Private power and new media: the case of the corporate suppression of WikiLeaks and its implications for the exercise of fundamental rights on the Internet

Angela Daly
PhD candidate, Department of Law, European University Institute. LLM (Universite de Paris 1 Pantheon-Sorbonne, 2007); BA(Hons) (Balliol College, University of Oxford, 2006).

Abstract

The focus of this paper will be the recent conduct of various corporations in withdrawing Internet services provided to information portal WikiLeaks in light of the controversy surrounding WikiLeaks publishing classified documents of correspondence between the US State Department and its diplomatic missions around the world in late 2010. The implications for freedom of expression (especially the right to access information) on the Internet will be examined in the wake of WikiLeaks, particularly in the context of the infringer being a private actor, and one comprising a mono- or oligopoly. The motivation of these private actors in contributing to the suppression of WikiLeaks will be assessed to examine whether it constitutes an example of Birnhack and Elkin-Koren's 'invisible handshake' i.e. the 'emerging collaboration' between the state and multinational corporations on the Internet that they posit is producing 'the ultimate threat'. The legal recourse open to WikiLeaks and its users for the infringement of fundamental rights will be examined, especially the First Amendment to the US Constitution since the geographic location for these events has mostly been the USA. Finally, the postscript to the WikiLeaks controversy will be considered: the "information warfare" conducted by hackers will be examined to determine whether the exercise of power of these Internet corporations in a way which infringes fundamental rights can be checked by technological means, and whether hackers are indeed the true electronic defenders of freedom of expression.

1. Introduction

In November 2010, the online non-profit media organisation WikiLeaks published classified documents detailing correspondence between the US State department and its diplomatic missions around the world, numbering around 250,000 cables. In order to maximise media exposure, five 'old media' publications (namely the newspapers Der Spiegel, El País, Le Monde, the Guardian and the New York Times) were given prior access to the material on the condition that they complied with common deadlines over when the material was released, with the result of this being that the correspondence was released in parts over the course of many days, dominating newspaper headlines worldwide. These diplomatic cables contained classified information comprising comments on world leaders, foreign states, and various international and domestic issues.

The reaction to WikiLeaks' release of these classified documents from the American political class was generally condemnatory of the decision to publish the information publicly, invoking national security concerns and the jeopardising of US interests abroad. There were also reports of the US Justice Department considering charging Julian Assange, the founder of WikiLeaks, with espionage offences based on the release of the cables.

In the wake of the political reaction, there was also a response from the corporate world, with various companies, such as Amazon, PayPal, Visa and Mastercard, ceasing to continue the provision of services to WīkiLeaks.

In light of the above, this paper will firstly provide a detailed description of this corporate response to the Wikileaks controversy (section 2), prior to an assessment of the motivation for these actors to contribute to the suppression of WikiLeaks, to determine whether it is an example of Birnhack and Elkin-Koren's 'invisible hand' (section 3). The implications for freedom of expression on the Internet will then be analysed, especially in the situation of the infringer being a private actor constituting a mono- or oligopoly, before an examination of the legal resource open to WikiLeaks and its users for any infringement of fundamental rights (section 4). Lastly, the response to this corporate behaviour from the hacking community will be considered, particularly the Anonymous collective, to determine whether such exercises of corporate power on the Internet can be checked by employing technological means and whether hackers really are the defenders of online free expression (section 5).

2. The corporate response to WikiLeaks

Various corporate entities with different links to WikiLeaks stopped providing services to the organisation subsequent to the release of the US Embassy cables. More precise details of these instances are provided below.

2.1 Amazon.com

Amazon.com, the online company which started life selling books, has diversified into various other markets, including Amazon Web Services (AWS) which offers remote computing services over the Internet for other websites or client-based applications. WikiLeaks' website was being hosted by Amazon.com via these services prior to the US embassy cables controversy, yet on 1 December 2010 Amazon.com ceased to host the site. At first, Amazon.com did not comment on this cessation of service, but it subsequently issued a statement denying that either the government prompted them to stop hosting the site, or that mass-scale DDOS attacks prompted the website being taken off their servers. The company gave the reason for its actions as being that WikiLeaks violated AWS's terms of service, in particular the term stipulating that WikiLeaks must have all of the rights over the content posted online and that the use of this content must not cause injury to any person or entity. Amazon.com stated that it was 'clear' that WikiLeaks did not own or control all these rights over this content, and that it was 'not credible' that WikiLeaks could not have redacted the information in a way to ensure that 'innocent people' were not put in 'jeopardy'.

2.2 Apple

The interaction between Apple and WikiLeaks consisted of an application being created for Apple's App Store, which was submitted to the App Store on 11 December 2010 and approved for sale on 17 December 2010 [Albanesius, 2010]. The App Store is an online shop where users of Apple hardware such as the iPad, iPhone and iPod Touch can browse and download applications for their device, some of which are free, some of which are available at a cost. The specific WikiLeaks App was created by Igor Barinov, a developer not associated with WikiLeaks, and was described as giving instant access to WikiLeaks' material. Furthermore, $1 from every App purchased would be donated to WikiLeaks itself. On 20 December 2010, the App was removed from sale on the App

Store. According to Barinov's Twitter page, Apple gave no reason for its decision to cease offering the WikiLeaks app for sale.

2.3 Bank of America

On 17 December 2010, Bank of America issued a statement saying that it would no longer process any transactions it believed to be destined for WikiLeaks, stating furthermore that its action was due to its belief that WikiLeaks may have been engaging in activities that were inconsistent with the Bank's internal policies for processing payments [Schwartz, 2010].

