EJLT European Journal of Law and Technology

Human versus Inalienable Rights: Is there still a future for online protest in the Anonymous world?

Martina Gillen [1]

Cite as: Gillen, M 'Human versus Inalienable Rights: Is there still a future for online protest in the Anonymous world?' European Journal for Law and Technology, Vol. 3, No. 1, 2012

1. Abstract

The protection of legitimate political protest is one of the hallmarks of a functional liberal democracy. Certainly, there is increasing legal debate about the parameters of what constitutes legitimate protest and the appropriate scope of police powers to regulate it. However, there is no widespread call for the dismantling of the concept of a right to protest. The same consensus is not present however when one considers the right to protest in cyberspace. This article considers the possible reasons for this beginning with the recent practice of protest online, then by considering factors which may affect the legitimacy of that practice or which are unique to the online environment. The main argument of this paper is that human rights discourse as interpreted by the judiciary is very much focused on humans beings as embodied entities and thus has difficulty recognising that a human being acting in the disembodied sphere of cyberspace is still a rights bearing agent. In other words the disembodied human is alienated from their rights. With this in mind we shall explore the legal framework in which online protest operates within the EU and offer some suggestions about how online protest could be better managed and protected.

2. Introduction

The foundations of political protest online (what is traditionally understood by the term hacktivism) were laid down by the founding parents of the internet based upon their philosophical and ethical commitment to freedom of speech and their mastery of their technological sphere. [2] This has left the activity with something of an anarchic heritage and an anarchistic approach to activism. Nowhere has this been more evident in recent months than in the activities of the 'groups' known as Anonymous and Lulzsec. The activities of these groups range from those which fall clearly into within the range of the sort of activity that would normally attract the label of political protest (such as enabling election news to be channelled out of Iran), to those which occupy a 'grey' area such as the Chanology project (which purports to debunk financial abuses at the heart of Scientology provoked by its suppression of information about itself on the Internet) and the defacement of the SOCA website (allegedly part of a joint action between Anonymous and Lulzsec to attack and encourages attacks on any government or agency they could) and finally those which seem downright adolescent and bizarre with no discernible redeeming 'speech' or 'protest' features, for example the 'Habbo Raids' (where the Habbo Hotel environment is invaded by avatars behaving as a kind of virtual flash mob for example dancing in the form of a swastika to block access to the pools- It should be noted that the first raid may have had an anti-racist motivation but has since become something of an annual jamboree event) and the Epilepsy Forum attack (the refresh rate of a number of help sites was altered to potentially trigger seizures). [3] [4] The diversity of these actions illustrates the problems of this form of movement:

- Factionalism with extremist elements- because of the traditional hacker ethos of engaging in technological activities for enjoyment and fun in a decentralised organisation this can lead to chaotic and 'off message' activities. Almost inevitably there is also a clash between mainstream and in-group definitions of what constitutes acceptable humour. (Even if one accepts the group's contentions that

rigging various epilepsy help forums to cause seizures was not in fact one of their actions many would find their use of terms like Aids as a synonym for failure or breakdown distasteful).

- The Epilepsy Forum attack also highlights a further difficulty, which one might call the Attribution Issue. From an in-group perspective this is problematic because actions which will be damaging to the image of the group can be falsely attributed to them or, just as damaging, actions which dilute the ideological message of the group may be attributed to them. From an external regulatory perspective this difficulty of clearly attributing actions raises political difficulties in justifying the labelling of these groups as proscribed, as is a standard response to unacceptable groups.
- Despite near hysterical media reportage - for example the report which labelled Anonymous as 'hackers on steroids' (KTTV Fox 11 http://www.youtube.com/watch?v=DNO6G4ApJQY 26th July 2007)- many of the attacks rely on either brute force or phishing techniques which does not denote a high level of technological sophistication on the part of the bulk of the membership. The less sophisticated an action the more likely it is to cause damage as we shall see later this maybe significant for determining the legitimacy of an action.

The heart of the issue is of course defining the appropriate protected sphere of 'speech' and to a lesser extent the freedom to associate on the internet. This is the motivation behind many of the actions of Anonymous and protest groups of this kind and is a legitimate concern for all users. This paper shall consider whether this freedom can or should be reified as a right or whether the appropriate model from both a civil liberties and a regulatory perspective is user education and empowerment.

2.1 What is Hacktivism and how does it relate to Speech and Assembly?

Loose Definition

Hactivism is probably best described as the unification of political activism with computer hacking. It has some overlaps (or is often conflated with) online activism and cyber-terrorism. As Thomas (2001) has noted however it can be distinguished from both of these in general terms: On-line activism can be defined as non-disruptive and legal; hactivism is intended to be disruptive, though usually not damaging, and may or may not be illegal; cyberterrorism is intended to be not only disruptive, but also damaging, and is probably illegal. [5] Samuel (2004) has suggested a taxonomy of hacktivism which posits three distinct types of hacktivism. Political coding this might be best described as attempting to nullify or circumvent particular laws through technological means (for example by passing firewalls in repressive political regimes). Performative hacktivism which includes such activities as taking part virtual sit ins and web-site parodies etc., and finally the political cracking which is website defacement and redirects. Samuel views these as coming from hacker orientations with a progressively increasing willingness to engage in illegal activity. Since her work largely focuses on the participation of the hacktivist in modern politics from a socio-political perspective she can remain content with leaving the performative hacker in the centre area as author of as she puts it 'legally nebulous activities'. (Samuel A, 2004, pp. 48- 100) This present paper must take up this issue from a legal perspective and attempt to consider the performative hacker and how they are viewed s a legal subject and whether this view grants the end user the same rights to political expression in both the digital and offline worlds.

Finally, it should be noted that hacktivists have formed a unique self-identified community. Despite the diversity of their political agendas and allegiances, despite the cacophony of their messages, and the geographic distance which divides them they have managed to form a common community. The community infrastructure is easily observed they have their own websites, forums and even conferences and despite intense debate over strategies and purpose it is clear that they have formed a social movement. They certainly meet the description posited by Tarrow (1994), namely the '... collective challenge ... by people with ... solidarity in sustained with opponents and authorities'(p.3-4) The unifying factor appears to be the technology itself as both as organising tool for the community and as the identifying methodology of those who wish to be part of the group. (Samuel A, 2001) It is in this context that the Anonymous claim that 'We Are Legion' has more than mere rhetorical impact, as the 'Occupy' protests have shown this is an era where loci and methods of protest can unite individuals spread broadly across the political spectrum. Since the choice of methods is the main characteristic of the hactivist let us now look at the kinds of actions they can undertake in a general sense even above and beyond the specific examples already discussed.

2.2 The Hactivist's Toolkit

Broadly, speaking the methods used by hacktivists vary in correspondence with the taxonomy above. Political coders will engage in software development and will focus on issues with an online component (for example many of those working to circumvent the Great Firewall of China are motivated not or at least not mainly by China's political regime but by an abhorrence for any interference with the free flow of information - this is what is often called digitally correct thinking).Performative hackers are much more likely to use methods which are more closely analogous to real world civil disobedience such as parodies and sit-ins. Virtual sit-ins are a technique developed by the hacker group the electrohippies most notably used against the WTO in Seattle in 1999. During this sit-in over 452,000 people flooded the WTO's website and sent around 900 emails a day in an effort to make the site ineffective. The Electrohippies felt they 'accomplished their goal - by disrupting the World Trade Organization's online presence for four- to five-hour stretches - and [they] reduced the site's overall speed by half.' (Cassel D., 2000). The Electrohippies made sure that people knew why they were organizing the sit-in by publicizing their intentions before the event and writing a paper on their philosophy. The attempt to claim the moral if not legal high ground is clear such hacktivists view themselves as bringing street protest online. Currently the Electrohippies are designing tools that will help other hacktivists engage in the 'virtual sit-in' and to encourage hacktivisim to become more mainstream, Cassel (2000) quotes them as saying 'in cyberspace everyone can hear you scream - if you want them to.' [6]

If one examines the electrohippies' 'Occasional Paper Number One' it highlights the criteria under which these such groups might consider actions which shade into the more obviously illegal actions like a denial of service attack or at least consider them morally justified:

> 'the electrohippies collective believe that the acts or views perpetrated by the targets of a DoS action must be reprehensible to many in society at large, and not just to a small group. It is on this basis that the collective undertook the action against the WTO during their conference in Seattle, and it is also the basis upon which we are planning future actions.' [7]

Similarly, they also highlight the feeling that universally categorising these actions as terrorism is disproportionate and repressive. The key distinction that they make is one of public mandate and openness of activity (the underlying precept being that if one wishes to exercise the same rights as real world protesters then one should lay oneself open to the same risks as them). Commenting on denial of service attacks they make a distinction between their own client side distributed denial of service actions perpetrated openly by many activists and server-side denial of service actions perpetrated by only one or two activists using zombie computers. So, the difference between the two actions is one of popular legitimacy versus individual will. The structure of the client-side distributed actions developed by the electrohippies means that there must be widespread support across a country, or continent in order to make the system work:

> 'Our method has built within it the guarantee of democratic accountability. If people don't vote with their modems (rather than voting with their feet) the action would be an abject failure.Fundamentally, it's the mode of the protest on the Internet that is important when evaluating the legitimacy of the action. The power that computer technology, linked via the Internet, gives to the individual is an important factor in levelling the traditional imbalance between the individual and government or large corporations.' [8]

This commentary goes straight to the heart of the issue it may well be that very broadly supported actions which would in and of themselves be perfectly legal and harmless may become illegal due to scale. This is an issue we shall return to frequently throughout this paper.

