Uses and Abuses of Cyberspace

Andrew D Murray, London School of Economics and Political Science
Uses and Abuses of Cyberspace: Coming to Grips with the Present Dangers

Andrew Murray

As I write this in early December 2010 the world is gripped by the Wikileaks scandal. Julian Assange the Wikileaks founder is in Wandsworth Prison in southwest London while he awaits a bail hearing pending a full hearing on a European Arrest Warrant issued in Sweden on charges of serious sexual assault. The media debate and opine as to whether this is a politically motivated act undertaken by the Swedish state on behalf of the Government of the United States of America. Assange believes that upon his removal to Sweden (if permitted) he will be handed over to the US government, and meanwhile a group of online activists identified by the moniker “Anonymous” have carried out Distributed Denial of Service Attacks (DDOS) on a number of sites seen to be involved in attempts to stifle Wikileaks including Amazon, PayPal and MasterCard. Throughout the fog of the media war the Wikileaks site has remained online through the support of web users globally who have provided hosting, mirroring and internet protocol (IP) and domain name services. This serves to illustrate perhaps more clearly than any academic argument Jennings’ assumption that one of the “irreconcilable essentials of law” is change. Here we have a serious international event. One that if contained wholly within the UK would involve a number of potential criminal offences including the original offence committed by the individual who obtained the data, believed to be defence analyst Bradley Manning, which in the UK would be a breach of s.2 of the Computer Misuse Act 1990 (as well as no doubt an offence under the Official Secrets Acts 1911 to 1989), while the leaking of data by the Wikileaks site would likely be an offence under s.55 of the Data Protection Act 1998. Yet adding the international element changes this. The data were gathered in the United States and is being leaked via servers in Sweden and several other countries globally. Thus it is no longer clear if European

---

1 In the unlikely event any reader is unfamiliar with the Wikileaks scandal in November 2010 intermediary site Wikileaks began to reveal a number of private, confidential and even secret US government diplomatic cables both via its website and via partner media organisations. This led to a considerable public affairs debate across politics, the media and academia.

data protection rules apply given that the data were released in the United States and given that it may be publicised via Wikileaks servers in almost any global location. Even setting aside complex policy arguments on whether the details Wikileaks are releasing may be covered by either whistle blowing or public interest protections it is almost impossible for a lawyer to say with certainty whether the actions and activities of Wikileaks are legal or illegal.³ This suggests the change noted above is as Jennings predicted adversely challenging the other “irreconcilable essential of law”, certainty.⁴

Space and Cyberspace

Of key importance to the challenge of cyberspace to all areas of law, not just international law is the distinction between space and cyberspace. Space is the lawyer’s natural environment. It represents our place in the physical environment and is the cornerstone of our legal systems domestic and international. Concepts such as jurisdiction, domicile and enforcement of rights (and duties) are bordered by one’s physical location in space. Thus to turn to the Wikileaks example again we see that if personal data on European domiciled individuals were to be published via a Wikileaks server in the UK this may lead to a prosecution under s.55 of the Data Protection Act 1998, but as the data were released in the United States, then published at any number of global server sites the certainty of domicile, jurisdiction and most importantly enforcement of duties is undermined. The same accusation may be laid at the legal failure to curb the activities of the “Anonymous” cyber activist community. Their actions are a clear breach of s.3 of the UK Computer Misuse Act 1990. Why are they not prosecuted? Well some of these activists are certainly UK resident and may at some future time be prosecuted. But the distinction between space and cyberspace again causes problems for enforcement of the legal settlement. There is a large number of activists involved in the campaign with some estimates suggesting up to 300,000 people have downloaded the necessary software to take part in DDOS protest attacks and at least 9000 were involved in attacks on the MasterCard site. To ingather evidence on 9000 protesters and to then identify and prosecute them would be a massive task if the investigation were limited to a single jurisdiction but given the cross-border nature of the campaign it becomes an impossible task.