2.4 EveryDNS

EveryDNS, a domain name system (DNS) management service provider which was WikiLeaks' hosting provider in the USA, dropped WikiLeaks from its entries on 2 December 2010, claiming in a statement that it had done so because the domain wikileaks.org had become the target of 'multiple distributed denial of service (DDOS) attacks, claiming that these attacks threatened the stability of EveryDNS's infrastructure, and thus threatening access to around 500,000 other websites.

2.5 MasterCard

In early December 2010, the major payment processing company MasterCard announced that it would stop processing payments to WikiLeaks, with its reason for doing so being that WikiLeaks was engaging in illegal activity [McCullagh, 2010].

2.6 PayPal

PayPal, a service which allows payments and transfers of money to be made via the Internet, announced in a statement dated 3 December 2010 that it would permanently restrict one of its accounts which was being used to raise funds for WikiLeaks, claiming that the account was violating its Acceptable Use Policy, since the account involved activities that 'encourage[d], promote[d]. facilitate[d] or instruct[ed] others to engage in illegal activity'.

In February 2011, PayPal also suspended the account of Courage to Resist, an organisation raising money for the legal costs of Bradley Manning (a US army soldier arrested in May 2010 on suspicion of providing classified information to WikiLeaks – but not related to the US Embassy cables) [Indvik, 2011]. However, PayPal subsequently reversed its decision to suspend the account, claiming that the suspension had 'nothing to do with WikiLeaks', and instead the reason was that Courage to Resist had not complied with PayPal's policy regarding non-profit organisations being required to link a bank account to their PayPal account.

2.7 Tableau Software

Tableau Software, an American computer software company, provided data visualisation products to WikiLeaks for the contents of the leaked US embassy cables, subsequently removed them from the Internet on 1 December 2010. In a statement the company said that this was 'not an easy decision, nor one that we took lightly', but stated that the decision was based on their terms of service (in particular, users should not 'upload, post, email, transmit or otherwise make available

any content that they do not have the right to make available') as well as the company receiving a request from Senator Joe Lieberman, the chairman of the Senate Homeland Security Committee, calling for organisations providing services to WikiLeaks to terminate their relationship with the website [Fink, 2010].

2.8 Visa

Visa Inc., another major payment processing company, started suspending transactions destined for WikiLeaks on 7 December 2010 before carrying out an investigation into the organisation to determine whether its behaviour was contrary to Visa's operating rules. Visa Europe Ltd announced in January 2011 that it would continue to block donations to WikiLeaks until its own investigation was completed (which at the time of writing, has not yet happened).

3. A case of the 'invisible' handshake?

Having seen the various corporations above cutting off services to WikiLeaks, this section will analyse the motivations for their responses to the US embassy cables controversy, and determine whether it is an instance of Birnhack and Elkin-Koren's 'invisible handshake'. The section will commence with an explanation of what this invisible handshake is, before continuing on to analyse these companies' behaviour in order to make this determination.

3.1 The 'invisible handshake'

In their seminal article, Birnhack and Elkin-Koren identify what they call the 'invisible handshake' as the convergence of the interests of powerful private entities on the Internet and the State. The 'handshake' is 'invisible' since the average user/consumer/citizen is not usually aware of the extent of the cooperation between these two axes of power on the Internet, and this cooperation is often fairly clandestine and 'beyond the reach of judicial review'. Birnhack and Elkin-Koren posit that this interaction between government and its agencies, and multinational corporations produces 'the ultimate threat' to users' freedom on the Internet.

This state of affairs has come about due to the policies of the governments of various developed countries, particularly in North America and Europe, in adopting the role of regulator regarding the communications infrastructure, directing private behaviour through the use of rules, and thus in practice allowing the emergence of private entities in this environment, which exercise control over parts of the network. When the State wants to exert control over the network, it co-opts these pre-existing privately-managed nodes. Birnhack and Elkin-Koren note that the State has become more active in the Internet from about 2000 onwards, due to 'its growing significance for commence and community', and due also to geopolitical developments such as the use of the Internet by terrorists, especially in the wake of 9/11. The State is now functioning as an 'active player' on the Internet instead of a mere regulator, and is also acting using the Internet to fulfil its 'ancient duty of securing individual safety and national security'. To do this, the State co-opts private entities operating in the various layers of the Internet, either by obliging them to comply with State demands (through using legislative means) or by offering incentives for these entities to do so voluntarily. Although this is not abnormal behaviour from such States in their regulation form, until the 2000s such approaches had not been seen on the Internet, and the latter method of informally incentivising corporations to act in ways the governments want places such action firmly outside the scope of any administrative law checks, such as judicial review. One of the main reasons why these private entities are of interest to States is that by the nature of the products and services they offer, they simultaneously

perform a monitoring function of the information that passes through their node of control, in particular being able to identify real-world, offline characteristics of the user.

Furthermore, Birnhack and Elkin-Koren argue that increased concentration in Internet markets and increased entry costs due in part to potential liability for users' behaviour (principally in the US) has limited competition between corporations on the Internet, and so limited options for users, and this is convenient for States since markets which are more concentrated are easier to govern. In addition, the potential liability of online service providers at least encourages and at most forces these Internet corporations also to exercise a policing function over their users, turning them into private enforcement agents.

