Can you ever regulate the virtual world against economic crime?

Dr Clare Chambers

Clare.chambers@uwe.ac.uk UWE, Business and Law, Frenchay Campus, Coldhabour Lane, Bristol, BS16 1QY, United Kingdom.

Abstract

The question of whether you can ever regulate the virtual world against economic crime is one which cannot be answered easily in practice or in theory. This paper examines this question as part of a much larger study into virtual economic crime. Economic crime and money laundering are occurring in many virtual worlds and to prevent them would have a positive impact on the negation of terrorist financing. However in order to prevent economic crime, the legal jurisdiction of virtual worlds must first be established. The paper examines the academic debate thriving between Internet separatist and inclusionist, outlining the philosophical approach of the paper in turn in order to discuss whether you can ever regulate against economic crime in virtual worlds.

Introduction

The British Fraud Advisory Panel (FAP) has said ñthere is nothing virtual about online crime, it is all too real. It is time the government took this seriousò (1). The FAP has further opined that ñmoney laundering is the obvious risk. There will be a migration of fraudsters into these sites when they see all of the opportunitiesò. They describe the virtual world as ña parallel universe with almost no external rule of law, no enforced banking regulations or compliance, no policing and no government oversightò. (1)

Similarly, Field Fisher Waterhouse Solicitors iterated that, ñthe law doesnôt stop just because this is a virtual world, but with its borderless nature, it may be challenging to determine whose laws apply. And thereôs a culture of anonymity, so it is often difficult to known that you are dealing withò. (1) *So the question is can you ever regulate virtual worlds against economic crime?*

To begin, this paper it is important to draw the distinction between the Internet or cyberspace and virtual worlds. Virtual worlds can be seen as another layer of coding inside cyberspace. The terms virtual world and cyberspace shall be defined and applied to the paper in the first section of this paper.

To be able to ascertain whether laws can pervade the Internet and enter the virtual worlds, it must be established whether you can ever regulate cyberspace. There is a fruitful and rigorous academic debate as to whether there should be separate regulation for cyberspace and thus virtual worlds, a separatist point of view that virtual worlds laws should be distinct from real world laws or the inclusionist view that real world laws should be applicable in cyberspace and virtual world too, given the real world affect and consequences these virtual worlds have. Caution the aim of the paper is to examine whether economic crime can ever be regulated against within virtual worlds. The paper will be divided into three parts. The paper begins by discussing the impact of economic crime on the virtual world and how it is a present and current threat to not only the virtual world but the real world too.

Secondly the paper provides an examination of the inclusionist and separatist viewpoints will be undertaken. Thirdly the paper will discuss the constraints of control in both the real and the virtual. Finally the paper will examine jurisdictional issues such as democracy and rule of law of the virtual worlds. A caveat must be added to this paper in so much as it is part of a much larger study into economic crime in virtual worlds and the questions which are considered all too briefly here but more so in the study are:

- Who can govern the Internet?
- How is the Internet different from the virtual world?
- Who holds the democracy to decide what is right and wrong within the virtual worlds?
- Can you implement laws within the Internet and thus virtual worlds?
- Can virtual world laws be part of the real world legal system, and if so from what legal system, or are they separate from the real world?
- How can you impose laws onto a virtual world which crosses boarders and jurisdictions?
- Where can people who have committed a wrong in a virtual world be held accountable?

Internet and Virtual worlds

Before an examination can take place of whether economic crime can ever be regulated against in the virtual world, the definitions of virtual worlds and the Internet/cyberspace needs to be discussed. This is because as iterated above, the virtual worlds are considered within this paper as being immersed within the Internet/cyberspace rather than being one and the same thing.

The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suit (TCP/IP) to serve billions of users worldwide. It is a network of networks that are linked by a broad array of electronic, wireless and optical networking technologies. Cyberspace is the electronic medium of computer networks, in which online communication takes place. It is a term used by cyberpunk science fiction writer William Gibson. In this paper the author uses the terms as to mean the same and one thing, that being the global system of interconnected computer networks.

Conversely a virtual world, according to Castronova, (2) is a computer programme with three defining features: Interactivity; physicality and Persistence. Before examining these three elements let us turn to defining the word virtual and world, separately and in turn.

Virtual, as an adjective, is defined as: virtual(a): being actually such in almost every respect; "a practical failure"; "the once elegant temple lay in virtual ruinò; virtual(a): existing in essence or effect though not in actual fact; "a virtual dependence on charity"; "a virtual revolution"; "virtual reality".

