WHAT CAN A MEDIEVAL FRIAR TEACH US ABOUT THE INTERNET? DERIVING CRITERIA OF JUSTICE FOR CYBERLAW FROM THOMIST NATURAL LAW THEORY.

©Brandt Dainow, 2013
bd@thinkmetrics.com

TO BE PUBLISHED IN
Journal of Philosophy & Technology (110), 2013
DOI: 10.1007/s13347-013-0110-2

Abstract

This paper applies a very traditional position within Natural Law Theory to Cyberspace. I shall first justify a Natural Law approach to Cyberspace by exploring the difficulties raised by the Internet to traditional principles of jurisprudence and the difficulties this presents for a Positive Law Theory account of legislation of Cyberspace. This will focus on issues relating to geography. I shall then explicate the paradigm of Natural Law accounts, the Treatise on Law, by Thomas Aquinas. From this account will emerge the structure of law and the metaphysics of justice. I shall explore those aspects of Cyberspace which cause geography to be problematic for Positive Law Theory, and show how these are essential, unavoidable and beneficial. I will then apply Aquinas's structure of law and metaphysics of justice to these characteristics. From this will emerge an alternative approach to cyberlaw which has no problem with the nature of Cyberspace as it is, but treats it as a positive foundation for new legal developments.

Introduction

Today Cyberspace[1] confronts legal theory with previously unimagined challenges, yet in terms of human history it is so new as to barely qualify as having started. We can reasonably expect it to extend its reach to most human beings, and to develop its capabilities in many ways not yet imagined. During its first decade the Web was largely unlegislated. While some international agreements provided a platform for the regulation of the Internet, human activity using that infrastructure was largely bereft of legal framework.

[1] I shall use the term 'Internet' to refer to the technical infrastructure of the global ICT system; the wiring, the routers and gateways and other hardware which makes possible this global network activity and also the software which operates the physical infrastructure, from HTML and XML at the top, to TCP/IP and the protocols of the OSI Network Model at the bottom. I shall use the term 'the Web' to refer to the wider human experience which obtains from use of the Internet. This includes the individual, social, and political experience. The term 'cyberspace' is becoming fairly common in legal discussions (Xia 2011), so I shall use the term 'Cyberspace' to refer to the target of regulatory and legislative practice, which often includes elements of regulation of both human practice and technical feature in parallel. For example, data protection legislation, in mandating technical practices with regard to data storage (Internet), and human practices regarding usage and ownership of this data (Web), demonstrates how Cyberspace can encompass both the Internet and the Web, yet treat each separately. I shall use the term 'cyberlaw' to refer to laws in respect of Cyberspace.

As the Web has grown, and particularly as it has developed in its capacity to influence areas in the material world such as politics and business, legislation of the Web is starting to develop. Much potential cyberlaw has been vociferously opposed by web users. Not all of this resistance has come from radical anarchist hackers. Much has come from large corporations and from ordinary citizens. Some of that legislation has been withdrawn, while some of it has passed into law. It has been common for this opposition to be founded on the basis that the proposed legislation breaks the "spirit of the Web" or that it somehow damages the essence of what makes the Web the good that it is. Sometimes the word "justice" is coined as an evaluative criterion in these debates, though without much precision behind the term, for the principles which provide justificatory framework for cyberlaw remain largely undeveloped. Meanwhile governments are grappling with issues of a type never raised before; it is often difficult, or even impossible, to determine under whose jurisdiction an online act falls. Simultaneously we are witnessing the rise of non-governmental organisations with levels of regulatory power once reserved for nation states (and the occasional barbarian horde). This situation has raised many concerns and calls for a rethinking of legal philosophy as it applies to Cyberspace.

There are many standards by which we can evaluate a law. We can evaluate it on a utilitarian basis, in terms of its consequences. We can evaluate it positively, in terms of the procedures and other "social facts" (Marmour 2011) by which it was produced. Finally, we can evaluate a law morally, in terms of justice. The concept of just versus unjust law provides a mechanism by which we can individually determine to what degree we are morally obliged to obey a law. In strong cases it may provide a justificatory mechanism by which we can hold it is legitimate, or even obligatory, to disobey that law. This moral approach falls under the heading of Natural Law Theory. It is this approach which provides a foundation for many modern transnational legal systems and processes, commencing with the Nuremburg Trials and the UN Charter (Mirabella 2011), and which continues to heavily influence many aspects of law and jurisprudence.

The basis for legal development of Cyberspace can be difficult. Often laws are developed on the basis they will produce positive outcomes. However, as a phenomenon without precedence, we cannot look to previous examples of Cyberspace for understanding. We may be able to derive some valuable insights from analogies with other cultural or technological systems, but no society has had the historical experience of the emergence of a World Wide Web. As a result we cannot look to the past to see what has worked or use the lessons of history to anticipate the problems of the future. Furthermore, we have never seen a mature, fully developed ubiquitous ICT network. Much of the technology is yet to be invented and we cannot know what human practices a fully developed World Wide Web will give rise to. However, we do know the Web of today was created largely by people using technology in unexpected ways. It is therefore difficult to attribute much certainty to predictions of the utilitarian consequences of any given cyberlaw. This makes assessing internet legislation in terms of its consequences extremely problematic.

Problems for Positive Law

Even more pressing than this inability to see forward are issues of governance. Traditional Positive Law accounts of the basis for legal authority are presented with difficulties when it comes to regulating Cyberspace because the traditional principles underpinning legal authority do not hold. The Internet was not pre-designed, but is a self-organizing system (Ghanbari 2008, Stevens & Right 1994). As different components of the infrastructure have evolved, so different systems and mechanisms have organically evolved to regulate those

components (Pagallo 2013). As a consequence, no single body has been responsible for its development, but rather a network of organizations, of disparate organizational type, have emerged (Reidenberg 1996, Marsden 2008, Vedder 2003). Today, three alternative forms of regulating authority are preferred by differing sectors; national governments, international bodies and treaties, and self-organised bodies of involved groups offering self-regulation (Mayer-Schönberger 2003, Vedder 2003, Leeuw & Leeuw 2012). A powerful libertarian voice is held by the self-organising groups which have been most responsible for the development of Cyberspace (Reidenberg 1996), many of whom argue it has developed extremely well with barely any legislation and therefore the most appropriate legal framework is a minimal one (Wilske & Schiller 1997, Frieden 2001). While some of these groups are recognizable, such as industry bodies like the various national Internet Service Providers Associations and standards bodies like the IETF or advocacy groups, such as the Electronic Frontier Foundation, groupings like the Open Source movement are hard to define as organizations in the traditional sense, yet provide a more coordinated and focused effect than previous social movements (Choi et. al. 2009). This raises issues of legitimacy and accountability while also presenting an unfamiliar landscape for regulatory and legislative action (Vedder 2003).