3.2 The motivation for cutting off WikiLeaks

The companies considered above gave three types of reason for their decisions to suspend services to WikiLeaks: (suspected) violation by WikiLeaks of the company's terms of service; (danger of) damage to the company's technical infrastructure; and pressure from the US government, particularly in the form of Senator Joe Lieberman, to sever ties with WikiLeaks. Apple is the only company not to have given any reason for pulling the WikiLeaks app from its App Store.

EveryDNS was the only company which explicitly stated that it had terminated its relationship with WikiLeaks due to infrastructural reasons. In contrast, Amazon explicitly denied that this was a motivation for ending its relationship with WikiLeaks.

Tableau Software explicitly stated that part of its motivation to terminate its relationship with WikiLeaks was due to the request it received from Senator Lieberman requested it to do so. The decision to do so was strongly criticised by James Ball, who created the visualisation, claiming it 'smack[ed] of cowardice and blind censorship' [Arthur, 2010].

The other companies claimed that their motivation for ceasing to provide services to WikiLeaks was due to its behaviour (potentially) violating their internal policies, either because WikiLeaks did not have rights over the content, the publication of the content could endanger 'innocent people' (i.e. those persons whose names were mentioned in the leaked cables), or because WikiLeaks was more generally engaged in 'illegal' activity or encouraging others to engage in illegal activity (i.e. the actual leaking or dissemination of the leak of classified documents). However, these claims of illegality or lack of rights over the content are mere allegations since there has been no authoritative legal pronouncement on the matters, and the claims regarding the jeopardisation of the safety of individuals are also mere speculation. Furthermore, even if an illegal act was committed by the person who leaked the information to WikiLeaks, it would seem that WikiLeaks in disseminating that information enjoys the protection of the First Amendment vis-à-vis prosecution by the US Government [Benkler, 2011]. Nevertheless, the signals coming from Senator Lieberman were highly condemnatory of any corporate collaboration with WikiLeaks: even though Amazon claimed its decision was wholly based on a potential violation of its terms of service, it had been in close contact with Senator Lieberman when coming to its decision, and the Senator himself issued a statement saying that this was 'the right decision' and 'should set the standard for other companies'. Moreover, it is unclear what kind and amount of pressure was put on Amazon 'behind the scenes' by Senator Lieberman and his staff to sever its ties with WikiLeaks – indeed, the Guardian claimed Amazon was put under 'heavy political pressure' to stop hosting WikiLeaks [MacAskill, 2010].

3.3 The invisible handshake in cutting off services to WikiLeaks?

Although none of the corporations examined were legally obliged to cut off services to WikiLeaks (e.g. none of them were served with a legal instrument specifically forcing them to do so), and despite the fact that some of them explicitly stated that government pressure was not a reason for ceasing their relationship with WikiLeaks, there does appear to be in practice a manifestation of the invisible handshake between these corporations and the (US) government over WikiLeaks. The rhetoric of the US political class at the time was almost entirely against WikiLeaks' behaviour, with the more sober coming from *inter alia* the White House (which issued a statement saying that WikiLeaks had 'put at risk our diplomats, intelligence professionals, and people around the world who come to the United States for assistance in promoting democracy and open government', terming WikiLeaks' behaviour 'reckless and dangerous action'), and US Secretary of State Hillary Clinton (saying that WikiLeaks' disclosure of this information 'puts people's lives in danger, threatens our national security and undermines our efforts to work with other countries to solve shared problems') [Jackson, 2010], to the more emotive, such as Senator Mitch McConnell, US Senate Minority Leader, who called founder of WikiLeaks Julian Assange ‘a high-tech terrorist’ and said he should ‘be prosecuted to the fullest extent of the law’ [Curry, 2010]. Furthermore, there has been speculation about the possibility of a secret US grand jury espionage investigation into WikiLeaks [Beaumont, 2011].

Thus, there would appear to be at least a climate of moral and political if not yet legal condemnation of WikiLeaks' behaviour generated by the US government, and at most pressure and threats applied to the corporations facilitating the functioning of WikiLeaks. The corporations' response in cutting off these services to WikiLeaks would appear to fit into the conceptualisation of the invisible handshake as corporations being obliged or strongly encouraged by the government (with the possible threat of legal proceedings if the corporations do not comply with the government's demands). In this way, by co-opting these private entities and their nodes of control, the US government has been able to make the functioning of WikiLeaks much more difficult (although not impossible, as despite the withdrawal of these services, WikiLeaks was still accessible on the Internet). Although, as mentioned above, this kind of behaviour from governments vis-à-vis corporations and vice versa is not unheard of, instances of this happening on the Internet are growing in prominence, especially since in the 1990s such government/corporate control seemed unlikely. Indeed, this may be an attempt by governments of liberal democracies which place a strong emphasis on market mechanisms, such as the US, to manipulate the functioning of the Internet to approximate a new manifestation of Herman and Chomsky’s ‘propaganda model’ of the mass media.

Indeed, Birnhack and Elkin-Koren themselves have commented on the case of WikiLeaks and the corporate response, and themselves identify it as 'a demonstration of an unholy alliance between government and large private corporations'. They note the 'shaky legal ground' on which the US government is standing when it comes to the legality of WikiLeaks' behaviour since, as mentioned above, even if the leak itself was illegal, its dissemination by a receiver of the leak such as WikiLeaks would seemingly be perfectly legal, and indeed protected from government interference by the free speech guarantees under the First Amendment to the US Constitution. However, attempts by private entities to cut off services to WikiLeaks are not subject to such Constitutional constraints protecting free expression and so constitute a more effective way of containing the leak.