Or as: Virtual (a) having the essence or effect but not the appearance or form of. The word comes from the Medieval Latin term *virtualis* or *virtus* meaning virtue. Virtue is defined as: Virtue (a) the quality or practice of moral excellence or righteousness; Virtue (b) the particular moral excellence; Virtue (c) any of the cardinal virtues; justice, temperate, and fortitude Virtue (e) an affective active, or inherent power or force. Virtue comes from Old French *Vertu* and Latin *Vertus* meaning manliness and courage, (Vir man).

These definitions give us a clue as to why the name was chosen for the virtual world. The first definition, virtual is the beingô actually such in almost every respectõ, goes along with the line of thinking of the book. The world created online is as close to reality as possible. It simulates the

real world and demonstrates it desire to be as close as possible to the real thing but incorporating every day aspects into the virtual world, which is given no escape. It is more of a utopia than a virtual reality. The second definition; that virtual is ‘existing in essence or effect though not in actual fact’ also agrees with the assertion that the virtual world exists as a world but in reality, or in actual fact, it is not a real world. The third definition still does not pose a problem for this theory to word. Virtual is, ‘having the essence or effect but not the appearance or form of’. In a virtual world there is no form other than pixels on the computer screen but it has the essence and the effect of a real world.

From the definitions above we can determine that a virtual world is one that exhibits all the characteristics of a real world and the only difference being is that the virtual one has no physical form to it. If this is the case, then is hard to see why there are no legal ramifications for actions in world. Returning to Catronova’s (2) idea of what a virtual world is somewhat differs from the literal definition of what a virtual world is. In so far as that the author believes that these elements can be taken and can demonstrate that the virtual world created is not actually virtual, but a continuum of the real world, placed in a virtual platform. If this is so, and which is what the chapter argues, then the virtual should be subject to real world laws. Economics is a perfect example of how virtual economics is actually highly influenced and driven by the economic factors in the real world. This is because there is a single common denominator of the two worlds. That being human beings. The question is whether anything that is created played and thought about by Humans can ever be truly virtual? As mentioned above Castronova (2) examines three elements of what constitutes a virtual world. The first can be expanded to include the idea that the game can be accessed remotely by a large number of people, with ‘the command inputs of one person affecting the command inputs of other people’. (2) In other words to create and develop a society within the computer game. This interactivity can be further expanded to demonstrate the idea that the ‘command inputs’ are given by real world people, and have affects in world and in the real world on other input commands. Therefore put simple, the real world is affected by the actions in world, outlining the idea that the virtual is not so virtual.

The second element of Castronova’s virtual world is physicality, that being ‘people can access the programme through an interface that simulates a first-person physical environment on their computer screen; the environment is generally ruled by natural laws of Earth’. By having this synergy with the real world, these virtual worlds are taking on the appearance of being a continuum of the real world and not being as virtual as their name suggests.

The final and third element is that of persistence. This being the idea that the computer remembers the closing play of that person or people, whether anyone is using it or not. (2) Nothing alters unless the users of that virtual world make it happen. Thereby, demonstrating that the world needs people to make it world, it needs the real world influences to ensure that the in world occurrences happen. In other words, the virtual world cannot operate without real world influences.

Having examined the definitions of what a virtual world is it can be logically deduced that a virtual world is all but real part from its lack of physical form. Therefore if it has real world affects and is all but real baring its physical form could it not be right to say there needs to be a ‘Rule of Law’ operating within the world.

The virtual world can be seen as another layer of coding within the Internet/cyberspace. By having this extra layer of coding the ability to locate an act of economic crime through the ISPôs and the many networks is complex and outside the remit of the normal law regulating the economic contracts for e-commerce due to the possibility of crossing jurisdictional boundaries within this extra layer of coding. Law which is present within the Internet does not deal with economic crime and merely uses an assimilation of real world laws. This it is proposed is ineffectual at detecting, locating and combating economic crime in virtual worlds. Why then is economic crime, in what ever form it takes, hard to regulate against in the virtual world.

Economic Crime

Virtual money laundering is far from clear. Whether it exists or not is debated amongst academics, regulation surrounding the crime is unclear; the manner in which the activities are carried out changes so quickly that it is largely unclear. What is most clear is the lack of knowledge in the field of real world money laundering is virtual money laundering. It is therefore this paperôs aim to discuss virtual money laundering.

Cyber crime ñis one of the fastest growing areas of crime, as more and more criminals exploit the speech, convenience and anonymity that modern technologies offer in order to commit a diverse range of crimesò.(3)

One element of cyber crime is that of financial crime. The international agency, Interpol which acts to combat virtual financial crime states that, ñthe global nature of the Internet allows criminals to commit almost any illegal activity anywhere in the world, which makes it essential for all countries to adopt their domestic offline controls to cover crimes committed in cyberspaceò.(2). This has two important implications: Firstly, Interpol has acknowledged that there is a real threat of financial crime being committed over the Internet and secondly, that because the virtual is a continuum of the real domestic laws should be applied to the virtual worlds. However, this causes problems of its own. With the Internet crossing a multitude of boundaries and therefore laws, it is unclear as to which domestic law should apply in each instance of crime committed. There are no international standards, which have to be met.