The challenge facing Positive Law Theory is that it requires an account in terms of social facts and procedures which become unclear (or even meaningless) in Cyberspace; the problematic nature of the Internet's relation to geographical location undermines the traditional basis for determining jurisdiction. Traditional accounts distinguish three kinds of jurisdiction when determining the limits of a state's jurisdictional scope; legislative jurisdiction, judicial jurisdiction and jurisdiction to enforce. Jurisdiction to enforce is generally dependent upon having judicial jurisdiction, which is dependent upon having legislative jurisdiction (Wilske & Schiller 1997). Legislative jurisdiction itself derives from a limited set of principles; territoriality, effects, personality and the protective principle. These principles are challenged in Cyberspace by their dependence on actions and consequences having identifiable geographic locations (Xia 2011).

The principle of territorial jurisdiction allows states to regulate persons, things or acts which occur within their state boundaries. Territorial jurisdiction becomes problematic in many ways with regard to Cyberspace. The Internet carries nothing to represent physical borders, making it difficult to apply the principle of territoriality. Actions may be situated in multiple distributed locations or cause effects in more than one place and therefore have the potential to involve more than one jurisdiction (Kulesza 2008, Xia 2011, Davis 2001). Furthermore, it can be difficult for citizens traversing nodes on the Web to understand what jurisdiction that node resides in or which state's legal code they should consider applicable (Xia 2011, Wilske & Schiller 1997).

The principle of effective jurisdiction permits states to regulate acts occurring outside the state boundaries which are intended to have an effect inside that state. The difficulty here is that most of Cyberspace is available in most of the world and on that basis every state in the world may claim jurisdiction (Davis 2001, Kulesza 2008). Furthermore, the default, or "natural" position is one of "open to all" – as we shall see, once a system is connected to the global TCP/IP network, it requires additional steps to restrict access.

The principle of personal jurisdiction allows states to regulate to prevent harm to their citizens when the actions occur outside state borders. However, this becomes problematic when people from multiple countries interact on the Web, each backed by their own jurisdictional claim, each remaining physically located within their own state borders. Things are made more complex by the absence of international agreements to resolve these

difficulties (Kulesza 2008). Furthermore, development of such agreements may be difficult because of competing cultural perspectives. Attitudes to online privacy, for example, are strongly culturally determined in terms of what people hold as constituting personal privacy, the desired aims of privacy legislation and the preferred balance between individuals, social groups and institutions (Capurro 2005). Further complicating this situation is the rise of trans-national concerns which cannot be solved within state frameworks, but rather require international bodies, or even new forms of organization (Pagallo 2013).

The last of the four principles, the protective principle, is only intended to cover actions taken by non-citizens outside national borders which are specifically intended to harm the state. This applies to a limited set of actions, such as terrorism or falsification of official documents, and is generally considered less problematic in terms of Cyberlaw. However, since it only applies to a very small fraction of online activity, the application of this principle does not address the substantial body of concerns (Kulesza 2008, Wilske & Schiller 1997).

This situation makes the evaluation of law difficult in terms of existing accounts of Positive Law Theory. To whose social facts, procedures or authorities are we to appeal? Where territoriality functions in new ways, either non-existent or multiple, can we identify which procedures apply or determine how to reconcile overlapping jurisdictions? Natural Law Theory provides an account of law which is not troubled by these concerns because it looks to the content of the regulation, not its form or origins. It provides a universal standard by which to evaluate legislation irrespective of the types of action being regulated or the nature of the regulating body.

Aquinas and Natural Law Theory

There are many accounts within the Natural Law tradition, and much variation between them. For example, Murphy holds that the central claim of Natural Law is nothing more than "that there is a positive internal claim between law and decisive reasons for action" (Murphy 2006, p. 1). By contrast, Westberg (1995) makes the stronger claim that the essence of Natural Law theory is that moral claims form the basis for the assessment of law. This view is echoed by Finnis (1980), who argues that Natural Law is concerned with the proposition that legal obligation is a form of moral obligation. Such disagreements tend to support the attitude that Natural Law Theory is a general term applying to a wide variety of positions, and that it is the application of the term, rather than the contents of the ideas, which unites them (Crowe 1962).

Be that as it may, there is general agreement that the treatment of law by Thomas Aquinas, as found in Questions 90 – 97 of the *Summa Theologicae I-II*, represents the paradigm of Natural Law Theory (Armstrong 1966; Crowe 1962; Henle 1993; Lisska 1996; Murphy 2006). In this section, which has become known as *The Treatise on Law*, Aquinas provides an account of law which entails moral obligation as a function of the metaphysical structure of the universe. Accompanied by his epistemology and his account of the nature of the human being, Aquinas provides a comprehensive account of the nature of law and its basis in morality and psychology. He also provides normative guidelines regarding many aspects of law, including evaluations of justice, obligation to obey and legislative procedures. Interest in Aquinas and Natural Law Theory revived after World War II, providing the basis for the concept of crimes against humanity and much of modern international law (Lisska 1996; Mirabella 2011). Recent accounts of Natural Law, such as Finnis's influential *Natural Law and Natural Rights* (1980), can be characterised as modifications or extensions of Aquinas. It

follows that if we can make sense of justice in Cyberspace using Aquinas, the entire corpus of Natural Law thinking is better placed to confront issues of cyberlaw.

Our starting point will be structure of law provided in Questions 90 – 97 of the *Summa Theologicae I-II*,[2] but we shall also draw upon Aquinas's metaphysics of good as found in Book 3 (Questions 2 and 3) of the *Liber de Veritate*. We shall examine how Aquinas defines law, good and justice, and how he connects these with the human. I shall seek to explicate the underlying principles within his schema and use them to produce an account of specific criteria for determining the justice (or otherwise) of cyberlaw.

Aquinas's Account of Law

Aquinas derives a number of concepts and methodologies from Aristotle which distinguish his approach. Most importantly, Aquinas tends to regard things as processes rather than states. For Aquinas a true understanding of something, especially living things and social systems, can only occur through an understanding of the final state to which their developmental processes are inclining. For Aquinas all living things have ends, states of affairs which they have an inbuilt, essential, inclination to achieve. For example, all beings are inclined to preserve their life; they have internal processes which preserve their lives, and they have behavioural predispositions which function to the same end. This concept of disposition towards ends is central to Aquinas's treatment of Natural Law (Lisska 1996). Aquinas also distinguishes between two forms of reason in the human; speculative reason and practical reason. Speculative reason may be understood as that which most people think of as the intellect and works through syllogistic reasoning. Practical reason, on the other hand, is action-oriented. Where speculative reason is concerned with premises and conclusions, practical reason is concerned with actions and consequences. Both forms of reason are rational in the sense of having a methodological consistency. Where reasoning occurs in an inconsistent manner, Aquinas characterises it as irrational.