Lastly, we come to the political crackers their protest remit extends to both on and offline issues in recent times, their tactics include website defacement, redirects, denial of service attacks sabotage and information theft. It is worth noting that the denial of service attacks and other online tactics adopted by groups in this category (for example LulzSec) rely on technical exploits rather than mass activism, though other aspects of allied groups work like the organisation of real world protests do. It is reported that LulzSec's fifty day hacking rampage in 2011 succeeded through the use of three main exploits; SQL injection-attacks (An SQL injection attack involves putting SQL instructions into a web form to make a poorly authored website perform operations on the database.), cross-site scripting (Cross site scripting is a type of computer security vulnerability typically found in Web applications that enables attackers to inject client-side script into Web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to bypass access controls.) and RFI (RFI otherwise known as remote file inclusion involves infiltrating a system with a file,

normally a shell script via a web application onto a server, the file can then be activated remotely gaining access to and potentially control of the targeted machine). RFI is particularly problematic as it may in principle at least be a serious danger to those using cloud computing. These activities are all clearly illegal if not always morally reprehensible many of these groups would claim that their actions are either mandated by public opinion or individual conscience.

In addition, some mention should be made of the concept of cyberwar that is actions such as these taken on a multinational/international level. This remains a shadowy topic. It maybe that such sustained attacks are usually the work of hackers hired specifically by their states to perform such actions. Certainly Government security expert Richard A. Clarke, in his book Cyber War (2010), defines 'cyberwarfare' as 'actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.' (p.6) Evidence of action on a scale justifying use of the term by a hacker or hactivist group is to the best of this author's knowledge not forthcoming. As Thomas (2001) notes it is interesting to see that hacktivists have chosen to be disruptive not destructive. (p.1) The key question remains given the nature and quality of the actions themselves and the motivations behind them are these diverse groups of individuals enjoying the same standard of freedom both on and off line. To analyse this further it is now necessary to consider briefly the kind of role hacktivism could have in modern political discourse.

Hacking the Body Politic

The reader should note that this section is intended only to offer a flavour of the literature both on the potential and the actual use of hacktivism in political life it is by no means intended to be treated as an extensive or exhaustive coverage of the issues, Rather it is hope that it will serve to demonstrate the legitimacy of the claims for the genuinely political nature of many of these activities.

Hacktivism in Political Theory

There are two key trends in the theoretical work on hacktivism in politics, first to consider whether it fits well with traditional definitions of civil disobedience and secondly the related idea that hacktivism represents the use of cyberspace as a form of public sphere in the Habermasian sense. In terms of the civil disobedience discourse a number of writers have considered the ethical dimension of hacktivism as an activity. (e.g. Thomas 2001 and Wray 1998). The core of the debate is a consideration of the balance between the perceived benefit as opposed to the damage caused and to some degree the popular mandate of the causes. Klang (2004) gives a clear and pragmatic resolution of this debate when he considers the elements of civil disobedience and their applicability to hacktivism his conclusion is most insightful:

> 'The criteria of disobedience and justification are easily met in online environments and do not conflict with traditional theory. The issue of non-violence is a bit more complex in the sense that the non-violence can be interpreted as zero-violence, however this is a flawed interpretation as zero-violence is an unobtainable goal. In the physical world we tolerate (to a varying degree) out lives being occasionally disrupted...These events are tolerated by society since they are deemed important to society....

The politically motivated online disobedience is actively partaking in a political discourse, the goals of this discourse...The disobedient is exercising fundamental rights of expression. Traditionally such rights are not limited without serious cause. The present legislative trend which criminalises online civil disobedience is too far reaching and seriously hampers the enjoyment of individuals civil rights.' (Klang, 2004, p.82)

The second strand of theoretical discourse around hacktivism is that of viewing it as a step along the road toward the fulfilment of (if not actually the fulfilment of) the Habermasian ideal of the deliberative democracy. That is to say they are a model of the socio-institutionally feasible means of public opinion-formation which is an integral part of a democracy. (e.g. Wiklund H, 2005) Habermas took the view that as advanced capitalist societies have developed, the core integrative function of communication has been increasingly disabled. Thus the legitimation of social institutions, indeed of nation states, is in crisis. By legitimation Habermas means citizens sense that the institutions within which they live are just, benevolent, in their best interest, and deserving of their support, loyalty, and adherence. Thus he further posited the need for institutional reform and the revival of the public sphere where citizens could deliberate and have their communications influence the state in other words a place of political conversation. In order for something function as a democratic public sphere participants should be able to take advantage of the best possible speech situations these for him were:

> **1.** *Every subject with the competence to speak and act is allowed to take part in a discourse.*
> **2a.** *Everyone is allowed to question any assertion whatever.*
> **2b.** *Everyone is allowed to introduce any assertion whatever into the discourse.*
> **2c.** *Everyone is allowed to express his attitudes, desires and needs.*
> **3.** *No speaker may be prevented, by internal or external coercion, from exercising his rights as laid down in* (1) *and* (2). (Habermas J, 1990, p.86)

The public sphere, therefore, manages to generate a political space which respects the rights of the individual and strengthens community. Because the communication which takes place in the 'ideal speech situation' is free of institutional coercion, dialogue in the public sphere can 'institute democratic discourses on the grassroots level'. [9] Though commentators looking at individual acts of hacktivism and see them as speech acts within this deliberation and indeed view hacktivist communities as deliberative democracies in their own right. (Houghton 2010), it remains a difficult theory to test in practise because of the evidentiary difficulty of analysing the discussions. Silenced or removed speakers would perforce not appear in the discussion logs or community archives. Further Dahlgren (2005) notes that the Habermasian model privileges reasoned discussion and as such ignores the irrational aspects of 'civic cultures'. However even critics do not question that the activities they are analysing have to some degree a political nature. Indeed given the weight of examples available this seems beyond doubt.

Hacktivism in Political Practice

Current contemporary reports make much of the impact of bloggers and other hacktivists upon the Arab Spring. [10]Certainly, there is a resonance for both groups with the Habermasian view that the capitalist system has lost its legitimacy by filing to communicate with the citizen. However, the hacktivism tradition in political life has a much longer profile than the recent events which have drawn it to the forefront of media and public attention. In 2004 Jordan and Taylor considered the already well formed hacktivism movements in their text, Hacktivism and Cyberwar. Their analysis consisted of detailed case-studies on hacker culture and its merging with protest. They highlight that in fact hacktivism began with sympathisers of the Zapatista movement. And goes through an evolution of stages much like that we have already outlined. The core technical seeds have always been there from the beginning however. Consider this quote from Ricardo Dominquez, a key figure in the Electronic Disturbance Theatre:

> 'In solidarity with the Zapatista movement we welcome all netsurfers with ideals of justice, freedom, solidarity and liberty within their hearts, to a virtual sit-in. On January 29, 1998 from 4:00 p.m. GMT (Greenwich Mean Time) to 5:00 p.m. (in the following five web sites, symbols of Mexican neoliberalism): [websites removed from quotation]
>
> Technical instructions: Connect with your browser to the upper mentioned web sites and push the bottom 'reload' several times for an hour (with in between an interval of few seconds).' [11]

This virtual sit-in not only brought the possibilities of direct electronic actions to the forefront of the Zapatista networks, it also initiated a more focused analysis of what methods of electronic civil disobedience might work. Several questions were brought up on the issues of net traffic, ISPs, and small international pipes. As Klang (2004) has noted these tactics were taken up and burgeoned across the sphere of political activism. He notes causes as diverse as an end to American war planes at Irish airports, anti-slavery movements, anti-poverty campaigning and even limited adoption by mainstream advocacy groups like Oxfam making use of hacktivism tactics.