³ Anecdotally discussions with several colleagues in a number of fields including media law, human rights, torts, public law and public international law provided no common answer.
How then does the rule of law apply in cyberspace? Some commentators point to traditional efforts to extend principles of international co-operation such as treaty formation and co-operation on policing and recognition of enforcement orders. There are several examples of such international co-operation. In the criminal law field there is the Council of Europe Convention on Cybercrime (with protocol). This is a framework convention which attempts to harmonise the criminal legal regimes of the forty-seven signatory states, which although mostly Council of Europe States includes external parties such as the United States of America, South Africa, Japan and Canada, on a number of key issues including computer misuse (or hacking), system and data interference, computer fraud and child pornography. Another example of such traditional international co-operation is to be found in taxation where the OECD Ottawa Taxation Framework attempts to harmonise rules on the imposition, collection and transfer of taxation revenue from online activities through a series of framework general principles. Although these measures broadly provide for some level of international co-operation on key principles there remains a weakness in that they still assume principles of jurisdiction, domicile and enforcement of rights (and duties) bordered by one’s physical location in space, i.e. space principles not cyberspace principles. This is the heart of a debate surrounding effective jurisdiction in cyberspace. The key distinction here is between de jure jurisdiction and de facto jurisdiction. While there may be de jure jurisdiction granted to a particular court or tribunal by either international settlement, or even under traditional rules for the finding of jurisdiction the de facto situation may be rather different. This debate has been characterised as a debate between cyberlibertarians and cyber-legal positivists.

**Cyberlibertarianism and Cyber-Legal Positivism**

The belief that the activities of individuals online may de facto escape the control of traditional legal settlements is founded in the Cyberlibertarian movement of the 1990s. The totem of cyberlibertarian thought is usually taken to be two works. David Post and David Johnson’s 1996 paper *Law and Borders — The Rise of Law in Cyberspace,* and John Perry

---

Barlow’s *A Declaration of the Independence of Cyberspace*. Johnson & Post in giving the foundational definition of cyberlibertarianism claimed that “the Net radically subverts a system of rule-making based on borders between physical spaces”. They argued that cyberspace undermined the ability for a state to assert de facto jurisdiction over online activities, and that cyberspace should therefore be recognised as a separate legal jurisdiction from the ‘real world’. Classical cyberlibertarianism contends that regulation founded upon traditional state sovereignty, based as it is upon notions of physical borders, cannot function effectively in cyberspace as individuals may move seamlessly between zones governed by differing regulatory regimes in accordance with their personal preferences. Simply put, they claimed the internet was unregulable as de jure legal controls were confined to the jurisdiction in which they were promulgated and/or recognised while content hosted and carried on the internet flowed seamlessly over these borders. Their legal formulation of cyberlibertarianism found political voice in John Perry Barlow’s classic *Declaration of the Independence of Cyberspace*. Here using powerful and politically evocative language he asserted that governments of the world had no sovereignty on the internet, as cyberspace does not fall within the borders of any jurisdiction.

We have no elected government, nor are we likely to have one, so I address you with no greater authority than that with which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.

Governments derive their just powers from the consent of the governed. You have neither solicited nor received ours. We did not invite you. You do not know us, nor do you know our world. Cyberspace does not lie within your borders. Do not think that you can build it, as though it were a public construction project. You cannot. It is an act of nature and it grows itself through our collective actions.

---

9 Made at Davos, Switzerland, February 8, 1996 Available from: https://projects.eff.org/~barlow/Declaration-Final.html
Thus Barlow uses the same systemic argument employed by Johnson and Post to develop a political argument to counterpoint their legal one. Not only are attempts to impose external legal controls in cyberspace doomed to fail because de facto legal controls cannot be imposed on a space with no physicality and no borders (and which is therefore open to regulatory arbitrage), but according to Barlow any attempt also lacks legitimacy as there is no recognised law-making authority for this space. This argument may be seen as a historical one. Made in the mid 1990s when the internet was a less regulated space and when movements to regulate online activities were in their infancy we may wish to dismiss cyberlibertarians as libertarian romantics but to do so would be a mistake as we shall see.

The question thus becomes: are the cyberlibertarians right? This is not an enquiry into the accuracy or otherwise of Barlow’s political argument but rather are Johnson and Post correct in claiming that there are no de facto legal controls emanating from sources external to the cyberspace sphere? The immediate response to this may be found in the works of a number of lawyers who follow a legally positivistic approach and who argue that effective de jure controls may be easily converted into de facto controls via the application of traditional rules of international private law. These cyber-legal positivistic arguments are common and may be seen in a number of sources but most commonly may be centred around the so called “fallacy” arguments common to Professor Chris Reed in the UK, and Professor Jack Goldsmith in the US. Goldsmith is probably the first academic lawyer to present the fallacy arguments. He identified three, in his words persistent, fallacies which infected cyberlibertarianism. These were (1) the fallacy that cyberspace is a separate space; (2) the fallacy that territorial governments cannot regulate the non-territorial net and (3) over-optimism that there will be cheap, plentiful information. For our purposes it is the first two fallacies and in particular fallacy #1 which is important. Goldsmith points out that: “Net users are not removed from our world. They are no more removed than telephone users, postal users, or carrier-pigeon users. They are in front of a screen in real space using a keyboard and scanner to communicate with someone else, often in a different territorial jurisdiction.”

