scripted

Volume 7, Issue 1, April 2010

THE ONLINE PUBLIC OR CYBERCITIZEN

Andrew Power[*]

Abstract

As both citizens and the state increasingly use online mediated environments, the nature of the public and thus public law has changed. As individuals and state actors use avatars as their online representatives in virtual environments, the notion of the cybercitizen is growing in importance.

In these environments, rules, protocols and acceptable behaviours exist amongst participants and are no less respected by the community they affect for their current lack of legal status. As governments move more of their activities online the state is recognising and legitimising a new public, or at least a new expression of public.

This paper looks at examples of the application of law to this new constituency and seeks to examine different ideas of identity and governance in an online mediated environment. It seeks to answer the question of whether the public can have coherent, congruent meanings across disparate areas of law, and to broaden the understanding of cyberlaw.

DOI: 10.2966/scrip. 070110.185

[*] Head of School of Creative Technologies at the Institute of Art, Design and Technology, Ireland; Doctoral student of Governance at Queens University Belfast.

1. Crime Online

Technology and crime have had a long association; the Internet simply provides a new medium for them. In discussing online crime a distinction should be drawn between activities - such as online theft – that are clearly crimes, private law issues such as disputes between buyers and sellers of online goods, and issues of anti-social behaviour or harassment. Some activities, such as spamming can, depending on severity, target, and context, fit into any of the these three categories.

The term 'cybercrime' thus encompasses this whole range of activities, but agreement on a single definition has not yet been achieved. Definitions include that used by Princeton University: "crime committed using a computer and the internet to steal a person's identity or sell contraband or stalk victims or disrupt operations with malevolent programs"[1] and the definition set out in the New World Encyclopedia:

> [A] term used broadly to describe activity in which computers or computer networks are the tool, target, or place of criminal activity. Cybercrime takes a number of forms including identity theft, internet fraud, violation of copyright laws through file sharing, hacking, computer viruses, denial of service attacks, and spam.[2]

The IT security company Symantec defines two categories of cybercrime:

> Type I, examples of this type of cybercrime include but are not limited to phishing, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud. Type II cybercrime includes, but is not limited to activities such as cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities.[3]

More succinct definitions include: "crimes perpetrated over the internet, typically having to do with online fraud"[4] and "crime committed using the Internet, for example stealing someone's personal information or introducing harmful programs into someone's computer".[5] Against this background, this paper takes a broad definition of the term cybercrime to include a range of activities, from those that are clear breaches of criminal law to those more properly described as private law issues.

---

[1] Available at http://wordnetweb.princeton.edu/perl/webwn?s=cybercrime (accessed 24 March 2010).

[2] Available at http://www.newworldencyclopedia.org/entry/Cyber_crime (accessed 24 March 2010).

[3] Available at http://www.symantec.com/norton/cybercrime/definition.jsp (accessed 24 March 2010).

[4] Available at http://www.pcmag.com/encyclopedia_term/0,2542,t=cybercrime&i=40628,00.asp (accessed 24 March 2010).

[5] Available at http://www.macmillandictionary.com/dictionary/british/cybercrime (accessed 24 March 2010).

The first case of Internet fraud was brought by the Federal Trade Commission in the US in 1994.[6] An early example of law being applied to online activity in the UK was Scotland's *Shetland Times v Wills,* involving the link of one paper's content to the website of another.[7] The issues of freedom of speech and protection from junk mail were fought out[8] in *Cyber Promotions v America Online* in 1996, and a defining case for the emerging field of cyberlaw was the 2000 case of *Yahoo!* v the French government, regarding the sale of Nazi memorabilia.[9]

In the absence of online police or a central controller of the Internet, the early focus was on the Internet Service Providers ("ISPs"), but over time the number and type of players have expanded. Search engines like Google have grown in importance; aggregators combine information and customise it to provide a single source of knowledge to users; blogs propagate the views of individuals to potentially huge audiences. All these have contributed to a changed and more complex environment. The advent of virtual machines, in which servers exist as software rather than hardware, makes the notion of tracking online activity to a physical location a meaningless concept.[10]