Aquinas's Four Laws

Aquinas defines four forms of law; eternal law, natural law, human law and divine law. Eternal law may be conceived as the cosmic order of things (Pattaro 2005). It is regulative to nature and normative to man's free will. On the basis of its regulative nature, it may be considered a type of law (*ST*, I-II, Q91, Art.1). Natural law can be understood as the manifestation of eternal law within creation as the underlying principles upon which the living world operates. All instincts, physical and biological processes are instantiations of principles of eternal law (*ST*, I-II, Q93, Art. 2).

While human beings are subject to the same biological and natural processes as any other animal, they also have the ability to reason. Natural law is here reflected in our natural "rational" characteristics (*ST*, I-II, Q91, Art. 2). There may be some debate about exactly

[2] The text of "the Summa," as it is known, is divided into three parts. The second part is further divided into two sub-parts, traditionally referenced as I-II and II-II. Each part is composed of a series of numbered questions. These questions are further divided into numbered articles. I shall follow the convention of citing references within *The Summa* by sub-part, part, question and article; for example (*ST*, I-II, Q91, Art. 4).

what constitutes "natural" in man, but this does not entail any logical difficulty for Aquinas. It is the existence of given human characteristics in the general sense which constitutes the premise of the argument, not any specific conceptualisations regarding how human nature is instantiated in real living people. So long as we accept that there is a basic human nature of some sort, we can use the concept of natural law.

Natural law offers only general principles. Human law is the development of those principles into specific regulations (*ST*, I-II, Q91, Art. 2). Natural law is non-contingent because the world has a certain given nature and humans have a given makeup. Aquinas regards it as rational to make laws which understand things as they are and irrational to do otherwise. Where human laws reflect the principles of natural law they may therefore be described as rational. If a law is not reflective of natural law then it is irrational and lacks validity. Aquinas holds such laws are only called 'law' because they are backed by state-sanctioned violence (ST, I-II, Q93, Art. 3). Divine Law is found in the Bible to provide guidance for situations which cannot be regulated and so does not concern us here.

The Nature of Good

Under Aquinas justice is what makes laws morally obligatory - we are morally obliged to obey just laws and not morally obliged to obey unjust ones. We can therefore develop a conception of justice by determining what would morally oblige us. Moral obligation pertains to action in that it is an injunction to act in certain ways. It therefore falls under the purview of practical reason. Practical reason is compelled by its nature to incline to good and will orient action to good in a properly functioning person.

Aquinas merges ends with good in a deep way which has often been misunderstood. His clearest treatment is found in Book 3 (Questions 2 and 3) of the *Liber de Veritate Catholicae Fidei Contra Errores Infidelium*, typically referred to as *Summa Contra Gentiles* or as *De Veritate*. Question 2 first shows that every act is for an end. The concern is primarily to see off the proposition that actions can be infinite. This is done analytically, showing that all actions are done for a purpose, which may be described as, and is, an end. Having established that every act is for an end, Question 3 sets out to show that every agent acts for a good. The critical task for Aquinas is to avoid a mere analytic proposition which simply defines 'good' as nothing more than the term for the end of a successful act.

Aquinas first establishes that desire (or appetite) represents an attractive orientation to good. Good's relationship to desire is that it provides the ends to desire and so good is the final cause of appetite. Aquinas then argues that good is not merely the object of desire, but is the fulfilment of potency. The aim of any act is to actualize a potency, so the aim of an act is to achieve a good. Aquinas uses this to define evil as that which limits the fulfilment of potential. Aquinas then offers a description of the way rational reason works. Intelligent agents act for a purpose, an end; they do not act chaotically. As intelligent agents, they determine what that end is for themselves, they are not puppets. This requires a combination of will (desire) and practical reason. The will desires the good - that is its essential nature. Practical reason can only select an end by considering what is desirable and practical reason will only find an end desirable if it is perceived as good. Since practical reason is what makes intelligent agents act, all intelligent acts are oriented towards achieving a good. Since what an act aims to achieve is its end, ends and goods are coterminous as a fact of practical reason.

It is not necessary to critique these arguments; our intent is merely to build upon Thomist Natural Law Theory to construct a set of criteria for justice. What we have seen is that, under the Thomist system, good and ends are closely intertwined; the difference is more a matter of

the perspective than a fundamental metaphysical or ontological separation of the two. This can be summed up as a "metaphysics of finality" (Lisska 1996, p.103)[3]. Under Aquinas good is embedded in the fabric of the universe. All temporal things are in process, moving from potency to actualisation and the fulfilment or frustration of that process is good or evil. Good is therefore something which can be determined objectively, in the sense that it can be tested for its effect on being and its actualisation of potencies. The actualisation of the natural potencies of the human thus becomes a set of goods. Practical reason is attracted to good and selects those ends which are good for the individual. If practical reason acts otherwise it is acting in a self-contradictory fashion – irrationally. To be moral is to therefore be attracted to good - which is to seek to operate rational practical reason in a manner so as to bring potency to act and to maintain or enhance being.

The Nature of Justice

Since moral obligation derives from an ontological good instead of a human practice, Aquinas does not allow that legal process is superior to conscience. For Aquinas laws can only morally oblige us if they are in accord with our conscience (*ST*, I-II, Q96, Art. 4). In a properly functioning human being, the conscience will be in accord with natural law. For a human law to accord with our conscience requires, therefore, that said law be in accord with natural law (or at least neutral to natural law). A law which is in accord with natural law will be "rational" in the sense of the rationality of practical reason. Our analysis of *De Veritate* indicates that a rational natural law will promote being, seek the good, not prevent the actualisation of potency and be in accord with human needs and dispositions. A law which meets these criteria may be termed 'rational.' A rational law is a just law and a just law is a rational law; the two terms are logically commutative.

According to Aquinas, all law can be categorised as either just or unjust.

> Laws have binding force insofar as they have justice. […] Things are just because they are right according to the rule of reason. […] The primary rule of reason is the natural law, […] And so every human law has as much of the nature of law as it is derived from the natural law, and a human law diverging in any way from the natural law will be a perversion of law and no longer a law (*ST*, I-II, Q95, Art. 2).

This provides us with the antecedents and consequences of justice. The source of the justice of a law is accordance with natural law (the way things are). The consequence of the justice of a law is moral obligation. Furthermore, there can be no unjust law. A law which is unjust is a broken law; it is 'bad law.' There may be extrinsic reasons for compliance, such

---

[3] It is this identification of ends with good which offers the primary point of attack against Thomist natural law – the accusation that this identification is a naturalistic (or "is/ought") fallacy. However, it is outside the scope of this paper to address this issue in any depth. Both Lisska (1996, pp. 33 - 48) and O'Connor (1967, p.72) offer excellent treatments of the issue in defence of Aquinas. What is clear is that the is/ought accusation treats values as an ontologically different type than Aquinas does. For him, values inhere within the material world. The primary facts of the material world, the nature of what is given, its processes and structures, *are* our primary values.

as "to avoid scandal or civil unrest," but unjust laws are "acts of violence rather than laws" (*ST*, I-II, Q96, Art. 4) because they compel through fear instead of conscience.