In the real world there are three stages to laundering money from illegal gains. These three stages are placing, layering and integration. The first stage, placing, is to put the money (which is normally cash) into a place such as a bank. In the case of virtual money laundering this could be a PayPal account as well. The second stage, layering, is to ensure that the money does not arouse suspicions. The criminal needs to carry out as many complicated and intricate transactions with the money so that any traces are hard to follow. The final stage, integration is where the criminal combines the so called dirty money with legitimate money, making the whole appearance of the money to be clean.

From this very brief description one can already see how the virtual world, the virtual economy and the virtual money transfers lends itself to the criminal world of laundering money. The dirty money can enter the virtual world through a pre-paid card, such as PayPal, where little identification is required. The money can be used to buy in world goods, through numerous accounts and then the criminal can sell these goods in world. The money from the investments in world can then be withdrawn from the

world via an ATM or money account and the money appears to be from a legitimate source. It is therefore laundered. (4)

The Financial Action Task Force highlighted concerns about the new method of electronic monetary transfers in 2006 with a view to this being a new method of financial crime for criminals. (5) However during the last four years little has been put in place to provide a deterrent, nor any regulations to ensure successful prosecutions. It is important to understand the ideology behind electronic or digital money and this paper shall now move on to discuss this. To be able to launder money through the Internet there needs to be a method in which to do this. Money is therefore converted into digital money, used within a virtual game, which has now converted the real money into a virtual in world currency and the means by which a criminal can launder criminal money is complete. ñAll virtual games use some sort of electronic monetary system. Electronic money is used as an electronic replacement for cashò. (6) There are various methods of using electronic money to facilitate money laundering; these are through an electronic purse, mobile payments, and Internet payment services and through digital precious metals.

Another problem of digital currencies is anonymity. ñAnonymity is a heavily marketed characteristic of the digital currency industryò. (7) This allows the cybercriminal an extra layer of protection when laundering money though digital methods. Some issuers of digital currency do require some form of identification but because this is done via the Internet the documents can be scanned or e-mailed or faxed, allowing for easy doctoring of the documents. The means of putting real money into digital money is plentiful and each allows the criminal a chance of an easy method of laundering money. For example, one can pay in cash to the issuers exchange bank account, thus the money is not traceable. Secondly exchanges also accept wire transfers or postal money orders also allowing another layer of difficulty in determining the source of the original money. Thirdly, money can be transferred via electronic money orders, cheques, and online banking transfers etcé all of which again are hard to determine the true source of the money. Fourthly money can be transferred into the exchanges via pre-paid cards (8) and money can be taken out via ATMôs (Automated Telling Machines).

The overwhelming argument for virtual money laundering and virtual financial crime is the international governments and the international law enforcementsô response to the threat. The Interpol, US State police and the London Metropolitan police force, all are targeting virtual financial crime as a major problem in the fight against terrorism. More than this though are the new reports, which detail the ongoing problem of fraud and financial crime occurring within the virtual worlds.

The economies of virtual worlds are similar to those in the real world, barring the legitimate control over the supply and demand of goods. By acknowledging this as a fact of virtual worlds, we can then lead onto the assumption that if an abstract phenomenon of replicating economies in virtual worlds, occurs, then it can logically be extrapolate that criminals will find a way of using the virtual worlds as a means of committing crimes. If we also appreciate that the virtual world is a continuum of the real then it should come of no surprise that criminals are using the Internet and virtual worlds as a means of laundering money. Where there is a loophole criminals will find a way to exploit it. This is what is occurring in the virtual worlds currently. Because there is a lack of clear legal structure and parameters, the criminals are using this black hole in the law as an opportunity to launder money for their

criminalôs activities. Just because there is little widely known about virtual money laundering does not mean that we cannot target it as a crime. One of the major problems is that little work is being conducted into this problem. Since the economic decline in 2007 to the present day the government (past and present) has been preoccupied with keeping the UKôs and the USAôs economies solvent. Although some work is being done, the latest Fraud Advisory research was conducted in 2007 and although it does start to promote awareness of this latest crime, much more needs to be done currently.