4. Implications for online free expression and legal recourse for WikiLeaks

In light of the above analysis on the corporate response to WikiLeaks constituting an example of the invisible handshake, this section examines the implications of this government co-optation of corporations for free expression on the Internet, looking in particular at what happens when the market in question is oligopolistic or dominated by one firm, such as the cases of the payment

processing firms and Apple's App Store respectively. The legal recourse open to WikiLeaks and its users for any infringement of their fundamental rights will then be considered.

4.1 The implications of the corporate response to WikiLeaks for online expression

As mentioned in the previous section, the practical effect of these corporations cutting services to WikiLeaks is to stifle the freedom of expression of WikiLeaks itself, as well as the right of its users to receive this information. However, since these corporations are private entities, they are not subject in the same way as State agencies to the constraints contained in the First Amendment to the US Constitution or for that matter Article 10 of the European Convention on Human Rights (ECHR) protecting free expression in Europe (the US and Europe being the primary arenas of the WikiLeaks controversy, the geographical locations of most of the actors involved, whether government, corporate, civil society or human individual – and so the jurisdictional focus of this piece). This issue extends beyond the scope of this particular incident involving WikiLeaks, and in fact highlights the extent of private entities' control over the Internet and the information disseminated over it. This gives cause for concern over civil liberties online: as MacKinnon puts it, '[w]hat is troubling and dangerous is that in the internet age, public discourse increasingly depends on digital spaces created, owned and operated by private companies'.

The relationship between Internet users (whether organisations such as WikiLeaks or individuals) and these Internet corporations offering products and services is governed by private arrangements (usually contract), in which (notwithstanding consumer protection law inserting certain terms into such contractual arrangements) the parties can stipulate the terms they wish and do not *prima facie* have to concern themselves with constitutional or treaty provisions on free expression. This is demonstrated in the corporations dealing with WikiLeaks giving as a reason for ceasing the provision of services as being WikiLeaks' (alleged) violation of their terms of service, to which WikiLeaks, when commencing using these services, agreed, and by which so was bound.

Yet, the logic of competitive markets for goods and services would suggest that even if the companies dealing with WikiLeaks cut off their services to the organisation, all is not lost: WikiLeaks merely needs to venture out again into the marketplace to obtain these services from competitors of these companies, which given WikiLeaks' demand for such services, ought to want to supply them.

However, if the market in question is not so competitive, either possessing an oligopoly or monopoly and if these corporations decide not to provide services to an organisation such as WikiLeaks, then WikiLeaks is in practice unable to procure these services from other sources and is effectively unable to disseminate the information it wants.

In the corporate responses above, the situation with the payment processing firms bears some resemblance to an oligopoly: the effect of Visa, Mastercard, PayPal and the Bank of America refusing to process payments for WikiLeaks dramatically reduced the possibility of donating to WikiLeaks. Indeed, it took mobile payment company Xipwire's positive action to facilitate payments to WikiLeaks for there to be a guarantee that those who wished could donate to the organisation (although this would appear to show that there are no, or low, entry barriers to this market) [Petrucci, 2010]. Thus, the power of such companies as Visa and Mastercard in the markets for payment processing, and in particular the level of control they can assert especially when combined, can be demonstrated by the fact that there have been various groups of legal proceedings against the two companies in both the US and the European Union for anticompetitive behaviour due to their large market shares. Furthermore, in light of these two companies cutting off services to WikiLeaks, members of the Dutch D66 political party in the European Parliament expressed fresh

concerns over the companies' level of dominance in the European market, and in particular the implicit illegitimacy of the American influence over the blocking of payments from European citizens to a European organisation i.e. WikiLeaks [Dekker, 2010].

Moreover, there is the more monopolistic position of Apple over its App Store, which withdrew the WikiLeaks app in wake of the controversy over the US embassy cable leaks. For a user of Apple's iPad, iPhone and iPod Touch platforms, unless they 'jailbreak' the device, they can only run programmes approved by Apple and available via the App Store. 'Jailbreaking' one of these devices would be p*rima facie* illegal in the US under the Digital Millennium Copyright Act as violating copyright law; however in July 2010 the US Copyright Office explicitly recognised an exception to the DCMA in this case, following a request from the Electronic Frontiers Foundation. Nevertheless, this at least gives Apple the power to control the Apps that are available to the users of its devices, and the ability to refuse Apps created by developers outside of Apple (such as the WikiLeaks App). There is the real potential for Apple to favour its Apps made in-house over Apps from external sources in an anticompetitive fashion, as well as exert some level of more ideological censorship over the kind of Apps that are available to the users of Apple devices.

Thus, the existence of a monopolistic or oligopolistic market worsens the circumstances for exercising the right to free expression on the Internet: in addition to the fact that constitutional/treaty guarantees of this right do not provide as weighty guarantees against infringements of the right by private entities as compared to governments, the existence of a mono- or oligopoly which acts in a way that impinges upon a user's free expression is even more detrimental since this denies or at least restricts even more the possibility of the user turning to a competitors to facilitate her free expression online.

4.2 The legal recourse available for corporate free speech violations

Following the analysis above, the legal options open to WikiLeaks are considered below.

Legal guarantees of free expression

As mentioned above, the right to free expression is protected in the jurisdictions under consideration by the First Amendment to the US Constitution and Article 10 of the ECHR.