This increased exposure and dissemination has lead to an evolution in causes and methodology. For example the Anonymous response to the removal of services from Wikileaks 'Operation Payback' is notable because instead of looking for computers which were susceptible to malware, users were voluntarily allowing their machines to be controlled for the purpose of implementing the DDoS attacks. By downloading a single piece of software, these volunteers became part of a botnet, which is controlled remotely to coordinate an attack. The result of this practice is hackers can now more easily gain access to large numbers of machines. Not only that, but when using a machine covertly, a hacker only has access to a fraction of the resources in order to remain undetected. By having willing partners, this new breed of hacktivists, can fully utilize the resources of each machine, making them many times more effective. Thus a smaller number of machines can do more damage and cause a larger media impact. It is worth noting here that though this was called 'Operation Payback' the damage to systems was to some extent less significant that the media reportage the

hacks received for the cause of Wikileaks. Hacktivism has a double edged relationship with media publicity however as the same coverage which makes a hack successful can also lead to more repressive governmental responses, publicity may also lead to a dilution or alteration of the meaning of the action as it becomes mediated through another medium. As Baudrillard observed: 'Transgression and subversion never get 'on the air' without being subtly negated as they are transformed into models, neutralized into signs, they are eviscerated of their meaning [...] there is no better way to reduce it than to administer it a mortal dose of publicity'. [12]

These questions are of course before the minds of current hacktivists but it is worth concluding this section with some quotations on the evolving political face of the hacktivist from Jordan and Taylor (2004):

> 'They are out there, to what future we cannot say. We can only point to the trends we have already identified. Not only has a rich and varied social movement come into existence, but this movement has shown significant potential for re-radicalising hacking and digital cultures generally. The importance of such cultures and of cyberspace in general in the twenty-first century means that hacktivists operate their politics in highly visible locations that are potentially privileged for effective action. Hacktivists represent resistance in viral times. Hacktivists are an opposition in, for and against cyberspace. Hacktivists are the first social movement of virtuality.' [13]

3. How Free is my Speech online or when is Politics not Political? : Considering the Legal Framework

As an international phenomenon naturally the specific legal standards applied to speech and association online vary from state to state. However, there is some international law on the topic. At the most fundamental level freedom of expression/association is protected by the United Nations Declaration of Human Rights (UDHR). The UDHR itself is of course is primarily aspirational . However, it is widely regarded as having acquired legal force since its adoption in 1948, as customary international law. Furthermore, it does inform the legally binding International Covenant on Civil and Political Rights (ICCPR) (the ICCPR enforcement mechanism is largely aimed at monitoring states and commenting on their adherence to the ICCPR with guidance on how to comply in future). The ICCPR in turn informs a number of regional rights declarations which are directly enforceable in national courts including the European Convention of Human Rights (ECHR). Across the board, these instruments recognize a broad right to freely express:

> ' ... not only to -'information' or -'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population. Such are the demands of that pluralism, tolerance and broadmindedness without which there is no 'democratic society'. [14]

Moreover, the former Special Rapporteur on freedom of expression, Ambeyi Ligabo, reported in his 2008 annual report to the Human Rights Council that ? 'the constant confrontation of ideas, even controversial ones, is a stepping stone to vibrant democratic society.' [15]

It is worth noting at this point, consistent with article 32 of the Vienna Convention on the interpretation of treaties, that 'the preparatory work of the treaty and the circumstances of its conclusion' (Vienna Convention on the Law of Treaties art. 32, 23 May 1969, 1155 U.N.T.S. 331) support that human rights are intended for human beings, and can only be restricted to protect rights equally held by another human being.
The *Travaux Préparatoires* affirm this proposition. Although early drafts and proposals of article 19 used varying terminology to protect persons, the drafts consistently used terms signifying rights for persons, not for collective groups or ideologies. Many early draft proposals used the term everyperson (including proposals from France (Bossuyt MJ, 1987 p.374) - The French version of the Covenant uses the words *'toute personne'*) and the United Nations Conference on Freedom of Information States specifically and consistently rejected proposals to extend the protection of article 19 to groups or ideologies. When the Committee debated what restrictions to include in article 19, it highlighted that ?the basic purpose of article 19 was to protect the right of the individual to freedom of opinion and expression and that the article should therefore contain as few restrictions as possible. (Bossuyt MJ, 1987 p.398) Many readers will be familiar with the case of *Markt Intern Verlag GmbH and Klaus Beermann v. Germany* [1989] 12 EHRR 161 and others which cover commercial speech under the ECHR as opposed to the ICCPR. This kind of case arises partially because all speech is covered by the terms of Article 10 and the courts have a duty to consider when the

state can lawfully interfere with it and partially because companies have legal personality and have in recent times tried to assert that because of this they can enjoy rights protection for rights which are practically applicable (expression, quiet enjoyment of property etc.) we shall explore this in greater depth later on.

However, since the high level international agreements have only a limited body of jurisprudence we will briefly outline the international position then focus on the cases under the ECHR which has basically the same terms as the UDHR and the ICCPR in order to give this analysis the broadest possible applicability. In other words EU law will be used as an indicator of how international law might develop and the directions it is likely to take since it has the most fully worked out jurisprudence on the matter. In a recent report specifically on freedom of expression and the internet the Special Rapporteur to the United Nations Human Rights Council stated that:

'The vast potential and benefits of the internet are rooted in its unique characteristics, such as its speed, worldwide reach and relative anonymity. At the same time, these distinctive features of the internet that enable individuals to disseminate information in 'real time' and to mobilize people has also created fear amongst Governments and the powerful. This has led to increased restrictions on the internet... In this regard, the Special Rapporteur also emphasizes that the existing international human rights standards, in particular article 19, paragraph 3, of the International Covenant on Civil and Political Rights, remain pertinent in determining the types of restrictions that are in breach of States' obligations to guarantee the right to freedom of expression.' [16] This assertion of the right to free expression over the internet is further bolstered by a recommendation that states not use and if appropriate repeal laws cutting users off from the internet on the basis of breach of intellectual property rights. [17] Naturally, in practice these cannot be absolute untrammelled rights and for the purpose of analysis we shall focus on the limitations placed on freedom of expression (which in principle is the same as those on freedom of association) under the ECHR. It should be noted that not only is the ECHR a multi-signatory convention in its own right but the wording of the limitations placed on the right is very close to that of the UDHR and so interpretations of it may be of wider applicability. The test for an appropriate limitation of the right to free expression under the Convention is one of proportionality. As Article 10 of the ECHR says:

> 'The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.'

In other words that the rights and freedoms of others and of society as a whole are weighed against the importance to the individual of the expression. Any limitation must be prescribed in law and necessary in a democratic society. Naturally this leads to a stronger degree of protection for socially useful speech which promotes the democratic ideal like political protest which will require a stronger more grave reason for its limitation. Furthermore, despite the margin of appreciation the State is not the final arbiter of that balance. As the European Court has said:

> '... the Contracting States enjoy a certain margin of appreciation in assessing the need for an interference, but this margin goes hand in hand with European supervision, whose extent will vary according to the case. Where there has been an interference with the exercise of the rights and freedoms guaranteed in paragraph 1 of Article 10, the supervision must be strict, because of the importance of the rights in question; the importance of these rights has been stressed by the Court many times. The necessity for restricting them must be convincingly established.'[18]

Thus the concept of what is protected free speech is defined and fenced round by the law of prohibited speech. Like a *Gestalt* image, the nature of the picture depends on which element of the picture the viewers' perceptions foreground. The argument of this paper is that the *Computer Misuse Act*, the Terrorism Laws and Copyright have been fore-grounded disproportionately in the legislative perspective and caused the space for lawful protest online to shrink to such an extent that human subjects protesting online enjoy much less freedom than human subjects in real life and that an alternative discourse needs to be developed to maintain human rights.

We will consider this proposition under three main headings.