Separatist's vs Inclusionist

The debate between two schools of thought on whether the Internet can or should be regulated is important to the discussion on financial crime because as we have seen above, financial crime can and does occur within virtual worlds. The debate as to whether economic crime can be regulated is grounded in the theoretical debate as to whether the Internet is capable of being regulated by real world laws or whether the Internet should be self-governing. In this section these two opposing views are analysed. To begin this discussion the work of John Perry Barlow in 1996 will be discussed. Barlow wrote the Declaration of the Independence of Cyberspace on behalf of cyberspace. (9) Barlow is a founding member of the Electronic Frontier Foundation and is renowned for his contribution to the debate on the applicability of government on the Internet and represent the separatist perspective. His work was the catalyst for many pro Internet self-governance research groups to be founded. Within the declaration Barlow provides an explosive piece of work demonstrating the attitudes towards the US Communications Decency Act which was the first piece of legislation in the US which prohibited pornography on the Internet. This Act engendered outrage that freedom of speech and communication were being curtailed by a government which, in the opinion of a few, and who will be examined later in the paper, did not have jurisdiction over cyberspace. Barlowôs declaration demonstrates the many features of tension between the two sides.

Barlowôs work demonstrates how difficult it is to regulate such a nebulous matter when there is lack of democracy and governmental control.

In his opening paragraph, Barlow directs the speech to the óweary giants of flesh and steelô whereas he states that he comes from óthe new of Mindô. Human beings will always be the controllers of the Internet, however indirectly, it is the human will which directs robots to use the Internet, (14) and it is the human mind which has created the Internet. The Internet can never be separated from this innate link to humans. To argue that the Internet is the new Mind is treacherous to the very being and uniqueness of the human evolution. Barlow rightly opines that the Internet is without government or leadership and therefore to initiate laws can only be done via self-governance and organic growth from the users of the Internet. Barlowôs seminal work declares that humans have no place at restricting the Internet with real world laws and that the two worlds are distinctly separate. This view has many contentious issues relating to the practice of e-commerce to the protection of basic human rights for all Internet users. More so it is an issue for economic crime, if Barlowôsô views are projected into that of combating economic crime, then governance and control over the criminal act would have to come from the users of the virtual worlds. This would not be a practical solution as the users of the Internet would not have the jurisdiction to create a form of redress for the aggrieved person. This is because

there is no governance or legal structure within the Internet if Barlowôs views are to be carried out literally. Economic crime would be allowed to occur without consequences or redress.

What this paper will move onto discuss now is the development of the argument between separatists and inclusionistôs and how democracy and governance can be built for cyberspace. In essence the virtual worlds are a world within the Internet and as such when economic crime is committed within them, how do we, as regulators manage to control and govern?

What are we are unclear of is a) is there any law present to prevent this from occurring.

Laws of constraint

It is important to consider the notion of what is and where is the Internet located. The Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite (TCP/IP) to serve billions of users worldwide. It is a *network of networks* that consists of millions of private, public, academic, business, and government networks, of local to global scope, that are linked by a broad array of electronic, wireless and optical networking technologies. Therefore there is not just one network to govern but many. Within these networks and on the Internet there are many virtual worlds. To gain access to these networks and thus virtual worlds a person has to sign up with an Internet service provider (ISP). These IPSôs are private companies who offer its customerôs access to the Internet through their network. You can already see that even within one country there are many networks with many ISPôs. This poses problems with tracking users down. Adding an additional layer of complexity is the use of networks which are not registered to a person but to a company such as a business, a university or an Internet café, where access to the Internet is provided by the person contracting with the IPS is not the person using the Internet. Therefore accountability can be lost. This is why economic crime and money laundering is so difficult to monitor and control within the Internet but it is made even harder when the crime takes place within a virtual world. The virtual worlds add another layer of Internet ôbubbleô around the crime.

Virtual worlds as we have discussed is a world within the Internet providing a space for people to create their own world in which to live in. Many are worlds without laws or rules but that do have an affect on the real world. Moreover there is another point of contention in that there is a belief that the Internet is not global but rooted in state control, in other words *Lex Electronica*. In other worlds, the Internet and its control is governed by each countries own laws. Schultz states that, ôthe Internet and its regulation cannot be seen a single phenomenonô (10) therefore for regulation to work affectively we need to ôchallenge the conventional wisdom that the Internet is inexorably globalô (10) Schultz argued that the answers may be found in the ôreconsideration of private international law standards in the light of public international law standards of jurisdictionô (10) He argues, in ôfavour of double standards of jurisdiction for the regulation of Internet content; one based on the principle of targeting, used to sanction behaviour, the other an incarnation of the effects doctrine, used to prevent actions and fulfil the cathartic function of law.ô (10) Furthermore Shultz believes that regulation of the Internet is entirely possible and indeed integral to its importance in society. The idea that the Internet is a boarder less world (10) has dominated the jurisprudential thinking for Internet law for many years. Today we can move on and see that in fact it does have boarders and can be regulated.