Justice in Cyberspace

We are now in a position to determine the attributes of justice with regard to cyberlaw. To determine the specific characteristics a cyberlaw must possess in order to be just requires determining the features of Cyberspace which form the equivalent of its eternal law and then tracing the manner in which they are expressed as natural laws in Cyberspace. These characteristics will be the essential properties of Cyberspace which are necessary to make it what it is and make it a good. In that Aquinas considers being in terms of process rather than state, the essential properties of Cyberspace we are looking for will be dynamic and reflect its operational systems, its capacity for, and mode of, growth and its ability to resist damage and preserve its existence. If we can determine what those properties are we will have determined the characteristics cyberlaw must possess in order to be just.

The Eternal Law of Cyberspace

Eternal law is the underlying order upon which the world is based. It represents a combination of structures and processes, objects and systems. It provides the enabling and limiting characteristics which force pattern onto natural law and determine what is potency and act, what constitutes being and what promotes or inhibits being and fulfilment. Determining the eternal law of Cyberspace is a reductionist process by which we seek to determine the technical processes underpinning human action. It is those characteristics which make the Web possible and which define its essential properties, without which it could not be. In Thomist terms, such features constitute the essential being of Cyberspace. In that the Web is technically supported and mediated by the Internet, eternal law will be located in the Internet's fundamental technical characteristics. These primary technical characteristics of the Internet will hold the status of the self-evident synthetic necessities by which the Internet can be and which are known to humans by their effects.

While there may be a number of such characteristics, we need only focus on one for the purposes of this discussion. We have seen that the relationship between online activity and physical geography is what causes the most difficulty for cyberlaw because there is no physical geography on the Internet. This is an essential property of the Internet, encoded into the core structures within the software which make the Internet and the Web possible. These structures do not have the capacity to represent geographical information. This is not an accident, they were designed not to represent geography because this makes transmission of data possible in ways which references to geography prevent. Not representing geography is a necessary characteristic for the Internet, the Web and Cyberspace. We shall therefore now examine why this is so and how this constitutes an example of eternal law in Cyberspace.

Aspatiality

Aspatiality is the term coined by Michalis Vafopoulos in *Being, Space and Time on the Web* (2012) to describe the well-known concept that items and actions on the Web cannot be identified as occupying specific geographical locations or any form of spatial orientation. A similar concept was used by Joohan Kim in *The Phenomenology of Digital Being* (2001, p.98):

> Digital-beings have no determinable spatiotemporality. This is the fundamental difference between physical things and digital-beings: while every physical thing is here or there, a digital-being is here and there. The

> specific spatial location of the Web cannot be determined. […] Temporality of a digital-being is not determinable, either. No physical instruments or any sort of chronometer can possibly determine temporality of a digital-being. In Heidegger's terms, digital-beings have no "datability."

The cause of aspatiality is the nature of the connective tissue of the Internet. An examination of the manner in which messages move around the Internet shows that the absence of geographical data is unavoidable because such an absence makes the Internet possible.

The Internet sits on a foundation of TCP/IP (Transmission Control Protocol/Internet Protocol), the two protocols which give devices the ability to exchange messages in a manner which makes the Internet possible. The Internet owes its very existence to the way message routing is handled by IP. The routing methodology of IP permits messages to move between nodes on the Internet in whatever happens to be the fastest route possible at any given moment in time. This flexible traffic flow permits devices to be added or removed from the Internet without any other portion needing to be reconfigured. In turn this permits the Internet to grow at a very rapid rate while also providing resilience when portions of the Internet infrastructure become damaged (traffic automatically flows around the damaged portion). This flexibility requires that routing be dynamic, automated and free of geographical consideration.

IP shields applications from the mechanisms which connect them to the Internet. The physical network is therefore irrelevant to internet-aware applications, allowing the physical infrastructure and its geographical arrangement to change without any impact on higher level activity (Rosen et. al. 1999). The connection between the originating device and the destination device is never direct; instead IP datagrams are passed from machine to machine until they arrive at their destination. Each datagram is composed of a header followed by the data being transmitted. The header contains all the information available to process the datagram, including its origin and destination (in the forms of IP addresses). It is not possible for the header to include information such as geographical location or information regarding which route a datagram should take or has taken (Stevens & Wright 1994). There is thus nothing within the structure of the messages being exchanged within the Internet which can represent geography.

Message transmission is controlled by routers whose function is to receive IP datagrams and send them onwards. Since these devices are what determine the traffic patterns within the Internet, it would, in theory, be possible to encode geographic information there. Many routing protocols are currently used in the Internet, which may be characterized as a collection of autonomous systems, each of which can select its own routing protocol for use within that system. This permits independent evolution of each portion of the infrastructure of the Internet and also of the software humans use to create the Web. This is a necessary, though not sufficient, condition for device-independence on the Internet. It is important to recognize that when a new device on the Internet sends a message to another, such as a request for a file, there is no need for any work to be done within the Internet to make provision for it. The system simply adapts automatically. As traffic increases some routes become congested; what was a moment ago the fastest route suddenly becomes slow and alternative routes become preferable. Hence IP standards specifically state that IP systems must support multiple routes (Stevens & Wright 1994) and it is a formal design principle of the IP protocol that "adaptability to change must be designed into all levels" (Braden 1989, p.6).

The paths which messages take over the Internet must be dynamic in order to provide efficient traffic flow and the ability to withstand changes to the network. Furthermore, since the function of IP routing is to move messages between computers, not geographical locations, there is no reference to geography within the various routing protocols or the data from which routing tables are composed, nor would such information serve any purpose. Distance on the Internet is defined in terms of intervening nodes ("hops"), not the number of kilometres or miles between them. The only information a router has about a remote network is the number of hops required to reach it and what node is next on the path to get there (Graziani & Johnson 2008). Taking geography into account could only slow the system; sometimes the fastest route between New York and Washington is via a router which just happens to be in Amsterdam. Geographical information is not of a type which could do anything other than inhibit the good order of the Internet by reducing the ability of traffic to adjust to changes in the network and maintain optimal message routes. Geographical considerations are not only impossible at the IP level, they would be harmful.

The measure of the robustness of this system as a consequence of its aspatial nature is evidenced by the maintenance of a consistent number of connections between nodes as the Internet has developed and changed. The "degree" of a node in a network is the number of connections it has to other nodes. The "degree probability" is the probability that a randomly selected node will have a given number of such connections. A probability distribution of all possible degrees can be plotted for the whole network, termed a "degree distribution." Despite the rapid growth of the Internet, uncoordinated by any central body, the degree distribution of the Internet has remained remarkably consistent (Izaguirre et. al. 2007) such that nodes on the Internet have maintained an average of six hops between them throughout its evolution (Ghanbari 2008). It is the dynamic and self-organizing nature of IP routing which has provided the ability of the Internet to self-organize. Without this ability to dynamically accommodate change and growth it is unlikely the Web would have developed.