is the key to enforcement of rights (and duties) and may be instrumental in solving problems of both jurisdiction and domicile. Effectively Goldsmith is saying that cyberspace is a communications media not a physical space – he denies the distinction between space and cyberspace and instead treats cyberspace as an extension of pre-existing (and legally regulable) communications media. This view has many supporters include Professor Chris Reed who defines Goldsmith’s fallacy #1 as “the cyberspace fallacy”, saying “the human and corporate actors and the computing and communications equipment through which the transaction is effected, all have a real-world existence and are located in one of more physical world legal jurisdictions”14. In this Reed and Goldsmith are essentially correct; there is no doubting that individuals and corporations undertake actions from within sovereign jurisdictions. However, the trans-border nature of internet activity has presented a significant challenge to traditional legal institutions in enforcing jurisdiction over online activities. At times, the law has struggled to establish effective jurisdiction,15 for as Gillies notes the “dematerialised nature of online commercial activities renders the location of the parties and the place where those activities take place difficult to determine”16. This issue is none more prevalent than in the related cases of Licra et UEJF v. Yahoo! Inc. and Yahoo! France,17 and Yahoo Inc. v. LICRA18 an action described by one US commentator as “a backlash response to the cultural and technological hegemony of the United States in the on-line world”.19

Space and Cyberspace: Licra et UEJF v. Yahoo! Inc. and Yahoo! France

This inter-jurisdictional dispute arose because Nazi memorabilia was being offered for sale on a Yahoo! auction site, which was accessible in France. The Ligue Internationale Contre le Racisme et l'Antisémitisme (LICRA) and the Union des Etudiants Juifs de France (UEJF) brought an action against Yahoo! on the grounds that offering the sale of Nazi memorabilia was illegal under Article R645-1 of the French Criminal Code. This case presented a

18 There were three hearings in California. A hearing before the District Court in which a decision was filed on 7 November 2001 — Yahoo Inc. v. LICRA 145 F. Supp. 2d 1168 (ND Cal. 2001) an appeal to the 9th Circuit in which a ruling was filed on 23 August 2004 — Yahoo Inc. v. LICRA 379 F. 3d 1120 (9th Cir. 2004) and an en banc rehearing before the 9th Circuit in which a ruling was filed on 12 January 2006 — Yahoo Inc. v. LICRA 433 F.3d 1199 (9th Cir. 2006).
challenge for establishing jurisdiction over online activities. As Yahoo! was a US company operating within the US, the Tribunal de Grand Instance de Paris had to assess whether the actions undertaken on foreign soil fell under its jurisdiction. Yahoo! argued that the French court was “not territorially competent over the matter because the alleged fault is committed on the territory of the United States”, but the court ruled otherwise: “the harm is suffered in France; our jurisdiction is therefore competent”. In addition to the local harm, the court found that Yahoo! were able to identify French customers. Yahoo! were using Internet Protocol (IP) numbers to identify – with significant accuracy – French visitors in order to display relevant advertising to them. A panel of technical experts gave evidence that it was technically possible for Yahoo! to use IP numbers to filter out French users, and the court ordered Yahoo! to install such filters or face a daily fine.

However, without the ability to enforce its will, the law has no real power. As Shultz notes: the territorial nature of enforcement jurisdiction is such that “the state can enforce its laws only against in-state actors, against entities with a presence on the territory of the state or with assets there.” This was exemplified in actions of Yahoo! immediately after the order was made. Instead of appealing the decision within the French legal system, Yahoo! took action against LICRA and UEJF in the US District Court of California, seeking a ‘declaratory judgment that two interim orders by a French court are unrecognizable and unenforceable’. They successfully argued that enforcement of the French ruling would violate the First Amendment in the US. The District court ruled in Yahoo!’s favour, undermining the jurisdiction of the French court. Yahoo! eventually ended the dispute by removing all Nazi material from their auction sites, citing public opinion as the reason. While the District Court’s decision was eventually reversed (in LICRA and UJEF’s favour), the issue of establishing effective jurisdiction seized the courts for almost six years and across two continents.