The problem with the Internet is that it has no central authority through which all communications can flow through (11). This is known as cloud computing and demonstrates the unpredictability of the route the communication through the Internet will take. This was the intention of the Internet creators was to create a world connected through networks, where computers spoke one the common language (Internet protocol language) and thus created a global network. However through day-to-day use of the Internet, aspects of undesirable behaviour occurred and the Internet community have moved away from the desire to have the Internet recognised as a single entity but of many entities under the umbrella of the name Internet. The Internet community have largely, argues Engle and Keller, decided that they want each country to decide on the regulation of the Internet according to their own values and moral code. (12) Therefore the notion that the Internet is boarder-less is false. Each countryôs own law and moral codes depicts what is and what is not acceptable to be published on the Internet. Schultz argues that ósafeguarding local values is one of the foundational roles of the stateö (10) therefore they must adhere to this social contract in relation to the Internet. It is this notion which leads us into the realms of sovereignty and jurisdiction. If each country has an over-whelming need and right to protect their own country, and each countries set of laws differs in relation to the protection right then the Internet which does cross boundaries could be in breach of those laws in another country. The idea of where jurisdiction lies is often debated (13) and will be more so later in the paper but for now we shall consider the application of constraints in both virtual and the real world.

Lessigs (14) is one of the main commentators advocating a continuation of laws for cyberspace which mirror those in the real world. Lessig does not see that the Internet or cyberspace as being a distinct entity from that of the real world. His work has drawn upon inferences of real world application in cyberspace. (14) [1] Lessig sees that any type of behaviour whether it is conducted in the real world or the virtual is constrained by four factors. These are: 1. Law; 2. Social norms; 3. Market and price; 4. Nature and architecture. (14). Law is but one of four restraints on peopleôs behaviour and it is how the government or people in control monitor and regulate these than can affect the outcome of the application of the law. Laws regulate by issuing sanctions so that if one does not comply they will be punished through a sanction imposed by the rule maker. The second constraint, social norms are those socially accepted trends which depict how one will behave in society, for example if you drink a cup of tea you drink it from the cup rather than the saucer. The third constraint he outlines is that of the marketplace which outlines the price of good and what one is willing or can afford to pay for them. He denotes that through the device of price, the market sets many opportunities and those ranges of opportunities available it regulates. Finally he opines that nature or architecture constrains behaviour. The one major variance between the real world constraints and the virtual world or cyberspace

[1] For more see: Lessig, L. ôThe Zones of Cyberspaceö (1995-1996) Stanford Law Review, 48, pp.1403-1411. Lessig, Lawrence, Jonathan Zittrain, Charles R. Nesson, William W. Fisher & Yochai Benkler. *Internet Law* (Foundation Press 2002); Lessig, Lawrence. *The Future of Ideas: The Fate of the Commons in a Connected World* (Random House 2001); Lessig, Lawrence. *Code: and Other Laws of Cyberspace* (Basic Books 1999). Lessig, Lawrence. "The Place of Cyberlaw" in *The Place of Law* (Austin Sarat ed., University of Michigan Press, 2003); Lessig, Lawrence. "The Law of the Horse: What Cyberlaw Might Teach" in *Communications Law and Policy: Cases and Materials* (Jerry Kang, Aspen Law and Business, 2001); and for more of his works see Lessigs Bibliography held at Harvard University: http://www.law.harvard.edu/faculty/directory/index.html?id=888&show=bibliography accessed 21 February 2001.

constraints is that of anonymity which is built into the architecture of cyberspace through code. In cyberspace óhiding who you are, or more precisely features about who you are is the simplistic thing in the world. The default in cyberspace is anonymityô. (14) Lessig believes this is the key to óregulability ï the ability of governments to regulate behaviour there.ô (14) Due to this use of code or architecture Lessig has previously argued that óit renders [cyberspace] essentially unregulableô. (14) Lessig believes that cyberspace óhas the potential to be the antithesis of a space of freedomô (14) contrary to the mainstream view that ócyberspace is unregulable. [Where] [n]o national can live without it, yet no nation will be able to control itô. (14) This now rather out of date view was anticipated by Lessig in 1998. Lessig throughout his writing on the subject has criticised this notion of cyberspace being unregulated, rather the manner in which cyberspace is regulated must be done so in recognition of the four constraints, as outline above. He believes that the laws, norms, market place and architecture in cyberspace do regulate the Internet. It is not the actions of the individuals within the space but locating the people who commit acts of wrong doings. Lessig calls this the óregulability of Cyberspaceô. (14) In other words, regulability is the governmentôs ability to regulate behaviour in cyberspace. óCyberspace is a less regulable space than real space. There is less that governments can doô. (14) However Lessig believes to get round an unregulable cyberspace governments need to govern within state boundaries of jurisdiction. It is when the Internet crosses state or country boundaries that the Internet, due to its anonymity becomes unregulable. Lessig also denotes that within cyberspace there are many different architecturesô which are controlled and monitored by many different governments. Each of these different architectures reflects the political will of the government. Therefore the architecture for the Internet is akin to it having its own constitution. Lessig compounds this argument:

> óIt sets the terms upon which people get access; it sets the rules, it controls their behaviour. In this sense it is its own sovereignty. An alternative sovereignty, competing with real space sovereigns, in the regulation of behaviour by real space citizens.ô (14)

Netiquette

In this paper we have discussed two opposing views, one offered by Barlow who believes the Internet is a separate entity from the real world where laws and governance are bespoke to cyberspace. The other by Lessig who believes that laws are present in cyberspace but that behaviour can be controlled and monitored by governments through the fragmentation of regulation of the architecture.. In Barlowôs pronouncement he states: ôThe only law that all our constituent cultures would generally recognize is the Golden Rule.ô (9) This golden rule comes from Netiquette. Netiquette is a book written by Virgina Shea in 1994 and updated online in 1997. (15) It articulates the doôs and donôts of online interaction. The intentions of the core rules posed by Shea are for ónet newbiesô who may forget that when online their actions may have real world consequences. These being: *Rule 1:* Remember the human; *Rule 2:* Adhere to the same standards of behaviour online that you follow in real life; *Rule 3:* Know where you are in cyberspace; *Rule 4:* Respect other people's time and bandwidth; *Rule 5:* Make yourself look good online; *Rule 6:* Share expert knowledge; *Rule 7:* Help keep flame wars under control; *Rule 8:* Respect other people's privacy; *Rule 9:* Don't abuse your power; *Rule 10:* Be forgiving of other people's mistakes.

Rule number 1 is the Golden Rule as articled and used by Barlow. The golden rule or rule number 1, remember the human dispels Barlowôs argument that the users of cyberspace are separate from the real world. By remembering the human, Barlow is acknowledging that every act or behaviour undertaken on the Internet has a real world affect and that users must be aware of this. It acknowledges the constraints on both worlds as outlined by Lessig above. The golden rule therefore accepts the presence of law in the virtual world and makes the statement offered by Barlow obsolete. Rule 2 is also important as it enforces the same standards of law and ethics within cyberspace. She asserts that sometimes in cyberspace people are tempted to commit crimes they normally would not, because they think the chances of getting caught are slim. (15) Shea denotes that óthis is a book on manners, not a legal manual. However, Netiquette mandates that you do your best to act within the laws of society and cyberspaceô. (15) Therefore the rules which Barlow bases all his cyberspace governance on, is in fact, a book about manners assimilated from the behaviour norms and laws of the real world. Rule 8 also outlines the importance of privacy and copyright and enforces the need to abide by the laws of the country the user is in. Thus asserting the basic foundation that although the Internet can be considered as a separate entity it is based on the rules and governance of the real world.

Within this paper we are concerned with the regulation of economic crime within virtual worlds. From Lessig we can assert that there are rules present on the Internet and within each countries jurisdiction userôs behaviour can be controlled through the use of architecture and code alteration. From Barlow, despite his argument in the declaration of independence, there is a notion that despite the division of the worlds, the users of cyberspace must óremember the human, and therefore not act outside the remit of real world constraints. *The question is therefore, how does law from the real world be translated into the virtual worlds through the middle layer of Internet and cyberspace matter?* For example, if we see the real world as the inner layer of a circle, with the Internet being the middle layer and the virtual worlds being the outer circle, it is hard to transpose the real world laws into the many virtual worlds through the many Internet service providers. Regulation of the Internet has and is being discussed but the regulation of the virtual world is one step removed from this discussion as the regulations or change in code has to transverse yet another layer of anonymity and jurisdictional lines. The inherent difficulties of regulating not only the Internet but the virtual worlds can therefore be seen. From many real world laws pass through many ISPôs to many virtual worlds. The origins and the end of one law passing through these complex coding systems are almost impossible to monitor, control and regulate. The question posed above, óhow the Internet is different from the virtual worldsô, is just this. A complex web of interconnected networks each providing access to different virtual worlds, thus virtual worlds add another layer of complexity to the jurisdictional issues of cyberspace. To regulate and monitor virtual worlds is even harder for state authorities because of the lack of accountability and the anonymity of not only the end user but the ISP and the countries jurisdiction. The starting point therefore has to be to gauge what is achieved in terms of legality in cyberspace and to try to find a solution able to transfer these complex webs of the net and virtual worlds. What is clear is that there needs to be international co-operation to maintain a level playing field across all jurisdictions over what is condoned as acceptable behaviour on the net. However this would be very hard to achieve given the dramatic differences in countries laws and applications of even basic human rights and civil liberties.