1. Peaceful Persuasion and Communicating Dissent (the rationale behind rights protection)
2. Maintenance of Public Space (the space problem)

3. Human Rights Arising from Ontic Vulnerability (re-imaging the disembodied human)
4. Peaceful Persuasion and Communicating Dissent (the rationale behind rights protection)

The Preferred Position of Political Speech

Traditionally political speech has been accorded the highest level of protection of all the forms of expression due to its necessity within a democratic society. The Court has stressed repeatedly that 'freedom of political debate is at the very core of the concept of democratic society which prevails throughout the Convention'. [19] Expression at election time is of particular importance. In *Bowman v UK* (1998) 26 EHRR, a case concerning expenditure limits placed on persons other than candidates at election time, the Court said: 'Freedom of expression is one of the 'conditions' necessary to ensure the free expression of the opinion of the people in the choice of the legislature [...] For this reason, it is particularly important in the period preceding an election that opinions and information of all kinds are permitted to circulate freely.' [20] It is not just narrow, party political expression which falls within this higher echelon. The Court stated in *Thorgeir Thorgeirson v Iceland* (1992) 14 EHRR 843 that 'there is no warrant in its case law for distinguishing [...] between political discussion and discussion of other matters of public concern'. [21]

Furthermore, in *VgT Verein Gegen Tierfabriken v Switzerland* (2002) 34 EHRR 4 the court considered a Swiss law against political advertising and as a result a film promoting vegetarianism was not broadcast. The Court in considering the legality of this made the point that the Swiss authorities did have a certain margin of appreciation on the question of whether there was a pressing social need to restrict the broadcast of an advertisement. Indeed the margin was 'particularly essential in commercial matters, especially in an area as complex and fluctuating as advertising'. [22] But the expression here was not regular commercial advertising in the sense that it was intended to persuade the public to buy a particular product. Rather it 'reflected controversial opinions pertaining to modern society in general'. Indeed the very reason the advert was banned by the Swiss authorities was because it was regarded as 'political' (para 70). Because of this the State's margin of appreciation must necessarily be reduced, for what was at stake was 'not a given individual's purely commercial interests, but his participation in a debate affecting the general interest' (para 71). Given that the reasons for the ban were that it was intended to prevent wealthy commercial groups from skewing the political process, and given that the organisation here was evidently not such a group, those reasons cannot have been 'relevant and sufficient' to justify this particular restriction (para 75). Further, there was no prohibition of political advertising in the print media. This disparity may have been due to the more intrusive nature of the broadcast media but the Court said that it must mean that the prohibition cannot have been of a 'particularly pressing nature' (para 74). Thus the ban constituted a breach of VgT's Article 10 rights.

Thus we have a situation where political speech is strongly protected as is speech with an element of public interest. However it should be noted that the Court will examine whether a public interest concern exists so for example where speech about a public figure is about aspects of their private lives unrelated to public duties, less protection will exist. [23] In contrast speech was found to be related to the general interest was found in *Fressoz and Roire v France* 5 BHRC 654 where it concerned the salaries of the head of Peugeot in the context of widespread industrial unrest relating to Peugeot's worker's wages. It would be fair to say in summation therefore that the Courts will be generous in the protection of political/public interest speech but retain for themselves the gate-keeping role of what can properly constitute such speech. This gate-keeping role also extends to consider when the rights and freedoms of others require political speech to be limited. In other words how to interpret the second limitation portion of the various rights protections.

Recognised Limitations of Political Speech

Although the bulk of this section will focus on the limitations which are applied specifically to political speech and protest we shall also briefly consider at this point a limitation on speech rights generally which could have a disproportionately deleterious effect on hacktivism; that is limitations imposed by copyright. Nimmer gives a bleak but broadly accurate view of the initial response from many copyright lawyers to the question of how does this affect human rights when he says that there can be no clash because the infringer in taking the expression of others 'is not engaging in *self* - expression in any meaningful sense'. [24] Similarly, Jeremy Waldon (1993 p.856-62) has characterised the standard perception of the copyright - free speech conflict as being one in which copyright is viewed as a strong and valuable property right as opposed to a weak free speech argument which emphasize the social interest in communication of information to the public (a weak argument since copyright is not over the information *per se*).

This is not to say however that there has been some amelioration of copyright in favour of free speech even in jurisdiction like the UK which has a long and strong copyright tradition. In *Ashdown v Telegraph Group Ltd* [2002] Ch 149 Lord Philips MR noted that 'Copyright is antithetical to freedom of expression. It prevents all, save the owner of the copyright, from expressing information in the form of the literary work protected by the copyright.' [25] He then went on to find however that freedom of expression does not extend to the freedom to convey information in the form of words used by someone else, though he conceded that in certain circumstances there might be an over-riding public interest in knowing the very words used by a person not withstanding their copyright over them. This judgement however does not consider the situation of satirists and social critics who have a legitimate reason to use the words of others. This seems to be a problem of framing as the debate about copyright and expression is largely being carried out among human rights rather than copyright scholars. There is a growing sense that copyright should not be a shield from political criticism but as yet the debate has not reached a definitive conclusion or been reflected in case law. [26]Furthermore, none of this takes account of the chilling effect that even a small potential for copyright claims could have upon ISPs willingness to host such material (the legal situation for ISPs is complex and although there are legally approved mechanisms in place to prevent them becoming liable for content posted by their users the more risk averse may wish to avoid the issue altogether by not hosting such sites).

We shall now move to consider the limitations placed on political speech in the real world. It is at this point that speech and assembly (Articles 10 and 11 of the ECHR) begin to coalesce as we consider protests. The underlying rationale of Articles 10 and 11 of the ECHR is to allow free expression and in particular free expression of a political or other socially useful nature. Article 11 bolsters the rights in Article 10 by permitting people to gather together and, provided they comply with the relevant legal rules, to locate themselves at a location most appropriate to the subject of their protest (for example animal rights protesters outside a University research lab). As the European Court of Human Rights hereafter ECtHR has put it:

> 'The Court also emphasises that one of the aims of freedom of assembly is to secure a forum for public debate and the open expression of protest. The protection of the expression of personal opinions, secured by Article 10, is one of the objectives of the freedom of peaceful assembly enshrined in Article 11. [27] The limitations that can be placed on the exercise of Articles 10 and 11 (and also the ICCPR) are only those which are necessary in a democratic state and prescribed by law. Although the terms of limitation differ in their specifics the underlying rational is the protection of overarching public interests: for example, national security or the competing rights of others. It is notable that in terms of assembling to protest the ECtHR has recognised that some degree of nuisance is acceptable, stating that '... freedom of assembly as enshrined in Article 11 of the Convention protects a demonstration that may annoy or give offence to persons opposed to the ideas or claims that it is seeking to promote'.[28]

Thus we have a real world limitation system focused on potential for harm and interference with the right of others but recognising that the social value of free speech is worth inconvenience and even offence. The same may not be true for those who take the apparently rationale step of wishing to protest in cyberspace where *de facto* no physical harm to others can occur.

Protest in Cyberspace

In relation to those who wish to protest in cyberspace the protection of these rights does not seem to be conducted with the same rigour. This seems incongruous given that the prime reason for restraining free speech in the real world is the potential for violent disorder which cannot occur in cyberspace. [29] The intersection of financial interests and concerns over internet security seem to have allowed the balance to be drawn in a disproportionate fashion in relation to cyber protest. So for example any action that could have the same effect as a deliberate denial of service attack (like multiple users organising an email protest) if done for an ideological reason could be construed as an act of terrorism as it seriously interferes with or endangers the security of an electronic system. [30] This potential lack of proportionality is legally very troubling as the function of the Convention and the Court which upholds it can be described thus.