There is a belief in some circles that the geographical location of an IP address can be determined *post hoc* (Poese et. al. 2011, Yong et. al. 2011). However, IP addresses are not allocated on a geographical basis and a single IP address may be used by multiple machines ("IP leasing") or, conversely, represent a gateway handling IP traffic for many devices. As a result a one-to-one correspondence between a specific device and an IP address can rarely be established with certainty. Efforts to circumvent this have focused on creating IP geolocation databases via traffic analysis, but these have been unsuccessful and, even when claiming to pinpoint a location, are unable to be more precise than a 50 – 100 mile radius (Poese et. al. 2011).

The other component of Cyberspace which directs the flow of data traffic occurs at the level of the human experience, so geography could, in theory, be represented at this level. The human-readable description of the nodes on the Internet and their resources is the URI (Uniform Resource Identifier)[4]. The URI is designed merely to represent an Internet resource in a uniform and minimalist manner. The syntactical conventions of the URI standard do not constrain the type of resource being identified, the method by which it is to

[4] The more commonly seen URL (Uniform Resource Location), or web address, is simply a type of URI which incorporates representation of its primary access mechanism, usually HTTP (W3C/IETF URI Planning Group 2001).

be accessed, or even what form of identification is being accomplished. The URI scheme is global in scope, such that "interpretation is independent of context," (Berners-Lee et al. 2005, p.9) including location. Furthermore, the relationship between a URI and the device or resource it references is intentionally unspecifiable so that devices or resources may change without changing the corresponding URI (Berners-Lee et al. 2005).

While many URL's contain references to nations, such as ".uk", the correlation of those references to the actual nation represented is a matter of social practice rather than physical location or technological encoding. A node accessed via a "co.uk" URL may be physically located in Australia without any technical issues being raised; a national domain designation is a name, not a location descriptor. Similarly, in order to balance traffic loads, a large international website may place multiple copies of the same site on hosts in many countries, all accessible via the same URL. These examples demonstrate that the country designation of a domain reflects, at most, the national allegiance of the website's governing authority rather than the physical location of the designated resource. Conversely, such national domains may be used for non-geographic purposes, as is the case with '.tv', supposedly the national domain designation for websites in Tuvalu, but in fact operated by private companies (in partnership with the government of Tuvalu) as profit-making enterprise selling '.tv' domain names for television-related websites.

In order to transmit data, human-selected URI's are converted into target IP addresses via DNS (Domain Name Service), so perhaps geography could be encoded there. However, the DNS resolution process is a mere mapping of domain names to IP addresses. There is no decision process involved in this mapping, it is merely a matter of one-to-one correspondences in lookup tables. As we have seen, IP contains no geographical reference. Since no algorithms or logical decisions are involved in the process of mapping a URI to an IP address, there is no space within DNS for reference to geography. In fact, DNS is designed to be independent of geography and of any reference to the underlying communications systems (Mockapetris, 1987).

What the above demonstrates is that geography is not represented within any of the systems which locate nodes and resources within the Internet. When people think they are making or using geographical references, as in URL's, it is really human practice and custom which attributes a connotation of geographical location, for no physical location is actually being described. The connection between the Internet and state territories is not problematic for contingent reasons, but because geography cannot be represented in the systems which provide connectivity between different points on the Internet. Furthermore, the needs of dynamic traffic flow dictate that geography cannot be built into these systems without serious, possibly fatal, harm to the Internet. From this it emerges that aspatiality is an essential property of the Internet, not merely an accident; the Internet was specifically designed to avoid geographical considerations. It is this precept which has permitted the Internet to maintain the same degree distribution during its growth and which makes it both robust and fast. Aspatiality emerges from our analysis as an eternal law of the Internet and therefore a guiding principle of justice in the natural law of Cyberspace.

An consequence of aspatiality as a precept of justice in Cyberspace is that IP traffic should flow freely, an ideal within the broader concept known as "net neutrality." As Tim Berners-Lee, inventor of HTML and much else of the Web, puts it:

> "When, seventeen years ago, I designed the Web, I did not have to ask anyone's permission. The new application rolled out over the existing Internet without modifying it. I tried then, and many people still work very hard still, to make the Web technology, in turn, a universal, neutral, platform. It must not

> discriminate against particular hardware, software, underlying network, language, culture, disability, or against particular types of data." (Berners-Lee Blog for MIT Decentralised Information Group, February 5th, 2006)

The precept of aspatiality links the free flow of IP traffic to justice. As we have seen, the ability of the Internet to dynamically modify IP traffic flow without human intervention and without reference to geography is essential to its being. The principle of net neutrality reflects this by holding that every datagram should be treated equally, independent of origin, destination and type of service (Berger-Kögler & Kruse, 2011). This is not the place to examine the debates regarding net neutrality in depth. However, we should note the efforts of many parties to undermine it. For example, some telecoms organisations wish to discriminate between different types of traffic. They may want to charge for IP traffic differently according to the data content or the destination or origin, or dump certain types of traffic when things are busy (Frieden 2008). The filtering of IP traffic based on datagram content has already been recommended by the International Telecommunications Union for the purpose of blocking spam email (ITU Recommendation X.1243, 2010). This recommends inspecting datagram content, cutting links with routers believed to be through-putting spam email, and blocking IP addresses. This is one of a range of ITU recommendations for handling spam, but the only one to suggest doing so at the IP level. The other recommendations have been implemented by many countries, but so far IP filtering has only been implemented in China (ITU-T Standards Q&A, 2013), which has also implemented IP filtering on a wide range of other grounds (OpenNet Initiative, 2012). More threats to IP freedom remain within the forum of the ITU. For example, the Russian Federation has proposed that each nation have the ability to create its own IP numbering system and URI conventions, and that global conformity be abandoned (Russian Federation, 2012). All such threats to the free and neutral flow of IP traffic emerge as unjust under our analysis.

There may well be other characteristics which are essential or necessary for Cyberspace to be what it is. The aim here is not to develop a complete analogue of eternal law for the Web, merely to identify a critical component which justifies the approach. Clearly other essential characteristics of the Internet remain to be explored in a wider examination of the eternal law of Cyberspace, but aspatiality creates a special concern for jurisprudence. It cannot be painted out of the picture - aspatiality is necessary for the Internet, and therefore the Web, to exist and to fulfil its greatest possible potential, its own *eudaimonia*.