Until recently, two categories of crime were being committed online. The first comprised those crimes which had existed offline but were now greatly facilitated by the Internet. This included misuse of credit cards, information theft, defamation, blackmail, obscenity, hate sites, money laundering, and copyright infringement. The second category was made up of crimes that had not existed before and included hacking, cyber vandalism, dissemination of viruses, denial of service attacks, and domain name hijacking. National laws were introduced in many jurisdictions in an attempt to combat these crimes[11]. Different approaches were tried, such as the *Convention on Cybercrime*[12] developed by the Council of Europe, and the US *National Strategy to Secure Cyberspace*[13]. Europe's Convention was created to "pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation." It deals particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. The American national strategy is part of the greater 'Homeland Security' project and is focused on preventing terrorist attack.

---

[6] E Katsh, "Online Dispute Resolution: Some Implications for the Emergence of Law in Cyberspace" (2007) 21:2 *International Review of Law, Computers & Technology* 97-107.

[7] *Shetland Times Ltd v Jonathan Wills and Another* [1997] SLT 669.

[8] D Post, "Governing Cyberspace" (1996) 43:1 *The Wayne Law Review* 155- 171.

[9] L Edwards, "The Changing Shape of Cyberlaw" (2004) 1:3 *SCRIPT-ed* 363-368.

[10] C Arthur and A Brown, "How to turn one computer into many" (2007) available at http://www.guardian.co.uk/technology/2007/nov/08/news.software (accessed 19 Nov 2009).

[11] An overview of the UK law in this area is available at JISC Legal http://www.jisclegal.ac.uk (accessed 19 Nov 2009).

[12] The Convention on Cybercrime is available at http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=185&CL=ENG (accessed 19 Nov 2009).

[13] The National Strategy to Secure Cyberspace is available at http://www.dhs.gov/xprevprot/programs/editorial_0329.shtm (accessed 19 Nov 2009).

As the web evolves from a communications system into a social and commercial environment, we are learning which businesses are best suited to this new online world. More and more people are buying and selling goods and services online, building relationships and seeking entertainment. In this environment, we have to ask who makes the rules, and who can enforce them? In addition to the regulation of business on the Internet, there is a growing need to look at a third category of crime, crimes against the person, the online public or cybercitizen.

2. Offences against a Virtual Public

Issues such as the digital divide, which existed both in economic and generational sense, are beginning to retreat. As technology becomes cheaper, more intuitive, and more prevalent, the barriers to entry are falling. The children of the dot.com generation, the digital natives, are becoming the students and entrepreneurs of today.[14] These digital natives are increasingly living in a world of virtual reality via environments like Second Life[15] and World of Warfare. Second Life, despite its rapid growth and current population of 13 million users is still one of the smaller virtual worlds. It is dwarfed by the number of children using clubpenguin.com, webkinz.com, and barbiegirls.com, amongst many others.[16] These children will have none of the reluctance of their parents about online interaction[17]. The new environments they inhabit will lead to new ideas of identity, new ideas of 'the public' and inevitably new crimes.

Individuals acting through their online avatars[18] or alternate personas constitute a new public, and present new issues of governance, both in cyberspace and of cyberspace. Harassing another individual through their online representation may be criminal or at the very least anti-social. There is however no doubt that these activities can lead to very real crimes offline.

The 'law of the land' does intervene when activities online 'spill out' into the real world, such as when the theft of online virtual goods leads to serious crime offline. In June 2005, Qiu Chengwei, a Chinese national, won a virtual sword in the online game

---

[14] Prensky discusses the generational differences in the way we use and interact with technology. He suggests that students today think differently and process information differently from previous students because of their interaction with technology. These students he calls Digital Natives. M Prensky, "Digital Natives, Digital Immigrants" (2001) from *On the Horizon,* 9:5 MCB University Press.