In carrying out its scrutiny of the impugned interference, the Court has to ascertain whether the respondent State exercised its discretion reasonably, carefully and in good faith. It must look at the interference complained of in the light of the case as a whole and determine whether it was:

> '... proportionate to the legitimate aim pursued' and whether the reasons adduced by the national authorities to justify itself are 'relevant and sufficient'. In doing so the Court must satisfy itself that the national authorities applied standards which are in conformity with the principles embodied....and moreover, that they based their decisions on an acceptable assessment of the relevant facts.' [31]

The difficulty seems to be drawing the line between protest in cyberspace and the prohibited activity of taking direct action (causing some form of harm or damage). The jurisprudence of the ECtHR makes it clear that once the protest moves from peaceful communication (albeit of an inconvenient or annoying nature) to any form of destructive or disruptive action then the rights protections are greatly diminished if not lost. [32]

If we continue with our terrorism example, the difficulty becomes clear. The legislation requires that to cross over into the forbidden ground of harmful action, which it would be lawful for the state to interfere with; that the action is designed to have a seriously impairing effect on an electronic system. However the meaning of 'designed' is unclear. [33] Does it require that a specific result is planned or simply that the actions planned lead to that particular result regardless of the protesters' intention? In relation to cyberspace is this sufficient protection of the right to protest given that successful mass communication could have this damaging effect? In other words protesters with a ground swell of public support would have to actively plan not to cause such an interference accidentally? There is the further issue of using social networking websites to plan such activities which raises the potential for mass involvement in inchoate offences under the Act. Terrorism is the most serious example hence why we have unpicked it in detail in this paper but of course there are also the strictures of computer misuse legislation and copyright which has been used to limit free speech in cyberspace. There is also in the background the worrying question of whether under the current ECtHR jurisprudence mass protest online would *de facto* be considered direct action precisely because of its potential to damage electronic systems regardless of the protesters intent. This issue has been further complicated by the statement of the special Rapporteur who whilst decrying state led deliberate denial of service attacks against rights groups also added that:

> '... it should be noted that States have an obligation to protect individuals against interference by third parties that undermines the enjoyment of the right to freedom of opinion and expression. This positive obligation to protect entails that States must take appropriate and effective measures to investigate actions taken by third parties, hold the persons responsible to account, and adopt measures to prevent such recurrence in the future.' [34]

Whilst this clearly covers individuals and not, for example, companies the 'duty' of States to minimise interference could be a double-edged sword opening the door to repression largely because of the slight weight given in judicial process to the interests to parties whose interest exists solely in cyberspace (see the comments on speech v. copyright above). This problem of rights minimisation arises because of the other two issues we shall be discussing in this paper, the lack of protected public space in cyberspace to act as a legitimate forum for protest and a misunderstanding of the nature of the human subject in cyberspace.

4. Maintenance of public space (the space problem)

The idea that cyberspace has no space for free discussion or space analogous to being in public in real life might on first blush seem absurd to the casual observer given the wide variety of speech activities which take place there and the multi-jurisdictional nature of the space. However, all the spaces are privately owned as a result of the infrastructure needed to support them. So for example to perform the equivalent of a peaceful picket outside a premises in cyberspace would require either the compliance of the subject of the protest to transmit your views, or a site dedicated to the protest (which lacks the communicative potential of a real world picket due to lack of proximity), or mass action like email complaints which could damage the system and fall foul of the law.

The situation is not the same for the real world protester as although courts are unlikely to overturn interests in real property in favour of the right to protest they are cognizant of the need to preserve a space for protest. Let us consider the case of *Appleby v UK*(2003) 37 EHRR 38 for example. This case concerns a right of access to private land (a town centre complex) to gather petition signatures against development in the area. The ECtHR was not persuaded on the facts that despite the changing face of human interactions effective protest required the automatic creation of rights of entry to private property, or even necessarily to all publicly-owned property. [35] *Appleby* however, has been stiffly criticised not only does this approach underplay the importance of location in that the site may be 'uniquely positioned', have a 'close connection' or 'symbolic importance'(Rowbottom J, 2005, p.189). In addition to this many commentators argue that the reasoning of the Chamber was fundamentally flawed in two ways. Firstly, it implicitly viewed property and expression as equal rights without considering the role of expression in a democratic society or the unusual situation applying to the land in question. This element is important for this discussion which would view the town centre complex in *Appleby* as being strongly analogous to the privately owned yet public spaces of the

Internet. Secondly, it ignored the importance of collective societal interests when making the balance. As Mead put it:

> 'The Chamber has unwittingly created [a logical impasse] by adhering to the straitjacket of public/private sphere. By espousing the absolute right of an owner to exclude, the Chamber has denied the need for a reasonableness test. However, only with a concept of reasonableness can there be any 'balancing' exercise at all. But, it is this balancing requirement that lies at the heart of the positive obligations concept in Article 10 and 11 and, indeed, at the heart of the exercise under Article 10 (2) for direct breaches by the State.' [36]

Finally, and perhaps most importantly for the current argument the decision in *Appleby* placed a great degree of weight on the fact that exclusion from the complex did not extinguish their right to effective protest the essence of the right remained intact as they could still launch door to door petitions etc. This is not necessarily the same with cyberspace where the word for door to door petition is spam. There was also the complicating factor of the land moving from government to private control in this case and the Chamber was reluctant to impose obligations about access on either the selling State or the private buyer much was made of the expense and difficulty of this and once again the deciding factor was that this was inappropriate as alternative modes of protest were available. The situation is far less clear cut in cyberspace particularly when one considers the factors already outlined above.

Furthermore, the alternatives available online are even more detrimental because of the amount of power they give to the party being protested against. The protester is forced to make either a distant protest at some different site or one which is limited in size and scale. It is interesting to consider whether there is any duty on the subject of the protest to supply resources that would allow them to receive a reasonable level of incoming traffic sufficient to get across the import and size of the protest or whether they could effectively make all protests potentially damaging to their system by having limited technological means. (It seems that economic considerations like the need to be perceived as secure and accessible by users is the only controlling factor here). Similarly, even if another site can be persuaded to house the protest how do protesters attract the attention of the public or even the party complained off? The obvious answer is to use the name in the site URL or otherwise prominently in the page. However, this may mean that the site hosts may go in fear of the laws of defamation and intellectual property. The La Rue report has highlighted this issue in so far as he has called for defamation to be decriminalized globally. However, a civil wrong could have an equal chilling effect. Those who host protests in the real world need have no fear of the law of defamation is it appropriate in all cases that defamation should effect those who host protest in cyberspace? Even though fair comment is a recognised defence the potential for legal action could have a marked chilling effect on freedom of speech.

The quashing of speech via the use of intellectual property is even greater. For example use of the name of the complained about company could be argued to be a breach of trademark, this question will hinge on the finding of an ICANN UDRP panel as to whether or not the protest has a legitimate interest in using the name in a URL. The UDRP does allow for a legitimate interest where '... you are making a legitimate non-commercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue. ' (Para 4Ciii UDRP) However, because the over-arching goal of the UDRP is to avoid confusion among users, panels have come to complex and confusing decisions which seem to require both the content of the page and the domain name to communicate the message. [37] Even if the panels adopt generous interpretations of legitimate interest is it appropriate that such a body be the arbiter of important civil rights? Furthermore, there is also the potential for bringing a normal civil case for breach of intellectual property rights with the threat of large damages as well. Although the law in this area does have fair use exceptions this potential is having a chilling effect. [38] The question then becomes why has rights protection in this area been so weak? The contention of this paper is that the problem lies with how rights are conceived.

5. Human Rights arising from Ontic Vulnerability (re-imaging the disembodied human)

Traditionally, the barrier to rights in cyberspace has always been the multi-jurisdictional nature of that sphere. The rationale being that although in theory rights arise because of the shared human condition but in practice are enforced in the state where the person lives. However, as regimes of international human rights law grow and develop the difficulty seems far more deep seated than that. It would seem that users as legal subjects

in cyberspace are perceived as lacking the appropriate quality of 'humanity' to attract such rights and only regain them once the action moves outside the online sphere. As rights theorists would put it is the embodied being whose ontic vulnerability that makes rights such a necessity. As we noted earlier under the ECtHR (and some other domestic rights regimes) have chosen to extend certain human rights protections to legal persons as well as actual persons. The conceptual justification behind this is two-fold.

The first concept is that of identification or lifting the corporate veil. Identification means that the rights of the legal person and those of the stakeholders are approached as being the same. An act or omission by the State then thus causes a human rights violation that regards the organization and the individual jointly. The 'corporate veil' - is then thus lifted this is only permitted in exceptional circumstances. The ECtHR considers this approach particularly appropriate 'where it is clearly established that it is impossible for the company to apply to the Convention institutions through the organs set up under its articles of incorporation or - in the event of liquidation - through its liquidators. [39] Although the European Court suggests that identification may also be practicable in other situations, the jurisprudence in this area is still poorly developed. It therefore seems that, other than in this situation, the interests of a legal person cannot be protected through its stakeholders by lifting the corporate veil, nor will natural persons be able to protect their human rights in that way.