The Natural Law of Cyberspace

We now enter the application of our precept of aspatiality at the level of the Internet to the human experience of the Web. The precept of aspatiality is reflected in the human experiences of disembodiment and de-localisation. Disembodiment occurs phenomenologically when one surfs the Web while maintaining a conceptual framework of the Web experience as that of physical movement. People see themselves as moving from place to place (web "site" to web "site"), while, in reality, one negotiates a spaceless geography composed of an ontological, rather than 3-dimensional, topography represented by entities such as the URL's of websites (Monnin & Halpin 2012). We may be "on" the Web, or "in" a website, but not in any physical sense and thus we experience ourselves as disembodied. This can lead to new conceptualisations of the nature of being. For example, Smart (2012) argues that this leads to deep changes in our cognitive and epistemic profiles, such that elements of our mental operations incorporate web resources so as to develop "mechanistic substrates" (Smart 2012, p. 446).

Aspatiality also leads to de-localisation of action. The distributed nature of the IP protocol means that much online activity cannot be located easily within three dimensional space. Imagine the following scenario: Someone in London is engaged in online text chat with someone in Singapore. They are doing this on a website which is physically located (ie: hosted) on a server in New York. The words typed in London and Singapore are first transmitted to New York, processed by the website, then transmitted back to appear simultaneously both in London and Singapore. Where does this conversation take place? With the rise of cloud computing, the website may no longer be hosted on a specific computer, but be within a "cloud" in which computing operations are distributed between different computers dynamically to share the workload. A cloud may be spread over much of the globe, so that the computer actually operating any given process may change from moment to moment (Voorsluys et. al. 2011).

These issues cannot be solved by determining which geographical regions are relevant; trying to cram these experiences into geographical constraints would be unjust to any individuals so treated. Doing so would ask individuals to attribute a specific remote geographical locus to their online activity and then understand themselves to be bound by the laws of that locality, no matter how distant it may be from their physical location or unknown to them that legal framework may be. However, while this appears unjust under this analysis, this is exactly what happens with many global websites. For example, Facebook's user agreement for all users outside Canada and the USA states all issues are governed under the laws of Ireland (Facebook, 2012), while Google's terms of service statement holds that everyone on the planet who uses Google's search system is bound by the laws of California (Google 2012). Under our analysis this common practice of pinning a global community of users down to a single region's laws emerges as unjust.

The customary method for developing positive laws for human practices on the Web has been to seek back to pre-existing concepts which seem to offer the best analogies with known experience, and then to apply the principles thereof as if the features of the Web were identical with, not analogous to, those traditional conceptualisations. For example, in July 2012, the legislature of the US state of Maryland passed a law forbidding employers from demanding access to employee's private social media pages. Bradley Shear, an attorney who worked on the drafting of the bill, described such social media pages as one's "digital home" (Rector, 2012) and so assigned the same rights and status as pertained to a physical property. This approach denies the very uniqueness of the Web, which is what generated the need for some additional work to regulate Cyberspace in the first place. By denying the unique aspects of the issues at hand, those which distinguish them from other issues, the rationality of the process is degraded and so, under Natural Law Theory, justice is reduced. Furthermore, in denying the reality of the situation, the chance of obtaining laws which appropriately respond to the needs for which they were generated is also reduced. As we have seen, under a Thomist conception, laws which lack rationality and hence justice do not, of themselves, warrant moral obligation beyond the need to keep the peace. Legislative justice in Cyberspace therefore requires recognition of, and support for, the aspatiality of Cyberspace. This does not mean that Cyberspace cannot be regulated, but the natural law position suggests that regulation via regional statute may not be the most just route. There is a growing body of opinion in support of international structures whose regulatory remits would be determined on grounds other than geography, basing jurisdiction on a particular form of technology (eg: viruses) or digital activity (eg: social networking) (Halavais 2000, Leeuw & Leeuw 2012) and such an approach would appear more just. The OECD is considering international arrangements for handling malware and we are now seeing the first thoughts in terms of similar structures based more on what happens in the Web, such as an

international privacy consortium (Kulesza 2008). However, as we have seen with issues of net neutrality, it is insufficient to merely have trans-national scope to a regulatory framework; the statutes produced must also be just.

Conclusions

Positive Law encounters difficulties with Cyberspace because geography is a weak, often non-existent, concept in Cyberspace. As we have seen, geography underpins the basis for jurisdiction by nation states, yet it is an essential property of the Internet that it *not* make reference to geography. Similarly, at the level of human's navigating via URI's, references to geography do not really exist; nor can they be imposed upon the Web. The result is that actions cannot be pinned to single geographical locations, but may span many, or may not be locatable in geographical terms at all. While the traditional foundations of state regulation are undercut by this lack of geography, the state's power to regulate has also been eroded by the *ad hoc* and dynamic nature of the Internet's development. This has led to the emergence of a wide range of organizational types with legitimate roles to play in regulation while at the same time devaluing the power of the state.

Ethical and legal positions tend to be based on metaphysics; once you conceive the world as being a certain way ethical and legal consequences usually follow. As a consequence, there exists a place for a metaphysics of Cyberspace which can serve as the foundation of one's positions regarding norms, law, rights, justice and so forth. Aquinas provides a simple basis for a metaphysics of Cyberspace because of his clear divisions of law and their integration into his metaphysics, a metaphysics which contains an inherent ethics. What I have done here is to accept his schema, the set of conceptual structures and their relationships, and use these to model Cyberspace. The idea that there are a set of knowable principles which underpin the manifest features of the world is not too surprising in the Western tradition. Aquinas's *modus operandi* is that the features (natural law) produced by these principles (eternal law) have positive value and that it is rational to behave in a manner which accords with them. Aquinas directed his commentary towards the material world. To the degree that the analogy of a "world" is applicable to the Web, it is possible to apply Aquinas's schema to this new digital "world." The task becomes one of identifying the eternal law of Cyberspace, those features which form its foundations and which differentiate it. One then determines a set of goods within these features and arrives at criteria of justice. The applicability of this process does not require acceptance of the content of Aquinas's concepts, such as belief in a Divine Mind, the existence of Platonic ideals, or a deistic creation. One need merely accept his fourfold division as a viable model for locating laws within a rational framework which attempts to reflect reality as it is.

The approach I have taken treats the Web and the Internet very much as processes, rather than states. My position is founded on a view of Cyberspace as evolving, as existing more in potential than in reality. Since its inception the Web has surprised us. Many of the most important innovations have resulted from people using Internet technologies in ways not anticipated by their inventors. At the time of writing there is no evidence of this trend slowing. There is every chance the Web will continue to evolve as long as programmatic devices and communications technology continue to evolve and as long as people can find new ways of using them. Under such a view, a long-term understanding of Cyberspace becomes both critical and highly problematic. In terms of what we should do with, and about, Cyberspace, we must therefore bear in mind that our ignorance is greater than our understanding. A process view of Cyberspace indicates that legislation designed to address a current circumstance may have significant impact on some unknown future circumstance, and

that this future impact may easily be more important than that of the present. Such a situation also pertains in other areas of technology. This issue was considered by Hans Jonas in *The Imperative of Responsibility* (1981). His solution was to adopt what he called "the heuristics of fear" (p. 22), in which we switch our focus away from trying to make things better and focus on avoiding making things worse.