[15] Second Life was created by Linden Labs of San Francisco. It allows users to create their own world communities with images, sound, and video from the real world. Second Life allows users to form communities for discussion, to buy online property, and develop businesses and other organisations. Business is done in 'Linden dollars' that can be converted to real US currency.

[16] D Wyld, "Government in 3D: How Public Leaders Can Draw on Virtual Worlds" (2008) *IBM Centre for The Business of Government,* available at http://www.businessofgovernment.org/pdfs/Wyld3dReport.pdf (accessed 19 Nov 2009).

[17] Children born after 1980 have been referred to as Millennials. They have grown up surrounded by digital media and are said to be sociable, collaborative, open-minded, confident, and achievement-oriented. A Junglas "Identity Formation, Learning Styles and Trust in Virtual Worlds" (2007) 38:4 *Database for Advances in Information Systems* 90-97.

[18] The Sanskrit word avatara means incarnation. In computing an avatar is a representation of the user in the form of a three-dimensional model.

Legend of Mir 3. He lent the sword to a fellow gamer Zhu Caoyuan who subsequently sold it. When Qiu reported the incident to the police he was told a virtual sword was not real property and was not protected by law. Qiu went to the home of Zhu and stabbed him to death in a very real crime for which he is now serving a life sentence.[19] In 2008, a Russian member of the Platanium clan of an MMORPG (massively multiplayer online role-playing game) was assaulted in the Russian city of Ufa by a member of the rival Coo-clocks clan in retaliation for a virtual assault in a role playing game (probably Lineage II). The man died of his injuries en route to hospital.[20] As a result of these incidents and others like them some countries, such as South Korea, have set up a section within the police force specifically to deal with 'in-game' crime.[21]

Even if the activity remains online and does not spill over into the real world, it is clear that crime can occur. In August 2005 a Japanese man was arrested for using software 'bots'[22] to 'virtually' assault online characters in the computer game *Lineage II* and steal their virtual possessions. He was then able to sell these items through a Japanese auction website for real money.[23] In October 2008, a Dutch court sentenced two teenagers to 360 hours of community service for 'virtually' beating up a classmate and stealing his digital goods.[24] Also in 2008, a 43 year old Japanese piano teacher who was 'virtually' married to a man in the online role playing game *Maple Story*, was so upset when he 'virtually' divorced her that she hacked his PC and deleted him from the game, thus committing a sort of 'virtual murder'.[25] This resulted in her arrest for illegally accessing his computer, and may yet result in a civil suit for damages.[26] In 2007, a Dutch teenager was arrested for stealing virtual furniture from 'rooms' in *Habbo Hotel*, a 3D social networking website; this virtual furniture was

---

[19] Reuters, "Gamer gets life for murder over virtual sword" (2005), available at http://news.cnet.co.uk/gamesgear/0,39029682,39189904,00.htm (accessed 19 Nov 2009).

[20] F Truta, "Russia - Gamer Kills Gamer over Gamer Killing Gamer... Er, In-Game!" (2008), available at http://news.softpedia.com/news/Russia-Gamer-Kills-Gamer-over-Gamer-Killing-Gamer-Er-In-Game-76619.shtml (accessed 19 Nov 2009).

[21] BBC, "Game theft led to fatal attack" (2005), available at http://news.bbc.co.uk/1/hi/technology/4397159.stm (accessed 19 Nov 2009).

[22] Also known as web robots, bots are software applications that run automated tasks over the Internet.

[23] W Knight, "Computer characters mugged in virtual crime spree" (2005), available at http://www.newscientist.com/article/dn7865 (accessed 19 Nov 2009).

[24]The Irish Times, "Woman faces jail for hacking her virtual husband to death" (2008), available at http://www.irishtimes.com/newspaper/frontpage/2008/1025/1224838828960.html (accessed 19 Nov 2009).

[25] Associated Press, "Japanese woman faces jail over online murder" (2008), available at http://www.guardian.co.uk/world/2008/oct/24/japan-games (accessed 19 Nov 2009).

