also important to note that the view that a ship forms part of the territory of the flag state is no longer correct. Questions of jurisdiction on board ships will be discussed in Chapter 10 and jurisdiction on board aircraft will be dealt with in Chapter 11.

> Where is cyberspace?[17] The answers seem to approach the metaphysical: it is everywhere and nowhere; it exists in the smallest bursts of matter and energy, and is called forth only by the presence of man through the intercession of an Internet Provider. If the answers are useless, it only shows that we are asking the wrong question. We want to ask first: what is cyberspace? Here, at least a functional answer is possible. Functionally, cyberspace is a place. It is a place where messages and webpages are posted for the whole world to see, if they can find them.[18] It is no further than your own computer terminal, but never closer than your image in a mirror.
>
> Unfortunately, when the common law confronts cyberspace the usual mode of analysis is analogy: not 'What is cyberspace?' but 'What is cyberspace like?' The answers are prosaic: a glorified telephone, a bookstore, a bulletin board. At the common law there is nothing new under the sun.[19] I propose that we must look at cyberspace through the lens of international law in order to properly give cyberspace a home in our laws.[20]
>
> The thesis of this paper is that there exists at international law a category which I call an 'international space'. Currently there are three such international spaces: Antarctica, outer space, and the high seas. For jurisdictional analysis, cyberspace should be treated as a fourth international space.
>
> After all, in cyberspace, jurisdiction is the overriding conceptual problem for domestic and foreign courts alike. Unless conceived of as an international space, cyberspace takes all of the traditional principles of conflicts-of-law and reduces them to absurdity. Whereas a thorny jurisdictional problem might traditionally involve two, three, even six or seven conflicting jurisdictions, the universe of laws which can apply to a simple homespun webpage is all of them. Jurisdiction

---

17 The term 'cyberspace' is sometimes treated as a synonym for the internet, but is really a broader concept. For example, we know exactly how the internet began, but not at what point the connections between a few domestic computers metamorphosed into a global virtual community that we now call cyberspace. I prefer the term because it emphasises that it can be treated as a place. William Gibson is credited with coining the term in his novel '*Neuromancer*.' Gibson's concept included a direct brain-computer link that gave the user the illusion of vision, moving about in the data 'matrix' to obtain information. William S Byassee, 'Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community', 30 *Wake Forest L Rev* 197, 198 n 5.

18 In his book *Wyrm*s, science fiction author Orson Scott Card describes a most remarkable place called Heffiji's house, which could have been a metaphor for cyberspace. Heffiji had a sign on her house reading 'Answers' that lured many curious people. She asked questions of all her visitors and wrote the answers down on scraps of paper. These scraps of paper were scattered all around her enormous house. Unfortunately she had no brain, so she could not learn anything. She did, however, know where she had put the pieces of paper, and you could learn anything from her if you asked the right question.

19 Ecclesiastes 1:9. Solomon could well have been speaking of cyberspace when he wrote, 'For a dream comes with much business, and a fool's voice with many words'. Ecclesiastes 5:3.

20 It is hornbook custom to cite *The Paquete Habana* for the proposition that 'international law is part of our law': *The Paquete Habana*, 175 US 677 (1900). With apologies to Voltaire: if *The Paquete Habana* did not exist, it would be necessary to invent it.

in cyberspace requires clear principles, and better principles rooted in international law, so that courts in all nations may be persuaded to the same conclusions.

I Principles of jurisdiction

There are three types of jurisdiction generally recognised in international law. These are the jurisdiction to prescribe, the jurisdiction to enforce, and the jurisdiction to adjudicate.[21] The jurisdiction to prescribe is the right of a state to make its law applicable to the activities, relations, the status of persons, or the interests of persons in things.[22] This paper deals almost exclusively with the jurisdiction to prescribe. However, it is useful here to note the distinction between the jurisdiction to prescribe a rule of law for a particular action and the jurisdiction to enforce that rule. This paper will not discuss extradition.

Under international law, there are six generally accepted bases of jurisdiction, usually listed in the order of preference:

1 Subjective territoriality
2 Objective territoriality
3 Nationality
4 Protective principle
5 Passive nationality
6 Universality

These bases of jurisdiction are theories under which a state may claim to have jurisdiction to prescribe a rule of law over an activity. Even where one of the bases of jurisdiction is present, the exercise of jurisdiction must still be reasonable.[23]

Subjective territoriality is by far the most important of the six. If an activity takes place within the territory of the forum state, then the forum state has the jurisdiction to prescribe a rule for that activity. The vast majority of criminal legislation in the world is of this type.