---

22 Yahoo Inc. v. LICRA 433 F.3d 1199 (9th Cir. 2006).
23 Although an intelligent international law audience will recognise this is not unusual in the sphere of conflicts of law what is interesting is the case was not finally settled by the courts but by the voluntary actions of Yahoo!. Had Yahoo! continued to host Nazi memorabilia the conflict would have remained extant with them in breach of the order of the Tribunal but shielded by the 1st Amendment.
It may be argued that the Yahoo! decision offers support for the long disregarded cyberlibertarian argument by illustrating how the issue of enforceable jurisdiction has been affected by the borderless nature of the internet. Johnson & Post said: “The rise of the global computer network is destroying the link between geographical location and ... the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena.” The information one contributes on the Internet can be retrieved in virtually any jurisdiction throughout the globe, and the de jure rules where one is domiciled are bound to be in conflict with the de jure rules elsewhere, for as highlighted by Shultz: “seen from the perspective of Internet content providers, the problem is that they may be subject to regulations of states to which they had no intention of sending information and to local laws the application of which they could thus not legitimately be expected to foresee.” Reed and Schultz both point out that if one were to expect de jure jurisdiction to be converted into de facto jurisdiction, then in order to prevent breaking the law of at least one state, one must comply with the most stringent laws found around the globe, or at least the most stringent laws among the nations where you have assets. This seems to place too much emphasis on a positivistic analysis which places an unrealistic burden on internet users.

**Space and Cyberspace: R. v Sheppard & Anor.**

Cyber-legal positivists often suggest that the Yahoo! case is an extraordinary case and point to a number of cases in which successful cross-jurisdictional enforcement has been effective. Cases such as defamation actions *Dow Jones & Co. Inc. v. Gutnick*, *Loutchansky v. Times Newspapers Ltd*, and *King v. Lewis*, or copyright cases such as *MGM Studios Inc. v. Grokster Ltd*, and *Universal Music Australia Pty Ltd v. Sharman License Holding Ltd.* Recently attention has been turned to an English case as the classical example of how one cannot escape de facto jurisdiction by simple “offshoring” content. It is argued by Cyber-
legal positivists that the case of R. v. Sheppard & Anor\textsuperscript{32} has shown that unlawful activities undertaken in cyberspace can be subject to successful prosecution within a real world jurisdiction. While domiciled in the United Kingdom, Mr Sheppard posted racially inflammatory material on a website hosted in California, and was subsequently convicted under s.19 of the Public Order Act 1986, whereby ‘a person who publishes or distributes written material which is threatening, abusive or insulting is guilty of an offence if he intends thereby to stir up racial hatred’. Mr. Sheppard appealed his conviction on the grounds that as the website was hosted outside of the UK, the publication of the material fell outside of the jurisdiction of the courts of England and Wales. Cyberlibertarian thought would deem this to be a classic example of the inability to regulate cyberspace activity. The technology within cyberspace has essentially removed the physicality of the traditional ‘hard copy’ publication and distribution model. People accessing the racially inflammatory material were essentially being delivered material from California, via a number of physical servers in various locations. The court ruled against the appellant, noting that a “substantial measure” of the activities constituting the crime took place in England. By operating and editing the website from within England, Mr Sheppard was found to be acting within the jurisdiction of England and Wales, rendering the physical location of the server irrelevant. Furthermore, the judge also noted that Mr Sheppard targeted the jurisdiction in question, having a dedicated page for British customers on the website (the only nationality with its own dedicated area), and having also offered publications for sale with the price in pounds sterling.

It may be argued that the ruling dismisses Johnson & Post’s argument that “the power to control activity in Cyberspace has only the most tenuous connections to physical location.”\textsuperscript{33} The case appears to show that there is in fact a real and direct connection between activities undertaken in cyberspace and the physical location in which one is located. Had the judge upheld the appeal, individuals within the jurisdiction of England and Wales would essentially be able to circumvent s.19 of the Public Order Act by publishing racially inflammatory content via servers located in the US using the shield of the First Amendment. This hypothetical world would entail a true realisation of cyberlibertarian theory. However, this judgement proved that jurisdiction can be established even if the content in question is hosted in cyberspace.

\textsuperscript{32} [2010] EWCA Crim 65.

That is it may have established that if it were entirely effective. While Mr Sheppard sits in a jail cell, his website still stands and may be accessed from any point on the globe with an internet connection including the United Kingdom. What we see here is an essential distinction in space and cyberspace. The courts of England and Wales have taken de facto jurisdiction over Mr Sheppard’s corporeal person but not his incorporeal identity. Thus the distinction between the cyberlibertarian ethos and the cyber-legal positivists is drawn into sharp relief. The cyberlibertarians were defining the inability of traditional states-based regulators to leverage de facto jurisdiction around the incorporeal identity of the individual which is made up of their online postings, accounts and alter-egos. The cyber-legal positivists were meanwhile focussing upon the corporeal identity if the individual which, of course, will be subject to de facto jurisdiction wherever they are domiciled and wherever they hold assets which may be seized. The issue of enforcement then simply becomes one of international private law. We are returned to Goldsmith’s rather arbitrary distinction that the internet is a communications media not a physical space. What \textit{R. v. Sheppard & Anor} demonstrates is that this is not strictly true, as has been the common theme of this essay there is space and cyberspace. While the courts of England and Wales take jurisdiction over Mr Sheppard’s corporeal presence in space, they have been denied de facto jurisdiction over his virtual identity (or presence) in cyberspace and as a result the harm which s.19 of the Public Order Act seeks to prevent continues to occur in the UK every time an individual accesses Mr Sheppard’s website from the UK. How then is de facto jurisdiction established over his cyber-presence?