First Amendment to the US Constitution

The First Amendment has traditionally been conceived of as a right enforceable against the American government, as opposed to a right enforceable against private parties such as corporations. Indeed, one way in which the American and European conceptions of free speech differ is that in the US not only is the First Amendment not enforceable against private entities such as corporations, but they themselves are considered to be 'speakers' and entitled to enjoy the right as well. The European approach centres more on the individual human person and is based on the ideas of autonomy and human dignity, and involves more government regulation of expression, such as that emanating from legal as opposed to human persons, and hate speech.

Nevertheless, the limitations of this conception of the right to free expression in the Internet environment have been recognised. Yemini (writing in the context of the net neutrality debate but with conclusions on this issue which can be applied more widely) critiques the ‘traditional bilateral conception’ of the First Amendment as the scenario of a conflict between a speaker and the (US)

government and claims that this makes it inadequate for dealing with the 'multiple-speaker environment' found on the Internet. The issue with free expression and private entities in the net neutrality debate revolves around the fact that Internet Services Providers (which are usually private entities in liberal democracies) have the technological means to control and manipulate the information that Internet users send and receive, yet they are not, under the traditional conception of free expression, subject to regulation on that basis, or indeed proceedings for infringement of the right. Yet, as explored above, the other layers of the Internet are similarly owned and controlled by private entities, which can exert their power in ways which are not in accordance with free expression.

Indeed, Benkler also recognises the difficulty in a First Amendment action in these circumstances. Certainly a direct action against the private providers under the current conception of the First Amendment is not possible, and it would be 'extremely difficult to bring action against the government or its officials' due to any pressure from the government that was applied to these private actors being indirect and subtle.

Article 10 of the ECHR

The situation in Europe differs somewhat: Art 10 of the ECHR protecting free expression is an obligation primarily pertaining to contracting States, and is usually conceived of as a negative freedom. Nevertheless, the Article itself has been found to have some horizontal, positive effect in the case of *Khurshid Mustafa and Tarzibachi v Sweden*, a dispute between tenants and their landlord over a satellite dish the tenants had installed to receive Arabic and Farsi language programmes against the terms of the tenancy agreement. In this case, the European Court of Human Rights (ECtHR) found that the applicants' freedom to receive information via satellite broadcast, which formed part of Art 10, had been violated as the State, Sweden, had 'failed in their positive obligation to protect that right'. It is possible that the reasoning in this decision could also be applied to the freedom to receive information on the Internet, and it could be argued that Internet users (as opposed to WikiLeaks itself) had this right infringed by companies such as Amazon refusing to host WikiLeaks. However, due to the WikiLeaks website itself migrating to different servers, as well as various 'mirror sites' of WikiLeaks appearing in various other locations on the Internet, these attempts to 'shut down' WikiLeaks and prevent users accessing the information contained in the leaks did not work, and the fact that users could still see this information would suggest that the Court would not find that their right to receive information had been violated. Nevertheless, again through the ECHR apparatus, the corporations themselves cannot be directly censured for their behaviour.

Alternative pathways for legal recourse

Since the most direct legal protections of free expression cannot easily if at all be used against private entities, other pathways to upholding WikiLeaks' and its users' rights through the apparatus of private law will be explored below.

Competition law

Given the semblance of a monopoly in the form of Apple and oligopoly in the form of the payment processing firms, this part will consider whether competition law ('antitrust' in the US) can provide any remedies which would in fact go some way to correcting the infringements of freedom of expression.

Apple

In its position of control over the App Store, there is the possibility that Apple could be shown to be a dominant entity. It has complete control over the Apps which appear in its App Store even if they are created by other companies or individuals, and so could be said to be in a dominant position in the market for the provision of these services. However, since the practice of 'jailbreaking' Apple devices has been ruled to be legal in the US and is permitted in the EU, consumers can also choose to run apps from Apple's competitors' own app stores on their Apple devices. Nevertheless, if Apple is found to exhibit characteristics of a dominant position in the markets for apps (and particularly the market for apps for Apple devices), such as Apple's market share being enough for it to be considered dominant, then perhaps its refusal to allow the WikiLeaks app could be characterised as an abuse of this dominant position, in particular a refusal to deal or supply

In the EU, a refusal to supply, while not explicitly listed in Art 102 TFEU (which prohibits abuse of a dominant position), has been recognised as an abusive practice in the case law. Firstly, it would have to be shown that Apple possesses a dominant position, which is defined in the *United Brands* case as containing two elements: an ability for the undertaking to prevent competition and to behave independently of its competitors, customers and consumers. Apple in its position of control over its App Store would appear to occupy such a position. However, the relevant market must also be defined over which Apple is dominant – this could be the market for providing apps for Apple devices. Indeed, for Apple devices which have not been 'jailbroken' Apple is the only player in this market, whereas for Apple devices which have been jailbroken there are other app providers, so an analysis would have to be made of the extent to which Apple is dominant by e.g. looking at market share. Alternatively, the market for apps could be considered a sub-market, as in the *Kodak* case, in which consumers who have bought the main product e.g. an iPad are 'locked in' to the 'sub-market' i.e. apps from the App Store. Even if Apple is not dominant in the 'primary' market for devices, it could well be judged to be dominant in the sub-market.