[26] J Emigh, "Online gamer arrested for 'virtual murder' in Japan" (2008), available at http://www.betanews.com/article/Online-gamer-arrested-for-virtual-murder-in-Japan/1224888499 (accessed 19 Nov 2009).

valued at €4,000.[27] In Britain, a couple are divorcing after the wife discovered her husband's online alter-ego was having an affair online with another, virtual, woman.[28]

Offensive activities such as online assault, or even rape, have had very real effects, reportedly resulting in depression and suicide. This cyber bullying can occur as people become more closely associated with their online persona, to the extent that it is viewed, both by themselves and others, as an extension of self. A study of online bullying was conducted by Microsoft to mark the EU Commission's Safer Internet Day 2009, and in Ireland 22% of teenagers reported some form of online bullying, almost half of which occurred on social networking sites.[29]

3. Online Identity

Early studies of computer mediated communication in the 1980s suggested that email removed the social context clues such as gender, age, race, social status, and facial expression which induced a disinhibiting effect upon participants.[30] The advent of 3D virtual environments and the ability of participants to represent themselves as avatars provided an opportunity not only to hide social context clues, but to create alternate ones. This visual representation of self, and the ability to alter it, has introduced a new dimension to communication within online communities. In a survey of Second Life avatars, 45% said they tried to portray a "better" body image, 37% chose to portray themselves as younger, and more than 20% altered their gender.[31]

Turkle found that individuals working alone with computers used them in a gaming environment to work through issues of control and mastery.[32] When the computer was used as a communications medium the control provided by the computer helped to develop skills for collaboration and even intimacy. The medium allowed for the exploration of self and social context. Status Theory seeks to explain identity in terms of the process of exploration. Exploring virtual worlds offers us the opportunity to alter or control the exploration experience. Identity Theory sees identity as a lifelong and constantly evolving process of resolving the conflict between positive and negative developmental possibilities. Again the virtual environment provides opportunities to manufacture these developmental experiences. Virtual environments allow users to explore in safety elements of their personality which may be

---

[27] BBC, "Virtual theft leads to arrest" (2007), available at http://news.bbc.co.uk/2/hi/technology/7094764.stm (accessed 19 Nov 2009).

[28] Available at http://www.guardian.co.uk/technology/2008/nov/14/second-life-virtual-worlds-divorce (accessed 1 Feb 2010).

[29] A Sheehan, "One in five teens bullied online" (2009) available at http://www.independent.ie/national-news/one-in-five-teens-bullied-online-1635183.html (accessed 19 Nov 2009).

[30] M Williams, "Avatar Watching: Participant Observation in Graphical Online Environments" (2007) 7:1 *Qualitative Research* 5-24.

[31] WJ Au, "Surveying Second Life" (2007) *New World Notes* available at http://nwn.blogs.com/nwn/2007/04/second_life_dem.html (accessed 19 Nov 2009).

[32] S Turkle, "Constructions and Reconstructions of Self in Virtual Reality: Playing in the MUDs" (1994) 1:3 *Mind, Culture and Activity* 158-167, at 159.

underdeveloped. The cloak of an avatar can be used to encourage a cautious person to be more experimental or creative.[33]

The negative impact of this is the disinhibiting effect on a person's actions. There is the possibility of removing a sense of responsibility for the actions of your avatar. There can also be the objectification of a "character" in a game, which may be another player or may be just software. The potential to undermine an individual's inhibitions combined with the ability to act anonymously has the potential to lead to a breakdown in acceptable behaviour.