Objective territoriality is invoked where the action takes place outside the territory of the forum state, but the primary effect of that activity is within the forum state. The classic case is that of a rifleman in Canada shooting an American across Niagara Falls in New York. The shooting takes place in Canada; the murder – the effect – occurs in the United States. United States would have the jurisdiction to prescribe under this principle. This is sometimes called 'effects jurisdiction'. This has obvious implications for cyberspace, as will be discussed below.

Nationality is the basis for jurisdiction where the forum state asserts the right to prescribe a law for an action based on the nationality of the actor. Under Dutch law, for example, a Dutch national 'is liable to prosecution in Holland for an offence committed abroad, which is punishable under Netherlands law and which is also punishable under the law of the country where the offence was committed'.[24] Many other civil law countries have similar laws, notably France.

21 Restatement (Third) of Foreign Relations, SS 401.

22 *Ibid*, SS 402.

23 Restatement SS 403.

24 *Public Prosecutor v Y*, Supreme Court, 1957 (1961) 24 *Int L Rep* 265, 265.

Passive Nationality is a theory of jurisdiction based on the nationality of the victim. Often passive and 'active' nationality are invoked together to establish jurisdiction. A state has more interest in prosecuting an offence when both the offender and the victim are nationals of that state. This principle is rarely used for two reasons. First, it is offensive to insist that foreign laws are not sufficient to protect your citizens abroad. One of the complaints that sparked the Boxer rebellion in China in 1901 was the privilege of foreigners to be tried only by their own laws. There actually was a US District Court for China during this period. Second, the victim is not being prosecuted. You need to seize the actor in order to have a criminal prosecution.

The Protective Principle is often seen as the ugly stepchild of Objective Territoriality. This principle expresses the desire of a sovereign to punish actions committed in other places solely because it feels threatened by those actions. This principle is invoked where the 'victim' would be the government or sovereignty itself. For example, in *United States v Rodriguez*, 182 F Supp 479 (SD Cal 1960), the defendants were charged with making false statements in immigration applications while they were outside the United States. This principle is disfavoured for the obvious reason that it can easily offend the sovereignty of another nation. Such cases are usually referred to the State Department, not the Justice Department.

The final basis of jurisdiction is Universal jurisdiction, sometimes referred to as 'universal interest' jurisdiction. Historically this was the right of any sovereign to catch and punish pirates. This has expanded during the past century and a half to include more of *jus cogens*: slavery, genocide, and hijacking (air piracy).[25] Although this may at first glance seem extendible to net piracy in the future, to computer hacking and viruses, this is unlikely given the traditionally tortoise-like development of the universal jurisdiction. Just as important, universal jurisdiction traditionally covers only very serious crimes.[26] Because it covers serious crimes, all nations have due-process-like problems with convictions under this principle.

The general mode international conflicts-of-law analysis is to weigh the interests of competing states in determining whether there is jurisdiction to prescribe. Although subjective territoriality usually trumps other interests, a strong state interest in protecting its nationals can outweigh a weak state interest in prosecuting the crime on its own soil.

It is not always clear what it means for an individual defendant if the state lacks the jurisdiction to prescribe law. Under some domestic legal systems, a defendant will be released if the court purported to convict the defendant where there was no jurisdiction to prescribe. In the United States, this question is nastily intertwined with due process analysis and presumptions about the intent of Congress to violate international law. The court will construe US law, where possible, to conform to international law. I will not attempt to extricate it here. At a minimum under international law, a claim will accrue to the state whose sovereignty is offended by the conviction of its national.

---

25 *Jus cogens*, 'compelling law' means a peremptory norm of general international law from which no derogation is permitted.

26 See, eg, US Constitution, Art I, Sec 8 (granting Congress the right 'To Define and Punish Piracies and Felonies committed on the High Seas, and Offenses against the Law of Nations').

II The theory of the uploader and the downloader

Man interacts with cyberspace in two primary ways: we put information in cyberspace; we take information from cyberspace. Both actions are limited and concrete, and can be performed in the safety and comfort of one's own home. At law in cyberspace, then, there are two distinct actors: the uploader and the downloader.[27] Under this theory, the uploader and the downloader act like spies in the classic information drop – the uploader puts information into a location in cyberspace, and the downloader accesses it at a later time. Neither need be aware of each other's identity. Unlike the classic information drop, however, there need not be any intent to communicate at all: a webpage is just a *vox clamantis in deserto*.[28] Some pages are accessed by thousands of random people all over the world, while others languish as untrodden paving stones in the infinite paths of cyberspace.