The second concept recognizes that an action or omission by the state against a legal person may also constitute a human rights violation in its own right against interested natural parties. In this approach, then, the infringement against the corporation and the violation against the individual are formally separate instead of being seen as one. The individual then claims and obtains protection of rights of his or her own rather than of the legal person, but the juridical entity might benefit indirectly from that. The ECtHR has laid out some considerations to take into account to determine for when this might happen:

- When the natural person is the sole owner or shareholder of the company, or in effect is carrying out his or her business through the company. [40]
- The infringement against the company also personally affected the individual [41]
- Acts or omissions in criminal investigations or proceedings that cause an infringement of the rights of the legal person might, under these conditions, thus also constitute a distinguishable violation on its own against the natural person to whom the organization belongs. Meanwhile, employees, executive directors and majority shareholders as a rule cannot claim to be a victim of infringements of any rights of the legal person.[42] Exceptions are conceivable, however. In case the legal person is a media organization and its right to freedom of expression (Article 10 ECHR) is violated because of criminal broadcasting or publishing restrictions, not only the sole shareholder but also employee journalists who are directly affected may themselves enjoy the protection of the European Convention. [43]

The European Convention also offers human rights protection to individual minority shareholders when measures against the company have a direct bearing on the rights inherent in owning stocks or shares. [44] These exceptions are very much based upon maximising the rights of the corporeal individual furthermore they are an exception based upon the interplay between legal and actual persons and as such serve to underscore the unusually and inappropriately low level of protection afforded to cyber- protesters. Corporations have managed to reverse to some degree the incorporation process to re-emphasise the rights of the individuals within them this concession is not without its critics as we shall see particularly in the current economic climate but it is something of an exception which proves the rue of rights vested in embodied persons regardless of how they choose to manifest themselves. Let us now move to the consideration of ontological vulnerability as a basis for human rights which is the key focus of this section.

In the broader philosophical of embodiment and the understanding of pain embedded in human rights has a long history. [45] We shall focus on specifically law based theory. This is intended to be an illustration rather than an exhaustive discussion. Turner (2006) has considered in detail the development and history of human rights how it links with citizenship and institution formation. He makes a compelling case for the pervasiveness and necessity of the vulnerability theory in human rights discourse.

> 'Human beings experience pain and humiliation because they are vulnerable. While humans may not share a common culture, they are bound together by the risks and perturbations that arise from their vulnerability. Because we have a common ontological condition as vulnerable, intelligent beings, human happiness is diverse, but misery is common and uniform. This need for ontological security provides a strong moral argument against cultural relativism and offers an endorsement of rights claims for protection from suffering and indignity.

> While liberal theory is largely about the political dimension of human rights, ontological insecurity indicates a cluster of salient social and economic rights...that are fundamentally connected with human embodiment.' [46]

Fineman (2008) proposes a similar relationship between the ontological vulnerability of the embodied person and societal or institutional vulnerability that the two supplement and amplify each other.

> 'One promising theoretical potential of making vulnerability central in an analysis of equality is that attention to the situation of the vulnerable individual allows us to redirect out focus onto the societal institutions that are created in response to individual vulnerability. This institutional focus has the effect of supplementing attention to the individual subject by placing him/her in social context.' [47]

Anna Greer concerned that the institutional emphasis in rights law and theory has allowed rights discourse to go astray, ultimately leading to such anomalies as the granting of right to companies (as we discussed above) has tried to re-orient and correct the deviation by asserting that embodiment is a common thread in human rights discourse. Not only does vulnerability inform along with other sociological factors the formation of institutions but actually it is appropriate to view these institutions as formalised responses to specific instances of human vulnerability that are common and well known. For Greer (2010) the UDHR is a passionate defence of the vulnerable human.

International human rights law, on this reading, should be conceptualised as a juridical instantiations of our shared duty to respond to the fundamental incidents of a human ontic commonality. This characterisation sits well with Hunt's analysis of the origins of rights in the eighteenth century, as well as the arguments offered here for the relationship between embodied vulnerability and the UDHR paradigm. It is also the case that contemporary human rights awareness, based on evidence that public opinion is indeed mobilised by a sense of moral proximity to distant others all over the globe, reflects the role of embodied vulnerability and a related empathy. [48] The intention with this kind of theory is to highlight the difference between the rights bearer as legal subject and the rights bearer as embodied human person. This mode of thinking is designed to protect human rights law from encroachment by entities such as corporations who are legal subjects (and thus technically capable of bearing rights) but not embodied human persons. Thus conversely under these theories the computer user who is often viewed as being a disembodied entity once they enter cyberspace has a difficulty engaging rights that are framed in terms of the embodied world. This position might be crudely summarised as asking what harm can come to you in cyberspace and responding that since there is no physical/actual harm no rights can apply. [49]

The present author whole heartedly agrees with the use of ontic vulnerability as the basis of rights in the real world, and the paramount importance of viewing the rights bearer in the context of a living human being. However, it is important to add that the existential or ontic vulnerability of users in cyberspace has been greatly down-played. How many times have protesters been silenced by rendering them non-existent in the virtual sphere through governmental use of firewalls or by simply shutting down the net infrastructure in a region by using the law or political power to influence ISPS (as Egypt reportedly did during recent unrest). Tie this vulnerability in with the difficulties described above and the net user begins to look like a very vulnerable and unprotected being. It has long been recognised that government and corporate action could threaten the Internet's continuance as a viable environment (for example the current debate on net neutrality) but theorists need to extend this further and recognise that the online identities of users are also threatened and that if those users are to be rights bearing individuals in any real sense in the modern world then some of those rights need to follow them into the virtual sphere.

It is also perhaps worth noting here as a side point that part of the difficulty may be that ironically enough online protesters often fail to win the narrative war, their stories in and off themselves may not attract the 'empathy' that Greer speaks of. Heightened fears about cyber war and fear for personal property may be alienating cyber protesters from their natural defenders. Certainly, in his work on indigenous people one of the key factors Niezen (2010) noted in invigorating rights was creating a narrative of vulnerability or more accurately a body of knowledge of that suffering and the identity of the sufferers that could be widely understood:

> 'Publics are the abstract, invisible, intended audiences of outreach engaged in by those with very tangible grievances. And the ideas held but publics do matter, not just because of their possible influence on those who hold power, but because of the possibility that the publics themselves might be influenced by the claimants of rights. This in itself encourages the repositioning of local knowledge and identities toward their public consumers, bringing about largely unexamined dynamics to the recovery and representation of our collective selves.' [50]

Cyberactivists have lost out to the greater preparedness of the politico-corporate world which is growing in their capacity to deal with such attacks whilst still being able to 'enjoy' the moral high ground.

> 'Whether the target of activism is the actors of corporate globalization or oppressive governments, the tendencies we see are very similar. On the one hand the Internet is more and more integrated into resistance, sub-state actors are increasingly taking on state level agendas.' [51]

This largely comes about because website defacement/crashing is public facing and therefore attention grabbing. However it would rarely impact upon core secure systems which attracts the unclear and emotive label of cyberwar. [52] The recent rise and sudden disbanding is a good example of this in that as soon as it became evident that the group was getting serious negative attention from both the police and rival hackers it disbanded. The troubling aspect from a regulatory perspective is of course that it is unclear whether it was law enforcement or other hackers who caused the group to abandon their self styled 'voyage'.

The disbanding of LulzSec might seem like an important victory for the forces of law and order - after all, this is the group credited with attacks on everything from Sony to the CIA. But in this shadowy world of claims, boasts and posturing, nothing is quite what it seems. It may have been other members of the hacker 'community' - disgruntled with the antics of LulzSec - who forced the group into retreat. A document posted online in the last 24 hours purports to be a history of LulzSec, complete with full details on its leaders. It stated:

> 'We've been tracking and infiltrating these kids,' says the document, and its account goes on to name people in the UK, Amsterdam and New York, along with their social networking profiles and other details....But even if LulzSec has gone offline, its members and other hackers trying to make a name for themselves may soon pop up elsewhere. And the other question is whether we should take any publicity-hungry group like this too seriously. The real damage is more likely being done by criminal groups who wouldn't dream of boasting of their exploits on Twitter or anywhere else. [53]

Cyberprotesters then have difficulty in meeting both the legal and sociological paradigm of parties worthy of rights protection because of the disembodied nature of their activities and the unsympathetic image in the public mind of cyberprotest.

6. Conclusions and Recommendations

How then to combat the limitations to free speech online? It would seem that the current rights regime cannot do it unless the notion of how and when the human is the subject of rights is radically rethought or perhaps more accurately the nature of online person-hood is reconsidered. The ontological vulnerability of the user online needs to be foregrounded and emphasised as does the increasingly corporate nature of the Internet. Judicial guidelines need to redefine the boundary between speech and direct action for the digital age old ideas based on trespass and physical harm are not suited to the Internet for the reasons we have discussed namely the lack of public space and a tendency to minimise protest rights.