Nevertheless, on the assumption that Apple is dominant in both markets or at least it is dominant in the (sub)market for Apps (which would seen *prima facie* to be the case), its decision to cease providing access to the WikiLeaks app could be characterised as an anticompetitive refusal to deal. Since the WikiLeaks app was initially available through the App Store, and was then suspended, Apple's action in doing so would thus be the termination of an existing supply relationship, as established in the *Commercial Solvents* decision (as opposed to a refusal to supply a new customer, for which a distinction is made in the case law), resulting in the vertical foreclosure of the WikiLeaks app. Economic harm was suffered (since the WikiLeaks app was being sold through the App Store, with $1 from each download being donated to the WikiLeaks organisation).

In terms of procedure, there could be public enforcement proceedings brought against Apple by the European Commission and/or the national competition authorities, in addition to private enforcement in domestic courts. If the former route is pursued, and Apple is found to have engaged in anticompetitive behaviour infringing Art 102, then large fines can be imposed on Apple by the Commission. Regarding the latter route, Art 102 has direct effect in the legal systems of Member States, and since the ECJ's judgement in *Courage v Crehan*, there has been a right to damages for the breach of this Article in the legal systems of Member States. The WikiLeaks app may wish to seek injunctive relief in the form of an injunction to ensure access as an alternative to damages.

As regards the US position, the judiciary there has also developed the concept of refusal to supply, which in some cases constitutes an infringement of the Sherman Act. In light of the decision in *Verzion v Trinko*, it would appear that the American courts would follow a similar approach to their

European counterparts in assessing the anti-competitive behaviour of Apple vis-à-vis the WikiLeaks app.

Angela Daly 1/4/11 18:35
Comment: Query: burden of proof on WikiLeaks app to show that it was competitor with Apple's own services?

Payment processing firms

The other potential source of a competition claim is the behaviour of the payment processing firms (Visa, Mastercard, PayPal and Bank of America) in refusing to provide services to WikiLeaks.

The most evident path to pursue here would be to show a collective dominance abuse by these firms, which in the EU is also contrary to Art 102. In order to show this, firstly the undertakings must together occupy a dominant position in the market, and here the market would be for payment processing (perhaps more specifically Internet-based payment processing). However, for an abuse of collective dominance to exist, there would have to be a 'link' between the firms i.e. some sort of agreement to behave in this way. This would have to be shown, although the 'agreement' could even be one of the payment firms telling the others that it was going to cease authorising payments to WikiLeaks. In the absence of such an agreement being able to be shown, some sort of oligopolistic interdependence between the firms could be argued, but the fact that another payment firm, Xipwire, managed to ensure that WikiLeaks could still receive payments would suggest that there were low entry barriers to this market, and so the argument of oligopolistic interdependence would not hold.

As regards US antitrust law, it would seem to be more difficult than in EU competition law to show an abuse of collective dominance, as this concept is less developed there as compared to Europe.

Contract and tort

Given the nature of the agreements between WikiLeaks and the entities providing it with services, WikiLeaks may find it easier to obtain remedies in the traditional private law areas of contract and tort.

In the US context, Benkler recognises contractual actions as a possible route for WikiLeaks, based on a wrongful denial of service. He argues that the best path to take would be to argue that in the contracts WikiLeaks had with the commercial service providers, there was an implied contractual obligation not to withhold service unreasonably or without good faith, and that the obligation of good faith may be a sufficient basis for a court to examine the conduct of these service providers and sanction them for 'cutting off critical services to a client where that is done in order to suppress their speech'.

Benkler also considers the possibility of a US tort action, in particular the behaviour of these service providers being a tortious interference with the prospective economic advantage of WikiLeaks, but he acknowledges that it may be tenuous to demonstrate the economic advantage part of this for 'voluntary organizations' such as WikiLeaks. Nevertheless, this may be easier to demonstrate as regards the payment processing organisations since their ceasing of providing services to WikiLeaks was evidently aimed at preventing WikiLeaks from receiving donations which fund the organisation.

As regards the European picture, WikiLeaks would have to seek remedies in national courts (since contract and tort are still legal regimes mainly pertaining to the Member States' jurisdiction as opposed to coming under codifying, harmonising Europe-wide instruments). An interesting development in the contract law of some European countries (especially Germany, the Netherlands and the United Kingdom) is the process of 'constitutionalisation' of this area of law through the

increasing application of fundamental rights to this regime. Thus, for example in proceedings for breach of contract between two private parties, it could be argued that the court should adjudicate the dispute in a way which protects fundamental rights. So in proceedings in such jurisdictions, WikiLeaks could argue that since its right to free expression has been infringed by these service providers breaching the contracts they had with WikiLeaks; and so a court adjudicating the breach ought to decide the case in a way which upholds WikiLeaks' right, taking the fundamental right to free expression into consideration when deciding whether the breach of contract was wholly unlawful or could be justified.

5. The postscript to the cables leak: hackers as the avenging angels of online expression?

However, the saga of the corporate response to WikiLeaks did not stop at these corporate cessions of services. Indeed, there was yet a further extra-legal reaction, this time coming from the online hacking community. This section will analyse the hackers' conduct in particular the Anonymous collective, and determine whether corporate power infringing fundamental rights can be checked in this way, and whether hackers really are defenders of online free expression.