In both civil and criminal law, most actions taken by uploaders and downloaders present no jurisdictional difficulties. A state can forbid, on its own territory, the uploading and downloading of material it considers harmful to its interests. A state can therefore forbid anyone from uploading a gambling site from its territory, and can forbid any one within its territory from downloading, ie interacting,[29] with a gambling site in cyberspace.

Two old American cases demonstrate how this theory would play out. *The Schooner Exchange* (1812) held that a French war vessel was not subject to American law, although it was in an American port.[30] A webpage would be ascribed the nationality of its creator, and not subject to the law of wherever it happened to be downloaded.

The *Cutting* case (1887) provides an example of how an uploader should be viewed in a foreign jurisdiction which is offended by material uploaded into cyberspace. Mr Cutting published an article in Texas which offended a Mexican citizen. When Mr Cutting visited Mexico he was incarcerated on criminal libel charges. The Secretary of State instructed the American ambassador to inform the Mexican government that 'the judicial tribunals of Mexico were not competent under the rules of international law to try a citizen of the United States for an offence committed and consummated in his own country, merely because the person offended happened to be a Mexican'.[31] As a general proposition, where uploading certain material is a crime, it is an offence 'committed and consummated' in the state where the uploader is located.

III Rejecting territoriality: the trouble with Minnesota

There is no doubt that what many states want to do is altogether more troubling: states want to exercise jurisdiction over uploaders (and to a lesser extent,

27 I am here ignoring direct communication over the internet, involving e-mail. This will be dealt with later. Suffice it to say now that these direct communications do not present the same conflict-of-laws problems as general postings to the world.

28 The voice of one crying out in the desert. Matthew 3:3; Isaiah 40:3. Whether cyberspace is preparing the way for the Lord is beyond the scope of this paper.

29 Interacting may involve considerably more than downloading, but it always involves the act of downloading.

30 *The Schooner Exchange v McFaddon* (1812) 11 US (7 Cranch) 116. We can ignore for now the question of whether the ship's status as a war vessel was dispositive. The 'temporary presence' doctrine was elaborated in later cases.

31 Letter, Secretary of State to United States Ambassador to Mexico, Department of State, Washington, 1 November 1887.

downloaders) outside their own territorial boundaries. Minnesota is apparently the first jurisdiction (it is no coincidence that this is a jurisdiction not traditionally involved with foreign relations) to attempt a general exercise of such jurisdiction. Minnesota's Attorney General, Hubert Humphrey III, has issued a memorandum stating that 'Persons outside of Minnesota who transmit information via the internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws'.[32]

Their concerns are no doubt sincere, but the memorandum is somewhat less than sincere. Of course everybody 'knows' that all information in cyberspace will be downloaded in Minnesota. It is totally foreseeable. Minnesota's rule makes all of cyberspace subject to Minnesota law. Naturally, if every state took this approach (and under Minnesota's guidelines, there is no reason why every state could not) the result would be unbearable, especially for multinational corporations with attachable assets lying all over the world. Much more sensible is the opinion of the Florida Attorney General that 'the resolution of these matters must be addressed at the national, if not international, level'.[33]

The Minnesota Attorney General has laid out a simple syllogism, of the sort that is always suspect: anyone who 'being without the state, intentionally causes a result within the state prohibited by the criminal laws of this state' is subject to prosecution in Minnesota.[34] This simple approach, appealing at first, dissolves upon a sufficiently textured international legal analysis.

An interesting question for strict constructionists, which need not detain us here, is whether, under the federal system, Minnesota has any obligations under international law. As a practical matter, Minnesota, as well as all states and nations, will be constrained by international law. One can observe that the Supreme Court always interprets Congressional mandates, where possible, in accordance with international law, and that presumption is surely stronger against state legislatures. Indeed, most provisions of US foreign relations law are designed to keep international questions in federal hands. Treaties, of course, are the 'supreme law of the land', superior to any state law (US Constitution, Art VI). At any rate, considerations of comity, which are underdeveloped and often thinly conceived in relations between the United States, will be important if Minnesota attempts to assert this jurisdiction internationally.[35]

Minnesota's approach has several problems. First, Minnesota has ignored the presumption against extraterritorial application of US laws. It seems that the Minnesota Attorney General was under the impression that, because the mode of analysis for conflicts-of-law is the same for conflicts between American states as for a conflicts between an American state and a foreign country, the results will also always be the same. Of course they will not. The sovereignty of individual American states is not as easily offended (or defended) as the sovereignty of