Public policy and generally accepted norms would have to be considered and again this poses issues given to societal differences globally. Whether a unified agreed set of rules ever be agreed upon is nebulous as best. An additional issue that that even if rules are agreed upon and the above issues are transgressed the organic evolution of the virtual worlds will ensure that the laws are out of date before they become applicable. The time sensitivity of laws within virtual world means that real world laws will struggle to maintain pace with the technology. Reidenberg articulates that óthe current Internet technology create ambiguity or sovereign territory because network boundaries intersect and transcend national borders.ô(16)

Jurisdiction for virtual worlds

To say that the Internet or cyberspace is free from law is untrue. To say that virtual worlds are without laws is also untrue. However the laws are not joined up, in other words they are sporadic, piecemeal and do not provide the protection required. Why is this? Jurisdictions globally are struggling with the notion of cyberspace and how all the many networks, IPSôs and virtual worlds can be encompassed within one set of rules of regulations. We can see from cases such as Yahoo (17) and Zippo (18) that courts are making important decisions into the remit of jurisdiction in cyber law cases. However whether they can be translated into the virtual world is unclear. Yahoo was the first case where a foreign court imposed their countryôs will on another through the Internet. Zippo too was a seminal case, establishing the Zippo sliding scale of minimum standard of contact to establish jurisdiction. Both these cases related to cyberspace and as we have established virtual worlds are contained as separate entities inside cyberspace. Therefore they need to be extrapolated into the virtual world. It too has been established that laws are present in cyberspace and that whether it be a separatist view or an inclusionist view, cyberspace and the virtual world do have an impact on the real world. Therefore we can use this as a foundation for examining whether virtual worlds can a) have rule of law, therefore is able to have laws pervade into them from the real world and b) who has jurisdiction.

Economic crime in virtual worlds has real world effects, whether this is fraud or money laundering a human being (Barlowôs Golden Rule) is being harmed. In most real world legal system, economic crime and money laundering is against the law. Criminals are using the Internet to create new ways of committing crime and because of the network of ISPôs and many virtual worlds, jurisdiction is hard to establish. Theoretically though if we take the inclusionist point of view we can view use real world laws to establish a legal system within virtual worlds. To enter a virtual world, everyone needs to go through an IPS to log onto the Internet and sign into the virtual world. Each IPS is registered and controlled in a real world jurisdiction. If each of these ISPôs ensures that all their users are required to sign a contract which overtly acknowledges that they shall not commit economic crime or launder money and if they do they shall a) be reported to the relevant authority and b) have their ISP rights revoked and be banned from access the Internet for a period of time. This would allow each jurisdiction to deal with the person under their own legal system but also would prevent virtual worlds harbouring criminals. In many ways this resembles the technological blocking which many countries use to prevent access to the Internet.

Combating Virtual Financial Crime

Despite the problems of regulating cyberspace as iterative above by the views of the separatists and the inclusionists, the lack of compliance and monitoring, there is a real and present need to find a solution to this in order to combat virtual economic crime. Interpol state four main aspects to consider in the future to combat virtual financial crime. Those being:

- Law enforcement agencies need to know where servers are based in instances of financial crime. These may be located in different countries which may pose a problem when it comes to locating the legal form which is to be taken. There needs to be a collaborative database which record where servers are based and this information needs to be shared between law enforcement agencies. In order for there to be an agreement as to the legal form which is to be taken countries should create an agreement in advance of any instances of economic crime.
- Law enforcement agencies need to influence legislatures in the future to take into account virtual financial crime when drafting new pieces of legislation. Consideration needs to be given not only for prosecution but also the recovery of assets and information from each virtual crime committed.
- Barriers between law enforcement agencies and the industry must be broken down to ensure for accountability of data crossing networks. This could be achieved by creating an international research project which sets up and creates databases on server locations and works in conjunction with countries to agree on locality of law for instances of financial crime.
- Law enforcement agencies need to learn how to investigate virtual crimes. (19) This can only be done through collaborative partnership and the sharing of ideas and practices on combating virtual economic crime.