A second issue is identity security and identity theft. Our identity has been reduced to a series of facts such as name, gender, date of birth, social security number, and so on, and stored on multiple databases. It may even be further reduced to a number or a password. Where is all of this information stored, is it accurate, is it secure, is it consistent between systems, who has access to it, who can edit it? Of all the information held what is the minimum subset required to establish identity in the eyes of authority? The introduction of the Identity Cards Act 2006 in the UK assumes that one person has one identity. It reduces identity down to a defined collection of recorded data and the standard for establishing identity is thus reduced. If error, fraud or impersonation occurs it is left to the wronged individual to establish the truth of the situation.[34]

4. National Laws or Cyber Laws

There are two views about the need for 'cyberlaws'. One side argues that rules for online activities in cyberspace need to come from territorial states.[35] The other side argue that there is a case for considering cyberspace as a different place where we can and should make new rules. Johnson and Post were among the first to argue that cyberspace constitutes a new and different space where different rules must apply.[36] Their argument was that in the off-line world there is generally a correspondence between borders drawn in physical space, between nation states, and borders in legal space. The point at which one set of laws stops and another starts is normally at the physical border of a country. This correspondence is the result of four interrelated factors. First, the *power* to control a space: law-making requires the ability to enforce the law and impose sanctions, which is a function of national governments. Second, the *effect* of a law given the proximity of the law maker to those affected. A third consideration is the *legitimacy* of the law, or the degree to which the law is implemented with the consent of the governed. Finally, the *notice* given to those affected by the law, or the warnings provided to those affected to abide by a given law. The advent of the Internet has broken the link between geography and these four principles. How does an individual know where the other individuals, services or institutions might be located or what rules, if any, apply?

---

[33] A Junglas, "Identity Formation, Learning Styles and Trust in Virtual Worlds" (2007) 38:4 *Database for Advances in Information Systems* 90-97.

[34] C Sullivan, "Conceptualising Identity" (2007) 21:3 *International Review of Law, Computers & Technology* 237-261.

[35] JL Goldsmith, "Against Cyberanarchy" (1998) 65 *University of Chicago Law Review* 1199-1250.

[36] D Johnson and D Post, "Law and Borders – The Rise of Law in Cyberspace" (1997) 48:5 *The Stanford Law Review* 1367-1402.

Is there a virtual space or cyberspace where traditional legal systems have no jurisdiction, where a new order can be built by the inhabitants of that space? The idea of cyberspace as a place you can go to where new laws might apply is supported by the fact that you must make a decision to go there, normally by deciding to access a computer and enter a password. In this sense there is a boundary you cross to get 'there'. David Post suggested that it may be that cyberspace could signal the "final days of a governance system relying on individual sovereign states as [the] primary law-making authority, a system that has served us, often for better and sometimes for worse, for the last half millennium".[37]

Two opposing models of governance have been suggested. The first is a centralised system of control, which would involve coordination among the existing sovereign powers and some form of multilateral agreement or 'Grand Internet Treaty'. This would also require the establishment of international governing bodies similar to the World Trade Organization.

A second option is the decentralisation of law-making and the development of processes that do not impose a framework of law but allow one to emerge. In this case, individual service providers would develop their own systems of governance and standards of behaviour; the law will come from the bottom up as users select services, products and environment that match their standards and ethics. In this scenario our understanding of justice may change as we see what emerges from un-coerced individual choice.[38] The relative legitimacy of hard versus soft laws may depend on the society they are seeking to govern. In the context of online social networks, soft laws have a power and system of enforcement more effective than the hard laws that might attempt to assert legitimacy.[39]

A third, and more interesting approach is suggested by Cannataci and Mifsud-Bonnici, who make the case that there is developing a mesh of private and state rules and remedies, which are independent and complementary.[40] Users adopt the source of these rules and remedies based on their 'fitness for purpose'. State regulation may be appropriate to control certain activities, technical standards may be more appropriate in other situations, and private regulation may be appropriate where access to national courts or processes is impossible. The intertwining of state and private regulation is both inevitable and necessary to provide real-time solutions to millions of online customers and consumers. This should lead to greater collaboration between private groups and states in the development and administration of rules. The mesh of regulation, like that of a fishing net, is more effective in catching larger participants than smaller ones. Corporate organisations are more likely than individuals to comply with regulations, thus the task of governance is to reduce the gaps in the mesh. Swire uses the metaphor of elephants and mice to explain this situation:

---

[37] D Post, "Governing Cyberspace" (1996) 43:1 *The Wayne Law Review* 155- 171.