32 Memorandum of Minnesota Attorney General.

33 Florida Attorney General, Formal Opinion: AG 95–70 (October 18, 1995).

34 Minnesota Statute SS 609.025 (1994) (cited in Memorandum of the Minnesota Attorney General).

35 Comity is the respect courts accord one another and the laws of other sovereigns. Like *forum non conveniens*, it is (in common law countries) a judge-made doctrine for declining jurisdiction. Civil law countries invoke comity more with statute than *sua sponte* court action. See generally Brian Pearce, *The Comity Doctrine as a Barrier to Judicial Jurisdiction: A US–EU Comparison* (1994) 30 *Stan J Int L* 525.

nation states. To put it another way, courts will accord France's interest in its sovereignty greater weight than Delaware's. This is especially true of French courts. Under the theory of international spaces, outlined below, Minnesota has no jurisdiction to prescribe law over objects in cyberspace because, under the federal system, Minnesota has no 'nationality' to assert. Nationality is, well, national, and the jurisdiction predicated thereon is federal.[36] Minnesota is not accustomed to dealing with international law, and it shows.

Second, Minnesota has conflated *in personam* jurisdiction with the jurisdiction to prescribe law. The former is subject to the 'minimum contacts'[37] analysis; the latter is not. A nexus with Minnesota territory sufficient to establish *in personam* jurisdiction over a defendant may not be sufficient to give Minnesota the jurisdiction to prescribe a rule of law for the action. Indeed, Minnesota courts may have *in personam* jurisdiction over a defendant but may, according to their own choice-of-law statutes, choose to apply foreign law in the case at hand. In criminal cases, where there is no jurisdiction to prescribe a rule of law, there is no jurisdiction at all.[38]

Minnesota has chosen to rely on 'effects' jurisdiction or 'objective territoriality', where it is the territoriality of the object state, rather than (or in addition to) that of the subject actor, which prescribes the rule of law. The 1965 Restatement (Second) of Foreign Relations described objective territoriality as the following:

> A state has jurisdiction to prescribe a rule of law attaching legal consequences to conduct that occurs outside its territory and causes and effect within its territory if either:
>
> (a) the conduct and its effect are generally recognised as constituent elements of a crime or tort under the law of states that have reasonably developed legal systems;[39] or
>
> (b) (i) the conduct and its effect are constituent elements of activity to which the rule applies;
>
> (ii) the effect within the territory is substantial;
>
> (iii) it occurs as a direct and foreseeable result of the conduct outside the territory; and
>
> (iv) the rule is not inconsistent with the principles of justice generally recognised by states that have reasonably developed legal systems. *The Restatement (Second) of Foreign Relations SS 18.*

Minnesota's rule misses the texture of this description. None of these cyberspace 'crimes' can meet part (a) of the test, because none of these are traditional crimes, generally recognised, and because the act of uploading is not currently a constituent element of any crime anywhere. Part (b) of the test is where the action is. It speaks of substantial effect and principles of justice generally recognised. Moreover, considerations of comity always play a major role in a basis of jurisdiction so offensive to foreign sovereignty. Objective territoriality is

36 This is not to say that federal courts may not turn to the state of residence of the criminal for the substantive law. This paper is about international jurisdiction, not federal jurisdiction.

37 *International Shoe v Washington* 326 US 310 (1945).

38 For example, an American court cannot convict a Swiss citizen for violation of Swiss law. *Habeas corpus* review would be swift and sweet for the defendant. The remedy here is extradition.

39 The older language was 'civilised nations'. No doubt in American and European courts it still means 'civilised nations' with all that implies.

not a blanket to be thrown over cyberspace, but is appropriate only in unusual circumstances. Minnesota needs to find another basis for asserting general jurisdiction over actions in cyberspace.

IV Rejecting territoriality: 'the law of the server'

Another poor approach to jurisdiction in cyberspace is to treat the location of the server where webpages are 'located' as the place of a criminal action for the purposes of territorial jurisdiction. Under this theory, a webpage 'located' on a server at Stanford University is subject to California law. Where the uploader is also in the forum state, or is a national of the forum state residing abroad, this approach is consistent with the theory of jurisdiction in international spaces.

But where the uploader is in a foreign jurisdiction,[40] this analysis displays fatal shortcomings. To say that a webpage is 'located' at the server means redefining downloading and uploading as a communication between two physical places, the location of the uploader and the 'location' of the webpage. This would territorialise cyberspace through its servers, creating exactly the kind of jurisdictional mayhem that the theory of international spaces seeks to avoid. As a practical matter, we know that data sent from an uploader to even a nearby server can travel in data packets through nodes around the world.