By placing his content on a Californian server Mr Sheppard effectively exported the de facto jurisdiction over his content to the United States, and in particular to the State of California. There, following the US Supreme Court decision in \textit{Reno v. ACLU},\textsuperscript{34} it is protected by the First Amendment. This allows US servers to be used as a safe haven for online hate speech.\textsuperscript{35} If an individual anywhere in the world is willing to take the risk and publish hate material to a US web server, the material is likely to stay there unmolested. Furthermore the constitutional status of the Supreme Court decision in \textit{Reno v. ACLU} renders the US Government unable to enter into any international treaty or agreement, or recognise an order of another court or

\textsuperscript{34} 521 US 844 (1997).
jurisdiction which would restrict the right of individuals awarded under Reno for as explained by Douglas Vick “The Reno decision will constrain the international community’s efforts to establish a comprehensive body of common rules for regulating Internet content. Under American law, treaties and other international accords are hierarchically inferior to the provisions of the US Constitution. A treaty provision, just like a congressional statute, is unenforceable if it fails to conform with First Amendment law.”

This handicap could clearly be seen in negotiations to draft the Council of Europe, Convention on Cybercrime. The Convention deals with only one ‘content-related offence’, that being the production or distribution of child pornography using a computer system. We know several of the states that took part in the drafting process were keen to include further content related offences, but that these never made the final text. The reason for this is to be found in the Explanatory Report: “The committee drafting the Convention discussed the possibility of including other content related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds.” Although the identity of the delegations in question is not revealed, it is clear that at least one of these would be the US delegation for the US delegation could not, as Douglas Vick had predicted, sign the US Government up to any treaty provisions which would conflict with First Amendment protection.

**Space, Cyberspace and International Law**

The present author is not an international lawyer by training or practice and therefore begs indulgence over his simplistic view of international law. If we are to have any hope of producing effective de facto jurisdiction for cyberspace content international lawyers must first accept there is a distinction between space and cyberspace. For too long cyberlawyers have debated whether or not effective legal controls may be leveraged into cyberspace without facing up to this distinction. Yes cyberspace may (when viewed from the space of the physical environment) look like a communications media. It is this perspective which leads

---

37 CETS No. 185, Budapest, 23.XI.2001
cyber-legal positivists to announce that of course the activities of an individual may be regulated in cyberspace as the individual remains domiciled in real space. Equally when one looks at cyberspace as a separate space by looking at the content of the place, one may erroneously imagine that it is unregulable as the cyberlibertarians did. The example of both Mr Sheppard and Mr Assange show that while the body may be regulated the outpourings of the mind may not, unless one takes a holistic view that space and cyberspace are two separate but connected places. Where does this leave the international lawyer? It suggests there are areas where international co-operation and perhaps even formalisation of law through treaty obligations are likely to be successful. These areas include e-commerce where the UNCITRAL Model Law on Electronic Commerce has been extremely successful in bringing harmony and international recognition,\(^{39}\) intellectual property rights where a number of WIPO treaties\(^{40}\) and others such as the recently finalised Anti-Counterfeiting Trade Agreement\(^{41}\) have been or are likely to be effective and in a number of criminal law measures where the Council of Europe Convention on Cybercrime has been effective in providing cooperation on matters of illegal interception and computer related fraud\(^{42}\). Unfortunately content related issues are more complex due to the effect of *Reno v. ACLU*. Here US-based servers will act as safe havens, as we saw in *Sheppard* (and perversely in reverse in the Wikileaks case). Content can be instantly mirrored and moved, as the Wikileaks case has shown to contain data when it is on the web is almost impossible. If lawyers want to create de facto control over content it cannot be though legal documents it must be though a web of terms and conditions of service and through Lessigian code-based solutions.\(^{43}\) Content may just be beyond the direct control of the international legal community, as predicted by the cyberlibertarians, after all.


\(^{40}\) Including the WIPO Performances and Phonograms Treaty of 1996, the WIPO Copyright Treaty of 1996