[38] *Ibid.*

[39] Hard law refers to the binding rules and regulations that make up legal systems in the traditional sense; soft law consists of informal rules which are non-binding but may, due to cultural norms or standards of conduct, have practical effect.

[40] J Cannataci and JP Mifsud-Bonnici, "Weaving the Mesh: Finding Remedies in Cyberspace" (2007) 21:1 *International Review of Law, Computers & Technology* 59-78, at 60.

> In short elephants are organisations that will be subject to the law, while mice can hope to ignore it. Elephants are large companies or other organizations that have major operations in a country. Elephants are powerful and have a thick skin, but are impossible to hide. They are undoubtedly subject to a counties jurisdiction. Once laws are enacted, they likely, will have to comply. By contrast mice are small and mobile actors, such as pornography sites or copyright violators, who can reopen immediately after being kicked off a server or can move offshore. Mice breed annoyingly quickly – new sites can open at any time. Where harm over the Internet is caused by mice, hidden in crannies in the network, traditional legal enforcement is more difficult.[41]

The current situation is in some ways clear in that the degree of 'seriousness' of the activity is a measure of how it is treated. Criminal activity continues to be addressed by national laws, and greater cooperation between states is the best route to all forms of crime that cross national borders. Civil wrongs are where possible addressed through the service provider and in some cases via the civil courts. Other anti-social activity, of the hacking or spamming variety, is tackled, where possible, by technical solutions, and the cat and mouse game between hackers and the software security industry continues. However, the more we are living and interacting online the more examples there are of attempts to provide online solutions to online problems. At the moment this is largely at the lower end of a scale of cost of loss, or level of serious wrong doing, but perhaps it gives clues to future solutions.

One such example is online dispute resolution ("ODR"). The flow of information across national borders weakens the application of law and creates increasingly complex online relationships. A new means of establishing standards of behaviour and or preventing and resolving disputes is needed. The growth of ODR was "not intended to challenge or displace an existing legal regime but to fill a vacuum where the authority of law was absent".[42] Katsh describes a number of experiments with ODR: a Virtual Magistrate to aid in disputes between ISPs and users, an Online Ombudsman Office to offer a general dispute resolution service (run by the University of Massachusetts) and an ODR to resolve family disputes (proposed by the University of Maryland).[43]

In the case of eBay, the ability of the company to be successful is dependent on the trust of customers that goods and services will exchange at agreed prices, and that buyers and sellers will act in good faith. The feedback rating system goes someway to providing this assurance to customers, but when disputes do arise there needed to be an effective process for dispute resolution. eBay engaged an Internet start up,

---

[41] P Swire, "Elephants and Mice Revisited: Law and Choice of Law on the Internet" (2005) 153 *University of Pennsylvania Law Review* 1978-1979.

[42] E Katsh, "Online Dispute Resolution: Some Implications for the Emergence of Law in Cyberspace" (2007) 21:2 *International Review of Law, Computers & Technology* 97-107, at 99.

[43] *Ibid.*

SquareTrade.com to provide this service. By automating the process and using web pages with forms and options to choose from, rather than an open ended email system, SquareTrade was able to handle many million individual disputes over the course of a year.

Wikipedia, the online encyclopaedia, also has a dispute resolution process to manage conflicting opinions or challenges to facts. It provides a service to track changes to entries, notify interested parties and facilitate changes were necessary. This system is necessary to create trust in the accuracy of the information provided as well as to resolve conflicts amongst contributors.