One could envision a system in which we accept the theory of the uploader and the downloader, but insist on exercising territorial jurisdiction over webpages 'located' at a server. Under the theory of the uploader and the downloader, the act of uploading is performed entirely at the computer terminal of the uploader, within one and only one state. Naturally, if that state is the same state as the server, then asserting jurisdiction over a webpage based on a territorial theory about the 'location' of the server rather than on the location of the uploading will produce no difference except in doctrine.

The effects of this doctrine will appear only when the uploader and the server are in different states. In that case, in order to say that the law of the server applies to the webpage, one must assert that the act of uploading had an effect in the forum state substantial enough to provide a basis for jurisdiction under the theory of objective territoriality or 'effects' jurisdiction. The theory of objective territoriality certainly can provide the basis for jurisdiction to prescribe in cyberspace under unusual circumstances, but it will not do as a general rule for ascribing criminal liability to foreign uploading, because all states have an equal interest here. Objective territoriality requires a special, unique interest.

The natural response is to point to the computer files which create a webpage and say that it would be false to claim that the webpage was anywhere else but on the server. This narrow approach ignores the interactivity of cyberspace in four important ways. The first problem can be best stated a question: can one say that a webpage really exists until it is accessed and constituted on the screen of the downloader? Surely the gif[41] file containing pornography cannot create offence until compiled and displayed on the downloader's machine. This is more than a metaphysical oddity. It is not hard to figure out who put garbage into

40 With today's technology, one can easily access an internet account from any other server in the world, by use of 'telnet' and 'rlogin' commands over the UNIX platform. In the future, this will presumably be easier. Indeed, it is not a farfetched idea to have a universal server utilising hard drive space around the world for storage, the way a single hard drive stores data on all over its dozens of sectors. We might as well start analysing it this way now.

41 The term 'gif file' refers to pictures saved in the Compuserve format, denoted by the file extension 'gif'. The 'g' is usually hard.

cyberspace, but it is very difficult to say what happens to it once it is there. If the webpage is located at Stanford, how does it 'travel' to Bolivia? Is the Bolivian coming to Stanford? Talk about asking the wrong questions!

Second, constituent parts of a webpage are often called from other servers, with the source code for the page consisting mostly of images called up from other places. We do not know what the future will bring, but we can only suppose that 'sites' consisting of data pulled from around the world at the downloader's request will become more common. Complexity will likely increase, not decrease.

Third, a webpage consists in large part of links to other pages which may be 'located' in other countries. Even if the data is not called up by the webpage itself, links to other data are presented to the downloader for him to (in today's mouse technology) click on. It becomes irrational to say that a webpage with links to gambling and pornography 'located' in 20 different countries is subject to the law of any and all of those countries. A government could criminalise the creation of links to certain sites, but this would create jurisdictional bedlam.[42] Of course as computer technology develops, the future will only create more interactivity and more absurdities. I would like to believe that this analysis of cyberspace would fail the Restatement test of reasonableness.[43]

Fourth, such interactivity is also supplemented by randomness and anonymity. This is often overlooked. In his article, 'Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community', William Byassee argues persuasively that territoriality should refer only to the 'physical components of the cyberspace community', who are the 'sender and recipient'.[44] The terms 'sender' and 'recipient', are terms implying intent of two (and only two) parties to communicate with each other. This is not the same as the 'uploader and downloader'. The downloader and the uploader do not know who the other is, or where the other is. For the downloader, the files are on his computer.

The substantive results of this analysis would lead to a considerable amount of seemingly random criminal liability, without really adding anything to a state's ability to control the content of cyberspace under the theory of international spaces. Persons travelling around cyberspace need to know what set of laws applies to their actions. If we reject the territorialisation of cyberspace, and accept the theory of the uploader and the downloader, we must reject the broad form of the 'law of the server'.

By contrast, under the theory of international spaces developed below, the rules are clear. The state where a server is located retains jurisdiction over the acts performed on that state's territory: the creation of the internet account for the foreign *persona non grata*, and the tolerance of that account (and the offensive

42 Picture a computer screen full of links, each one subject to the laws of at least one other jurisdiction, and the webpage itself subject to the law of its server on top of all that. Among other things, one shudders to consider the first amendment analysis of a law criminalising the HTML command, <a href = 'www.university.edu/~homepage'>. Or the random link.

43 1987 Restatement SS 403(1) 'Even when one of the bases for jurisdiction … is present, a state may not exercise jurisdiction to prescribe law with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable'.

44 William Byassee, 'Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community' (1995) 30 *Wake Forest L Rev* 197.