In the meantime government or NGO action can have positive effects. The La Rue report (A/HRC/17/27) has emphasised that ISPs should adopt terms of use which promote human rights. This kind of requirement could be used to invigorate the Internet as a zone of expression.

> '46. The Special Rapporteur notes that multi-stakeholder initiatives are essential to deal effectively with issues related to the Internet, and the Global Network Initiative serves as a helpful example to encourage good practice by corporations. Although only three corporations, namely Google, Microsoft, and Yahoo!, have participated in this initiative so far, the Special Rapporteur welcomes their commitment to undertake a human rights impact assessment of their decisions, including before entering a foreign market, and to ensure transparency and accountability when confronted with situations that may undermine the rights to freedom of expression and privacy...
>
> 48. More generally, the Special Rapporteur encourages corporations to establish clear and unambiguous terms of service in line with international human rights norms and principles, increase transparency of and accountability for their activities, and continuously review the impact of their services and technologies on the right to freedom of expression of their users, as well as on the potential pitfalls involved when they are misused. ' [54]

Users can be educated to enhance their understanding of the right to free speech afforded to them and how to use it in a legally acceptable manner. Spaces can also be created where users can set the agenda for protest and information dissemination, for this to be functional and draw impetus away from other forms of protest these would need to be truly open spaces where all forms of protest speech which could fall within the scope of political expression even if they are against the current government or could if untrue be construed as defamation (one of the reasons ISPs are cautious about hosting protest cites is the fear of defamation actions the Rapporteur has already commented on the importance of not using ISPS as censorship tools or holding them for failing to prevent illegal content.)Until something is done however, it does seem somewhat anomalous that a sphere of human activity created entirely by speech acts, has a greatly impaired protection for free speech.

Bibliography

Birnhack M, (2003) 'Acknowledging the Conflict between Copyright Law and Freedom of Expression under the Human Righs Act', *Entertainment Law Review* 24

Bossuyt MJ, (1987) Guide to the Travaux Préparatoires of the International Covenant on Civil and Political Rights (Dordrecht: M. Nijhoff)

Cassel D, (2000) Hactivisim in the Cyberstreets http://www.alternet.org/story/9223 (accessed 16/1/12)

[Originally published as 'Hactivism! Taking It Off the Streets, Protestors Are Acting Up Online' The San Francisco Bay Guardian Vol. 34 No. 28 (Apr 12-18 2000)]

Cellan Jones R, (2011) LulzSec hacking group announces end to cyber attacks BBC News Reort http://www.bbc.co.uk/news/uk-13918458 (accessed 16/1/12)

Clarke RA, and Knake R, (2010) Cyber War: The Next Threat to National Security and What to Do About It (London: HaperCollins)

Dahlgren P, (2005) 'The Internet, public spheres and political communication: dispersion and deliberation' Political Communication Vol.22 147 http://www.cblt.soton.ac.uk/multimedia/PDFs/Internet,%20public%20spheres,%20political%20communication.pdf

Dominguez R, (unknown) 'Digital Zapatismo' http://www.thing.net/~rdom/ecd/DigZap.html (accessed 16/1/12)

'Electrohippies' (2000) Occasional Paper 1: Client-side Distributed Denial-of-Service: Valid campaign tactic or terrorist act? http://www.fraw.org.uk/projects/electrohippies/archive/op-01.html (accessed 16/1/12)

Fineman M, (2008)'The Vulnerable Subject: Anchoring Equality in the Human Condition' Yale Journal of Law and Feminism 20(1)1

Greer A, (2010) Redirecting Human Rights: Facing the Challenge of Corporate Legal Humanity (Basingstoke, Hampshire/New York: Palgrave Macmillan)

Griffiths J (1999), 'Copyright Law and Censorship - The Impact of the Human Rights Act 1998', in Barendt E and Firth A, (eds) Yearbook of Copyright and Media Law Vol. IV (Oxford: Oxford University Press)

Griffiths J and Suthersanen U (eds.) (2005) Copyright and Free Speech (Oxford: Oxford University Press)

Habermas J, (1990) Moral Consciousness and Communicative Action. Lenhardt C and Nicholsen SW (trans.) (Cambridge: MIT Press)

Houghton T, http://nottingham-my.academia.edu/TessaHoughton/Talks/24890/The_Peoples_Republic_of_Hacktivism_A_public_sphere_theoretical_interpretation_of_online_independence_movements_and_the_Peoples_Republic_of_China 2010)

Hugenholtz B (2002) 'Copyright and Freedom of Expression in Europe' in N Elkin-Koren and N.W. Netanel (eds.) The Commodification of Information (Hague: Kluwer Law International)

Hunt L., (2007) Inventing Human Rights (New York/London: W.W. Norton & Company)

Ingram D, (1990) Critical Theory and Philosophy (New York: Paragon House)

Jordan T, and Taylor P, (2004) Hacktivism and Cyberwars: Rebels with a Cause? (London: Routledge)

Klang M, (2004) 'Civil Disobedience Online' Information, Communication and Ethics in Society Vol.2 75

Ligabo A, (2008) 'Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, U.N. Doc. A/HRC/7/14

Macmillan Patfield F, (1996) 'Towards a Reconciliation of Free Speech and Copyright',in Barendt E. *Yearbook of Copyright and Media Law 2* (Oxford: Oxford University Press)

Mead D, (2004) 'Strasbourg Succumbs to the Temptation 'To Make a God of the Right of Property': Peaceful Protest on Private Land and the Ramifications of Appleby v UK' Journal of Civil Liberties 98

Niezen R (2010) Public Justice and the Anthropology of Law (Cambridge: Cambridge University Press)

Nimmer M, (1970) 'Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press?' UCLA Law Review Vol.17 1180

Pinto T, (2001) 'The Influence of the ECHR on Intellectual Property Rights`, *European Intellectual Property Review* 209

Raymond ES (2000) The Revenge of the Hackers http://www.catb.org/~esr/faqs/hacker-revenge.html (accessed 16/1/12)

Raymond ES (2001) How to become a Hacker http://www.catb.org/~esr/faqs/hacker-howto.html (accessed 16/1/12)

Raymond ES (2002) A Brief History of Hackerdom http://www.catb.org/~esr/writings/cathedral-bazaar/hacker-history/index.html (accessed 16/1/12)

Rowbottom J, (2005) 'Property and Participation: a right of access for expressive activities' European Human Rights Law Review 186

Samuel A, (2001) 'Digital Disobedience: Hactivism in Political Context,' Annual Meeting of the American Political Science Association: The Internet as Agent of Change: Bridging Barriers to Cultural, Political and Activist Discourse, Aug-Sep 2001http://202.41.82.144/data/HACKING_INFORMATION/digitaldisobedience-hactivism.pdf (accessed 16/1/12)

Samuel A,(2004) Hacktivism and the Future of Political Participation (Ph.D. in Political Science: Harvard University) http://alexandrasamuel.com/dissertation/ (accessed 16/1/12)

Tarrow S, (1994) Power in Movement: Social Movements, Collective Action and Mass Politics in the Modern State (Cambridge: Cambridge University Press)

Thomas JLC, (2001) 'Ethics of Hactivism' Sans Institute http://www.aribo.eu/wp-content/uploads/2010/12/Thomas_2001-copy.pdf (accessed 16/1/12)

Torremans PLC (ed.), (2004). Copyright and Human Rights (Hague: Kluwer Law International)

Turner B. (2006) Vulnerability and Human Rights (University Park PA: Pennsylvania State University Press)

Vegh S. (2003) 'Classifying Forms of Online Activism: The Case of Cyberprotests against the World Bank' McCaughey M. and Ayres M.D.(eds.) Cyberactivism: Online Activism in Theory and Practice (London: Routledge)

Waldron J (1993) 'From Author to Copiers: Individual Rights and Social Values in Intellectual Property' Chicago-Kent Law Review Vol.68 840

Wall I (2008) 'On Pain and the Sense of Human Rights' Australian Feminist Law Journal Vol. 29 53

Wiklund H, (2005) 'A Habermasian Analysis of the Deliberative Democratic Potential of ICT-enabled services in Swedish Municiplaties' New Media & Society October Vol.7 701

Wray S, (1998) 'Electronic Civil Disobedience and the World Wide Web of Hacktivism:A Mapping of Extraparliamentarian Direct Action Net Politics' SWITCH 4.2 http://switch.sjsu.edu/web/v4n2/stefan/ [1999 Peace Review 11: 107-112]

A/HRC/17/27 (2011) Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

[1] Martina Gillen is a Senior Lecturer at Oxford Brookes University. Martina Gillen's current research focuses on Intellectual Property and IT Law and builds on a Ph.D that focused on ideas of community/customary law being developed into practical means of regulating online environments. She is particularly interested in Computer Misuse and the impact of Intellectual Property on software use and development. Martina also has a keen interest in jurisprudence and legal anthropology particularly legal evolution and the law of tribal peoples. Current research topics include regulation of non-commercial copyright infringement and intellectual property in the folkways of indigenous cultures.