I have adopted this approach to cyberlaw by arguing for evaluation of legislation within the Natural Law framework, in terms of justice. Aquinas stands at the centre of Natural Law theory and is therefore an excellent source from which to work. Furthermore, Aquinas's metaphysics is tuned to process, as in potency and actualisation, and so suits the nature of a Web in evolution. Aquinas develops the nature of legal justice from his metaphysics of the world. In order to use Aquinas we needed therefore to adapt his metaphysical schema to the "world" of Cyberspace. This enabled us to arrive at a position couched in terms which match the way people already experience the Web. Instead of seeking to answer the impossible question of how to apply geographical principles to Cyberspace, I have developed a position which accepts the Internet as it is. This required an explication of Aquinas's metaphysics, particularly those aspects which determine the nature of legal justice. Once we had identified these, we could seek for their equivalence in Cyberspace.

My methodology thus leads to a position where it becomes possible to argue coherently based on Cyberspace as it is, rather than become confused in a Procrustean attempt to trim it to fit old thinking patterns. As we have seen, this methodology leads to a position whereby it becomes more than unfortunate if one harms essential qualities of Cyberspace, it becomes positively unjust. Justice becomes a criterion of assessment irrespective of the nature of the regulatory body or the form that regulation takes and so puts all regulative endeavours on a comparable footing. In doing so it provides a mechanism for comparing alternative strategies for action which may take very different forms and also ties treatment of aspatial issues to an accepted justificatory platform already underpinning international law. This argues for Natural Law Theory as the only viable approach to present and future issues of cyberlaw.

Bibliography

Aquinas, Thomas. *Summa Contra Gentiles*, Book 3, translated by Vernon J. Bourke (1975) Notre Dame: University of Notre Dame Press.

Aquinas, Thomas. *The Summa Theologica of St. Thomas Aquinas, 2nd edition*, translated by Fathers of the English Dominican Province (1920), http://www.newadvent.org/summa/index.html. Accessed June 12, 2012.

Armstrong, R. A. (1966) *Primary and Secondary Precepts in Thomistic Natural Law Teaching*. The Hague: Martinus Nijhoff.

Berger-Kögler, U. & Kruse, J. (2011). Net Neutrality Regulation of the Internet? *International Journal Of Management And Network Economics* Vol. 2, 3 – 23. http://www.inderscience.com/link.php?id=42577. Accessed February 19 2013.

Berners-Lee T., Fielding R., Masinter L. (2005). *RFC 3986: Uniform Resource Identifier (URI): Generic Syntax*. Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3986.txt. Accessed February 12 2013.

Berners-Lee, T., (2006) *Public Policy and The Web Blog*, MIT Decentralised Information Group. http://dig.csail.mit.edu/breadcrumbs/taxonomy/term/23. Accessed March 4 2013.

Braden, R. (ed.) (1989). *RFC 1123: Requirements for Internet Hosts -- Application and Support.* Internet Engineering Task Force. http://www.ietf.org/rfc/rfc1123. Accessed February 12 2013

Capurro, R. (2005). Privacy. An Intercultural Perspective. *Ethics and Information Technology* Vol. 7, 37–47. http://www.springerlink.com/index/10.1007/s10676-005-4407-4. Accessed February 17 2013.

Choi, C. J., Kim, S.W., Yu, S. (2009). Global Ethics of Collective Internet Governance: Intrinsic Motivation and Open Source Software. *Journal of Business Ethics* Vol. 90, 523–531. doi: 10.1007/s10551-009-0057-5. Accessed February 17 2013.

Crowe, M. B., (1962). The Irreplaceable Natural Law. *Studies: An Irish Quarterly Review*, Vol. 51, 268 – 285. http://www.jstor.org/stable/30087745. Accessed May 9 2012.

Davis, P. (2001). Cyberspace: Countering the View that the Restatement (Second) of Conflict of Laws is Inadequate to Navigate the Borderless Reaches of the Intangible Frontier. *The Federal Communications Law Journal*. 339 - 363. http://law.indiana.edu/fclj/pubs/v54/no2/Davis.pdf. Accessed February 17 2013.

Facebook (2012). *Statement of Rights and Responsibilities*. Facebook Ireland Ltd. http://www.facebook.com/legal/terms. Accessed March 5 2013.

Finnis, John (1980). *Natural Law and Natural Rights.* Oxford: Oxford University Press.

Frieden, R. (2001). Revenge of the Bellheads: How the Netheads Lost Control of the Internet. *SSRN Electronic Journal* Vol. 26, 125 – 144. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=290121. Accessed March 1 2013.

Frieden, R. (2008). A Primer on Network Neutrality. *Intereconomics* Vol. 43, 4 – 15. http://www.springerlink.com/index/10.1007/s10272-008-0237-z. Accessed February 17 2013.

Ghanbari, Saeed (2008). *A Study on the Internet Topology*. Ebook. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.2072&rep=rep1&type=pdf. Accessed February 12 2013.

Google (2012). *Terms of Service*. Google Inc., http://www.google.com/intl/en/policies/terms/. Accessed March 2 2013.

Graziani, R., Johnson, A. (2008). *Routing Protocols and Concepts: CCNA Exploration Companion Guide*. Indianapolis: Cisco Systems, Inc.

Halavais, A. (2000) National Borders on the World Wide Web. *New Media & Society* Vol. 2, 7–28. http://nms.sagepub.com/cgi/doi/10.1177/14614440022225689 Accessed March 1 2013.

Henle, R.J. (1993). Background for St. Thomas's Treatise on Law. In Aquinas, Thomas, *The Treatise on Law: Summa Theologica I-II, qq.90-97,* translated by R.J. Henle. (pp. 3 – 114) Notre Dame: University of Notre Dame Press.

ITU-T (2013). *Standards Q&A*. International Telecommunications Union. http://groups.itu.int/itu-t/StandardsQA/tabid/1750/afv/post/aff/332/aft/696/afr/998/Default.aspx. Accessed March 1 2013.

ITU (2010). *X.1243:Interactive gateway system for countering spam*. International Telecommunications Union. http://www.itu.int/rec/T-REC-X.1243-201012-I/en. Accessed March 3 2013.

Izaguirre R., Eustorgio M., Santillán C., et al. (2007) Impact of Dynamic Growing on the Internet Degree Distribution. *Proceedings of the 2007 international conference on Frontiers of High Performance Computing and Networking*. Berlin: Springer-Verlag, 326–334. http://dl.acm.org/citation.cfm?id=2392366. Accessed February 24 2013.

Jonas, Hans (1981). *The Imperative of Responsibility*. Chicago: University of Chicago Press.