This intertwining of state, private, and technical solutions is likely to continue to develop as the de-facto model of Internet governance. That some 'Grand Internet Treaty' will be agreed between states seems less and less likely. At the 2005 International Summit on the Information Society in Tunis, Internet Governance was defined as:

> ...the development and application by governments, the private sector, and civil society, in their respective roles, of shared principles, norms, rules, decision making procedures and programmes that shape the evolution and utilisation of the Internet.[44]

5. Law-makers Online

Governments on both sides of the Atlantic are taking the issue of virtual life more seriously and beginning to engage with the online citizen directly. Early attempts at this involved putting existing services like revenue or motor tax online, but the process of lawmaking itself is now also becoming increasingly consultative. In a changing and increasingly virtual world government is reconnecting with the citizens where they are.

An attempt at creating a cyber-parliament occurred in the social networking site Second Life. In the United States a virtual House of Representatives was created by George Miller, a California Democrat, and chairman of the House Education and Labour Committee. Miller worked with George Lucas and John Gage of Sun Microsystems who together with Internet marketing company Clear Ink, built an entire virtual world for members of Congress and citizens to meet.[45] In January 2007 Miller held a Second Life 'press conference'[46] and is now running a project called 'Ask George', which allows voters to ask questions using videos, blogs, Facebook, text messages, Twitter, or email. Newt Gingrich, the former Speaker of the U.S. House of Representatives, spoke at Second Life's virtual Capitol building complete with virtual hecklers. A number of protesters were confined to an area behind the main seats, where they displayed banners like 'Conservatism Kills' and typed anti-

---

[44] Working Group on Internet Governance (2005) "Report of the Working Group on Internet Governance" available at http://www.wgig.org/docs/WGIGREPORT.doc (accessed 19 Nov 2009).

[45] S Grove, (2007) "A Second Life in Politics" available at http://abcnews.go.com/Politics/Story?id=2809023&page=1 (accessed 19 Nov 2009).

[46] CNET News (2007) "Images: Virtual politics in Second Life" available at http://news.cnet.com/2300-1028_3-6147452-1.html?tag=mncol (accessed 19 Nov 2009).

Republican slogans.[47] In 2008, Ed Markey the democratic representative for the state of Massachusetts and chair of the House Energy and Commerce Subcommittee on Telecommunications and the Internet, held a congressional hearing simultaneously in congress and online.

During the presidential campaign in the United States supporters of Hillary Clinton, Barack Obama and John Edwards set up de-facto headquarters and social organisations within Second Life. The communal aspect made it a good place for politicians to connect with a new group of voters, and had the advantage over blogs and chat rooms, given the physicality of the experience. The combination of real-time communication and movement with physically embodied characters or avatars results in an experience that is more realistic or involving than that of other online interactions. Second Life provides a strong sense of place during participation and, according to Nancy Scola, can be thought of as a physical Internet.[48]

In the French presidential election of 2007 all four major candidates opened virtual headquarters in Second Life to engage in debates, hold political rallies and take part in protests. Le Pen was the first French presidential candidate to do so, and was also the first to have the headquarters attacked by protesters. The campaigns attempted to create cyber-headquarters that reflected the personality and politics of the candidates. Interest in the French presidential campaigns was so high that during the election France ended up with the second highest number of Second Life avatars (subject only to the US) of any country.

6. Conclusion

As more and more of us spend a growing portion of our day online the concept of the cybercitizen is now established and recognised by business, government, and society. We are still learning how to recognise this concept in the law and to build an understanding of how this entity relates to national laws. The idea that in the future our behaviour will be governed by a network of national laws, user defined principles, technical requirements, and corporate guidelines, seems more and more likely. How breaches of this mesh of regulation, how we define appropriate behaviours in the many contexts in which we will interact with other, and the impact this will have on our ideas of governance, we will only see over time.

---

[47]E Reuters (2007) "Second Life Ready for Primetime at Gingrich event" available at http://secondlife.reuters.com/stories/2007/09/27/second-life-ready-for-primetime-at-gingrich-event/ (accessed 19 Nov 2009).

[48] N Scola, "Avatar Politics: The Social Applications of Second Life" (2007), available at http://www.ipdi.org/UploadedFiles/Avatar%20Politics.pdf (accessed 19 Nov 2009).