Conclusion

The debate regarding law within cyberspace and virtual worlds is nebulous at best. Technology is forever changing and so is the theoretical debate. However what can be seen is that criminals are now using cyberspace and virtual worlds for criminalsô acts. Each of these criminalsô acts has an effect on the real world. For democracies to sit by and watch this happen breaches our moral, ethical and legal codes. It is also clear that to control and monitor the Internet is a complex task and no single definitely answer has been found as to how to do this for the best. Virtual worlds add an extra layer of complexity to this debate due to the passage of information through many ISPôs, many networks and many virtual worlds. It is a tangled web which must be unwoven to establish jurisdiction. . Therefore the answer must lie in adopting real world laws into cyberspace and virtual worlds. To do this though requires decisions. Should each country monitor and control their own ISPôs providing them with jurisdiction? But what happens in jurisdictional cross overôs? If this is the case, should there instead be an international agreement as to what is acceptable conduct in cyberspace and virtual worlds? If this is the preferred option, who holds jurisdiction, who governs the Internet, and what laws are in place? Questions like these will only be answered over time through organic development. Due to the fluidity of the Internet and its whole purpose of being controlling and monitoring although must be done must be done so carefully and slowly. To get it wrong prevents freedom of speech and communication and

promulgates even more economic crime. To get it right would involve a meeting of the minds, something which the Internet should promote.

References

1. Fraud Advisory Panel. óCyber Crime: Social Networking and virtual worldsô, Issue 4, October 2009. http://www.fraudadvisorypanel.org/new/pdf_show.php?id=119 accessed 15 July 2010.

2. Catronova, E. óOn Virtual Economiesô, CESifo Working Papers, No. 752. July 2002

3. Interpol. óCybercrime fact sheetô, 2008. COM/FS/2008-07/FHT-02

4. Ryder, N. ñThe Financial Services Authority, the Reduction of Financial Crime and the Money Launderer ï A Game of Cat and Mouseò, (2008) Cambridge Law Journal, 67(3), 635-653.

5. Financial Action Task Force. óReport on New Payment Methods.ô October 2006. http://www.fatf-gafi.org/dataoecd/30/47/37627240.pdf accessed 16 July 2010.

6. Desguin, H. óMoney laundering through virtual gamesô. Strategic assessment. Florida Department of Law Enforcement, Office of Statewide Intelligence, October 2008. p.15.

7. US Department of Justice National Drug Intelligence Centre. óMoney laundering in digital currenciesô. Product No. 2008-R0709-003, June 2008. p.3.

8. NDIC 2006-R0803-001, óPrepaid stored value cards: A potential alternative to traditional money laundering methodsô, 2006.

9. Barlows, J. P. óDeclaration of Independence of Cyberspaceô, 8 February1996, https://projects.eff.org/~barlow/Declaration-Final.html accessed 8 February 2011.

10. Schultz, T. óCarving up the Internet, Jurisdiction, Legal Order and the private/Public International law Interfaceô, (2008), The European Journal of International Law, Vol.19, No.4. pp.801.

11. For more information see: Zittrain, óBe careful what you ask for: reconciling a global Internet and local law, in Thierer, A. & Crews, C.W. (eds), óWho Rules the Net? Internet governance and jurisdictionô, 2003, Washington D.C., Cato Institute, ISBN: 1-930865-43-0 at p.13.

12. Engle, C. & Keller, K.H. óGlobal networks and local values: A comparative looking at Germany and the United States, (2002) Washington, National Research Council, pp. 241, quote at p.46ff.

13. Wang, F.F. óObstacles and Solutions to Internet Jurisdiction: A comparative analysis of the EU and US Lawsô, (2008), Journal of International Commercial Law and Technologyô, Vol. 3, Issue 4, pp.233-241.

14. Lessig, L. óThe Laws of Cyberspaceô, Draft 3. (1998) presented at Taiwan Net ô98 conference, in Taipei, March 1998. http://www.lessig.org/content/articles/works/laws_cyberspace.pdf accessed 21 February 2011. pp.2.

15. Shea, V. óNetiquetteô, Albion Books, 1994, US. http://www.albion.com/bookNetiquette/0963702513p4.html accessed 16 February 2011.

16. Reidenberg, J.R. óTechnology and Internet Jurisdictionô, (2005) University of Pennsylvania Law Review Vol. 153. pp.1951-1974.

17. Ligue contre le racisme et l'antisémitisme et Union des étudiants juifs de France c. Yahoo! Inc. et Société Yahoo! France (LICRA v. Yahoo!) 2000

18. Zippo Mfr. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (W.D. Pa. 1997)

19. Interpol. ôVirtual Moneyô 27 May 2010.
http://interpol.int/Public/TechnologyCrime/CrimePrev/VirtualMoney.asp accessed 27 May 2010.