Kim, Joohan (2001). Phenomenology of Digital-Being. *Human Studies*, Vol. 24, 87 – 111. http://www.jstor.org/stable/20011305. Accessed October 4 2011.

Kulesza, J. (2003). Internet Governance and the Jurisdiction of States: Justification of the Need for an International Regulation of Cyberspace. *GigaNet Symposium Working Paper*. 1 – 22. http://ssrn.com/abstract=1445452. Accessed February 19 2013.

Leeuw F., Leeuw, B. (2012) Cyber Society and Digital Policies: Challenges to Evaluation? *Evaluation* Vol. 18, 111–127. doi: 10.1177/1356389011431777 Accessed February 28 2013.

Lisska, Anthony J. (1996). *Aquinas's Theory of Natural Law: An Analytic Reconstruction*. Oxford: Clarendon Press.

Marsden, Christopher T. (2008). Beyond Europe: The Internet, Regulation, and Multistakeholder Governance - Representing the Consumer Interest. *Journal of Consumer Policy*, Vol. 31, 115 - 132. http://link.springer.com/article/10.1007%2Fs10603-007-9056-z. Accessed February 18 2013.

Mayer-Schönberger, Viktor (2003). The Shape of Governance: Analysing the World of Internet Regulation. *Virginia Journal of International Law*, Vol. 43, 605 – 696. http://www.vmsweb.net/attachments/Govshape.pdf. Accessed August 9 2012.

Mirabella, Daniel (2011). The Death and Resurrection of Natural Law. *West Australian Jurist*, Vol. 2, 251 – 259. http://www.law.murdoch.edu.au/walta/articles/vol_2_2011/D%20Mirabella%20-%20The%20Death%20and%20Resurrection%20of%20Natural%20Law%20-%20WAJ%20-%20Vol2%20-%202011.pdf. Accessed October 28 2012.

Mockapetris, P. (1987) *RFC 1034: Domain Names - concepts and facilities*. Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3986.txt. Accessed February 12 2013.

Monnin, A., Halpin, H. (2012). Toward a Philosophy of the Web: Foundations and Open Problems. *Metaphilosophy*, Vol. 43, 361 – 379. http://dx.doi.org/10.1111/j.1467-9973.2012.01755.x. Accessed 17 June 2012.

Murphy, Mark (2006). *Natural Law in Jurisprudence and Politics.*, Cambridge: Cambridge University Press.

O'Connor, D. J. (1967). *Aquinas and Natural Law*. London: Macmillan.

OpenNet Initiative (2012). *Report on China*. https://opennet.net/research/profiles/china-including-hong-kong. Accessed March 4 2013.

Pagallo, Ugo (2013). Good Onlife Governance: On Law, Spontaneous Orders, and Design. *ONLIFE Initiative: Concept Reengineering for rethinking societal concerns in the digital transition*. 153 – 167. European Commission. https://ec.europa.eu/digital-agenda/onlife-initiative-0

Pattaro, Enrico (2005). An Overview on Practical Reason in Aquinas. *Scandinavian Studies in Law*, Vol. 48, 252 – 267. www.scandinavianlaw.se/pdf/48-16.pdf. Accessed August 20 2012.

Poese, I., Uhlig, S., Kaafar, M., et al. (2011). IP geolocation databases: unreliable? *ACM SIGCOMM Computer Communication Review* Vol. 41, 53–56. doi: 10.1145/1971162.1971171

Rector, K. (2012). Maryland becomes first state to ban employers from asking for social media passwords. *The Baltimore Sun*, http://articles.baltimoresun.com/2012-04-10/news/bs-md-privacy-law-20120410_1_facebook-password-social-media-bradley-shear. Accessed April 12 2012

Reidenberg, Joel R. (1996), Governing Networks and Cyberspace Rule-Making. *Emory Law Journal*, Vol. 45, 911 - 930. http://ssrn.com/abstract=11459. Accessed February 22 2013.

Rosen, K., Host, D., Farber, J., Rosinski, R. (1999) *Unix: The Complete Reference Guide*. New York: McGraw-Hill.

Russian Federation (2012). Proposals for the work of the conference. *World Conference on International Telecommunications Plenary Meeting*. http://files.wcitleaks.org/public/S12-WCIT12-C-0027!R1!MSW-E.pdf. Accessed March 6 2013.

Smart, Paul R. (2012). The Web-extended Mind. *Metaphilosophy*, Vol. 43, 446 – 463. http://dx.doi.org/10.1111/j.1467-9973.2012.01755.x. Accessed June 17 2012.

Stevens, W., Wright, G. (1994). *TCP/IP Illustrated: Vol. 1: The Protocols*. Reading: Addison-Wesley Publishing Company.

Vafopoulos, Michalis (2012). Being, Space, and Time on the Web. *Metaphilosophy*, Vol. 43, 405 – 425. http://dx.doi.org/10.1111/j.1467-9973.2012.01762.x. Accessed June 17 2012.

Vedder, Anton (2003). Internet NGOs: Legitimacy and Accountability. In Traunmüller, R. (ed.) *Electronic Government* (pp. 49 – 54). Berlin: Springer Berlin Heidelberg. http://link.springer.com/chapter/10.1007%2F10929179_8. Accessed 15 February 2013

Voorsluys, William; Broberg, James & Buyya, Rajkumar (2011). Introduction to Cloud Computing. In Buyya, R., Broberg, A., & Goscinski, A., *Cloud Computing: Principles and Paradigms* (pp. 2 – 44). New York: Wiley Press.

Westberg, Daniel (1995). The Relation between Positive and Natural Law in Aquinas. *Journal of Law and Religion*, Vol. 11, 1 – 22. http://www.jstor.org/stable/1051622. Accessed June 19 2012.

Wilske, S., Schiller, T. (1997). International Jurisdiction in Cyberspace: Which States may Regulate the Internet? *Federal Communications Law Journal* Vol. 50, 119 – 178. http://www.repository.law.indiana.edu/fclj/vol50/iss1/5. Accessed February 18 2013.

W3C/IETF URI Planning Interest Group (2001). *URIs, URLs, and URNs: Clarifications and Recommendations 1.0*. W3C. http://www.w3.org/TR/uri-clarification/. Accessed February 26 2013.

Xia, Feng (2011). Impacts of the Internet on Traditional Jurisdictional Principles in International Civil and Commercial Cases. *Law China*, Vol. 6, 387–402. http://link.springer.com/article/10.1007%2Fs11463-011-0135-3. Accessed February 10 2013.

Yong, W., Burgener, D., Flores, M., et. al. (2011). Towards Street-Level Client-Independent IP Geolocation. *8th Usenix Symposium on Networked Systems Design & Implementation*. www.usenix.org/event/nsdi11/tech/full_papers/Wang_Yong.pdf. Accessed April 10 2013.