5.1 Anonymous e-vengeance: hackers strike back

In its own response to the corporate response to WikiLeaks in cutting off services, the Internet hacking community started to attack the websites of various of the corporate actors involved in this conduct, primarily under the 'Anonymous' umbrella. Anonymous is a decentralised, organised collective of hackers which acts in concert in an anonymous fashion, and over the last few years its focus has been actions promoting Internet freedom in general and freedom of expression online in particular. Anonymous's attention turned to the WikiLeaks controversy, and in particular the cessation of services from the payment firms under the moniker "Operation Avenge Assange", a substrand of Anonymous's broader "Operation Payback", which originally comprised distributed denial of service (DDoS) attacks on opponents of piracy on the Internet, based on the fact they were infringing what Anonymous loosely considers as Internet freedom. In a statement on a website used by Anonymous, the collective claimed its extension of Operation Payback to attacking WikiLeaks' former service providers (particularly PayPal, which the statement explicitly mentions) was due to the censorious affront to online speech that these cessations of service represented [Correll, 2010].

After the announcement of the Operation Avenge Assange campaign, there was a number of DDoS attacks on the websites of the payment processing firms (and also EveryDNS, on 7 December 2010): Mastercard and Visa's websites were attacked on 8 December 2010, and on 9 and 10 December, two PayPal websites (thepaypalblog.com and api.paypal.com [port 443], respectively) were attacked, all being successfully brought down i.e. unavailable to Internet users for varying periods of time, which disrupted the companies' services as a result [Addley and Halliday, 2010]. There was also an unsuccessful attack on Amazon's website, which was aborted due to the fact it did not have an impact on the performance of Amazon's website due to its huge web-hosting capacity [Mutton, 2010].

5.2 Hackers as David against the corporate Goliath in the fight for online free expression?

Certainly, the actions of the decentralised yet coordinated hackers against the corporations which cut off services to WikiLeaks did manage to cause at least some disruption to the normal functioning of these entities, and gained a lot of publicity in doing so, compounding the negative

media image of the companies. Indeed, Anonymous itself seems to have 'come of age', transitioning from 'cyberpranksters' to full-blown 'hacktivists', using the same technical tools as industrial hackers for more explicitly political or ideological campaigns which are able to cause more damage to the systems of the targets [Cohen, 2010].

However, hacker groups such as Anonymous, especially given its seemingly horizontal control structure, are by their nature arbitrary: as regards free expression, it happens to be that they are affronted by the *de facto* restrictions on this right being exercised by WikiLeaks and its users, but they could easily shift their focus to another topic entirely, or act in a way themselves that infringes free expression, or other fundamental rights such as privacy. As regards the protection of free expression, or actions against infringers, hacker groups are not accountable or reliable in conducting these activities.

Furthermore, hackers themselves could be considered to be a type of "cyber-elite", or 21st century "digerati", since they have the technical power to conduct these kinds of cyber-attacks, and so require a certain amount of technical expertise, which may be beyond the skills of most normal Internet users. However, in order to participate in these recent attacks coordinated via Anonymous, less technical knowledge seems to be necessary, so less technically-literate users can get involved – indeed, in some cases users merely needed to download a programme from one of the Anonymous websites and press 'Run' once they had done so in order to participate. Nevertheless, the less technically literate seem not to be so competent in covering their electronic tracks when participating in such initiatives (which would seemingly fall under the criminalisation of this conduct in various countries as constituting misuses of computing equipment), and there may yet be a distinction based on technical expertise inasmuch as the more sophisticated hackers are less likely to be apprehended by law enforcement agencies as they can 'anonymise' more effectively their online activity.

Nevertheless, the hackers' response to the WikiLeaks saga shows that these Internet corporations are not entirely unstoppable behemoths in their conduct affecting free expression. While the legal regimes in place in the US and Europe may not provide wholly adequate remedies for free speech violations by private actors, the hackers' activity shows that there are extra-legal, civil society-based means of expressing discontent at such infringements, and indeed ways of 'punishing' violators. However, the problems with this approach is the 'mob justice' nature of entities such as Anonymous, with their lack of accountability, legitimacy and reliability, and so they cannot be considered as sustainable and fair means of enforcing and protecting free expression on the Internet vis-à-vis corporations.

5.3 Conclusion

So, where does all of this leave online free expression? The corporate response to WikiLeaks' release of the US embassy cables highlights the fact that the current conceptions of free expression are inadequate for the Internet context, where expression depends on an increasingly privatised sphere. As has been seen with the counter-action from Anonymous, there has been a thankful coincidence that there is some reproach for the corporations' behaviour from the hacking community – but, as detailed above, this is arbitrary, unreliable and capricious, as well as not preventing any similar future action in the same vein.

Pragmatically, entities such as WikiLeaks still retain the possibility of jurisdiction-shopping for the most favourable (virtual or physical) climate for online free expression e.g. by using servers based in such a jurisdiction, and engaging the services of companies also based there. For the continued and future enjoyment of free expression online, there is some hope on the horizon in the form of

schemes such as Iceland's Modern Media Initiative, which provides various legal guarantees and protections for freedom of information and expression online, and was in fact endorsed by WikiLeaks itself.

Acknowledgements

The author would like to thank Benjamin Farrand and Giorgio Monti for their helpful and insightful comments on this piece.