[2] An overview of the early hacker movement Raymond, E.S. (2002), 'A Brief History of Hackerdom' http://www.catb.org/~esr/writings/cathedral-bazaar/hacker-history/ar01s07.html The later hacker movement up to the present growth of the Free Libre and Open Source movement can be found at Raymond, E.S. (2000), 'The Revenge of the Hackers' http://www.catb.org/~esr/faqs/hacker-revenge.html The ethical hacker ethos is also fully explored at Raymond, E.S., 'How to be a Hacker' (2001)http://www.catb.org/~esr/faqs/hacker-howto.html

[3] KnowYourMeme http://knowyourmeme.com/memes/events/project-chanology 2011a

[4] KnowYourMeme http://knowyourmeme.com/memes/pools-closed 2011b

[5] p.1 http://www.aribo.eu/wp-content/uploads/2010/12/Thomas_2001-copy.pdf

[6] Cassel D, (2000) Hactivisim in the Cyberstreets http://www.alternet.org/story/9223 (accessed 16/1/12)

[7] Electrohippies, http://www.fraw.org.uk/projects/electrohippies/archive/op-01.html 2000)(emphasis in original)

[8] SElectrohippies, http://www.fraw.org.uk/projects/electrohippies/archive/op-01.html 2000) (emphasis in original)

[9] Ingram D, 1990, p.155

[10] e.g. herehttp://ijnet.org/blog/what-arab-spring-taught-journalists-2011and here(http://www.washingtonpost.com/lifestyle/style/the-hacktivists-of-telecomix-lend-a-hand-to-the-arab-spring/2011/12/05/gIQAAosraO_story.html) as well as within the Occupy movement (See e.g.Here http://pulsedowntown.wordpress.com/2011/10/29/occupy-%E2%80%9Chacktivists%E2%80%9D-use-skills-to-educate-agitate-organize/ and here http://hastac.org/blogs/michacardenas/2011/11/29/calling-all-hacktivists-occupydata-hack-thon-dec-9-11-2011-occupyla-o)

[11] Dominquez http://www.thing.net/~rdom/ecd/DigZap.html

[12] Baudrillard, 1981: p.173-4

[13] Jordan and Taylor (p.172)

[14] *Handyside v. United Kingdom* no. 5493/72, § 49, ECHR 1972

[15] A/HRC/7/14 <http://daccessods.un.org/access.nsf/Get?Open&DS=A/HRC/7/14&Lang=E para.66

[16] A/HRC/17/27http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf para. 23

[17] A/HRC/17/27 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf para. 49 and 50

[18] *Autronic AG v Switzerland* , judgment of 22 May 1990, Series A No. 178, para. 61

[19] *Lingens v Austria* (1986) 8 EHRR 103 para 42

[20] *Bowman v UK* (1998) 26 EHRR 1 para 42

[21] *Thorgeir Thorgeirson v Iceland* (1992) 14 EHRR 843 para 64

[22] *VgT Verein Gegen Tierfabriken v Switzerland (2002) 34 EHRR 4*

[23] see *Tammer v Estonia* (2001) 10 BHRC 543

[24] Nimmer M, 1970 p.1192

[25] *Ashdown v Telegraph Group Ltd* [2002] Ch 149 (para 30)

[26] For a flavour of this debate see: B. Hugenholtz 2002; J. Griffiths and U. Suthersanen 2005; F. Macmillan Patfield 1996; J, Griffiths 1999; T. Pinto 2001; M. Birnhack 2003; P.L.C Torremans 2004.

[27] see *Ezelin v. France*, 26 April 1991, § 37, Series A no. 202; *Éva Molnar v. Hungary* (Application no. 10346/05) at paragraph 43

[28] *Stankov v Bulgaria* (App 29221/95 and 29225/95) EctHR judgment 2 October 2001 at [86]

[29] See *Ezelin v France* (Application n. 11800/85) and *Ziliberberg v Moldova* (Application no. 61821/00) for examples of the courts position on traditional formal protests

[30] See the *UK Terrorism Act 2000* et al. The legislation also requires that the action be intended to influence the government, a government organisation, the public or a section of the public. Since this is de facto the motivation behind protest it was not discussed here.

[31] *Makhmaduv v Russia* (App 35082/04) ECtHR 26 July 2007 at [63]

[32] See for example *WG v Austria* (15509/89) where one man on a roadway handing out leaflets was held not to be protected because he had failed to comply with the national legal rules regarding public assemblies. The rationale being that this was necessary to prevent disorder which was interpreted in this case as ensuring the free flow of traffic. Thus it would seem that the Court is unsympathetic even to actions which cause marginal or incidental disruption.

[33] Lord Carlile's Report failed to give any clarification on the meaning of design in this context. He did use the words 'design and motive' interchangeably but only in so far as it relates to the use of 'designed' in s.1(1) not s.1(2) which is our present area of interest.

[34] A/HRC/17/27 para. 81

[35] *Appleby v UK* (2003) 37 EHRR 38 at [47]

[36] Mead D, 2004, p.108-9

[37] See for example *The Stanley Works v. McNeil & Associates* case. Available Online http://www.adrforum.com/domains/decisions/94671.htm

[38] See Bowman L, 2002 'Free Speech Feels Net Copyright Chill' http://news.cnet.com/2100-1023-963122.html and also a website http://www.chillingeffects.org/protest/ created to document this phenomenon by the Electronic Frontier Foundation and a number of US law schools

[39] ECtHR, Judgment of 24 October 1995, *Agrotexim v. Greece*, Appl. 14807/89, par. 66. See also ECtHR, Decision of 14 October 2008, *Ketko v. Ukraine, Appl. 31223/03; ECtHR* , Decision of 9 September 2004, *Capital Bank AD v. Bulgaria* , Appl. 49429/99, par. 1; ECtHR, Decision of 1 April 2004, *Camberrow MM5AD v. Bulgaria* , Appl. 50357/99, par. 1.

[40] ECtHR, Judgment of 11 October 2007, *Glas Nadezhda EOOD & Anatoliy Elenkov v. Bulgaria* , Appl. 14134/02, par. 40; ECtHR, Judgment of 26 October 2000, *G.J. v. Luxembourg* , Appl. 21156/93, par. 24.This may also apply if two brothers are the sole co-owners of a family business; see ECtHR, Judgment of15 November 2007, *Khamidov v. Russia*, Appl. 72118/01, par. 123-126.

[41] Cf. ECtHR, Judgment of 29 November 1991, *Pine Valley Developments Ltd v. Ireland*, Appl. 12742/87,par. 42.

[42] ECtHR, Decision of 14 October 2008, *Ketko v. Ukraine*, Appl. 31223/03 (property); ECtHR, Decision of 14 February 2006, *Bayramov v. Azerbaijan* , Appl. 23055/03 (fair trial, property); ECtHR, Judgment of 17 June 2008, *Meltex Ltd & Mesrop Movsesyan v. Armenia* , Appl. 32283/04, par. 66 (freedom of expression)

[43] Cf. ECtHR, Judgment of 28 March 1990, *Groppera Radio AG v. Switzerland* , Appl. 10890/84, par 46-51.

[44] ECtHR, Decision of 7 November 2002, *Olczak v. Poland* , Appl. 30417/96, par. 57-62

[45] For an overview see Wall 2004

[46] Turner (2006) at p.9

[47] Fineman (2008) at p.13

[48] Hunt (2007) at p. 167

[49] This type of theorisation also traces why disembodiment or quasi-disembodiment are such attractive tropes in legal theory and Western philosophy these explanations may also go some way to explaining why there is such a disconnect in law between users online activities and their status as rights bearing beings.

[50] Niezen at p. (p.xi-xii)

[51] Vegh S. 2003 p.92

[52] See a brief discussion https://www.infosecisland.com/blogview/12092-Experts-Continue-Efforts-to-Define-Cyber-War.html on the problems of the term cyberwar.

[53] Rory Cellan Jones, BBC Technology, http://www.bbc.co.uk/news/uk-13918458 26/6/2011

[54] La Rue report (A/HRC/17/27) para 46 and 48