References

http://loganleger.com/apple-app-store-antitrust
Amazon Web Services message. Available at: http://aws.amazon.com/message/65348
Chloe Albanesius *Apple Pulls WikiLeaks App from App Store* PC Mag 21 December 2010. Available at: http://www.pcmag.com/article2/0,2817,2374592,00.asp
http://twitter.com/wikileaksapp
Nelson D. Schwartz *Bank of America Suspends Payments to WikiLeaks* New York Times 18 December 2010. Available at: http://www.nytimes.com/2010/12/19/business/global/19bank.html?_r=1
BBC News *Cyber attack forces Wikileaks to change web address* 3 December 2010. Available at: http://www.bbc.co.uk/news/world-us-canada-11907641
Declan McCullagh *MasterCard pulls plug on WikiLeaks payments* Cnet News 6 December 2010. Available at: http://news.cnet.com/8301-31921_3-20024776-281.html
PayPal Statement regarding WikiLeaks 3 December 2010. Available at: https://www.thepaypalblog.com/2010/12/paypal-statement-regarding-wikileaks/
Lauren Indvik PayPal Halts Donations to Defense Fund for WikiLeaks Source Bradley Manning Mashable 25 February 2011. Available at: http://mashable.com/2011/02/24/paypal-bradley-manning/
PayPal Statement on Courage to Resist Situation PayPal blog 24 February 2011. Available at: https://www.thepaypalblog.com/2011/02/paypal-statement-on-courage-to-resist-situation/
Elisa Fink *Why we removed the WikiLeaks visualizations* Tableau Software website 2 December 2010. Available at:http://www.tableausoftware.com/about/blog/2010/12/why-we-removed-wikileaks-visualizations
BBC News Wikileaks' Visa payments suspended 7 December 2010. Available at: http://www.bbc.co.uk/news/business-11938320
Associated Press *No proof WikiLeaks breaking law, inquiry finds* Salon 26 January 2011. Available at: http://www.salon.com/news/politics/war_room/2011/01/26/wikileaks_not_breaking_law/index.html
Birnhack, Michael D. and Elkin-Koren, Niva, The Invisible Handshake: The Reemergence of the State in the Digital Environment. Virginia Journal of Law & Technology, 2003. Available at SSRN: http://ssrn.com/abstract=381020 or doi:10.2139/ssrn.381020
Charles Arthur WikiLeaks cables visualisation pulled after pressure from Joe Lieberman The Guardian 3 December 2010. Available at: http://www.guardian.co.uk/world/blog/2010/dec/03/wikileaks-tableau-visualisation-joe-lieberman
Amazon Severs Ties With WikiLeaks 1 December 2010, Website of Senator Joe Lieberman (CT). Available at: http://lieberman.senate.gov/index.cfm/news-events/news/2010/12/amazon-severs-ties-with-wikileaks
Ewen MacAskill WikiLeaks website pulled by Amazon after US political pressure *The Guardian* 2 December 2010. Available at: http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon?INTCMP=SRCH
BBC News Wikileaks release of embassy cables reveals US concerns 28 November 2010. Available at: http://www.bbc.co.uk/news/world-us-canada-11858895
David Jackson Obama aides condemn WikiLeaks; Obama orders review USA Today 29 November 2010. Available at: http://content.usatoday.com/communities/theoval/post/2010/11/obamas-team-faces-sensitive-diplomacy-over-wikileaks/1
Tom Curry McConnell optimistic on deals with Obama MSNBC 5 December 2010. Available at: http://www.msnbc.msn.com/id/40517039/ns/politics/40516927
Peter Beaumont WikiLeaks demands Google and Facebook unseal US subpoenas *The Guardian* 8 January 2011. Available at: http://www.guardian.co.uk/media/2011/jan/08/wikileaks-calls-google-facebook-us-subpoenas
Herman and Chomsky Manufacturing Consent: The Political Economy of the Mass Media 1988

Michael Birnhack and Niva Elkin-Koren WikiHunt and the (in)visible handshake openDemocracy 20 February 2011. Available at: http://www.opendemocracy.net/michael-birnack-niva-elkin-koren/wikihunt-and-invisible-handshake
Rebecca MacKinnon WikiLeaks, Amazon and the new threat to internet speech *CNN* 2 December 2010. Available at: http://articles.cnn.com/2010-12-02/opinion/mackinnon.wikileaks.amazon_1_wikileaks-founder-julian-assange-lieberman-youtube?_s=PM:OPINION
Joe Petrucci Philly mobile payment startup Xipwire collecting donations for WikiLeaks *Flying Kite* 7 December 2010. Available at: http://www.flyingkitemedia.com/features/xipwirewikileaks1207.aspx
Vincent Dekker Zorgen over dominantie Visa en Mastercard in Europa Trouw 9 December 2010. Available (in Dutch) at: http://www.trouw.nl/tr/nl/4324/Nieuws/article/detail/1800653/2010/12/09/Zorgen-over-dominantie-Visa-en-Mastercard-in-Europa.dhtml
Zeno-Zencovich "La Liberta d'espressione Media, mercato, potere nella società dell'informazione" Il Mulino, Bologna 2004
Yemini "Mandated Network Neutrality and the First Amendment: Lessons from *Turner* and a New Approach". Virginia Journal of Law and Technology, 2008. Available at SSRN: http://ssrn.com/abstract=984271
Benkler A Free Irresponsible Press, forthcoming Harvard Civil Rights-Civil Liberties Law Review 2011. Available at: http://www.benkler.org/Benkler%20Wikileaks%20CRCL%20Working%20Paper%20Feb_8.pdf
Ardiyok, Sahin, Comparative Analysis of Collective Dominance (July, 17 2008). Journal of Yeditepe University Faculty of Law, Vol. 3, No. 1, 2006. Available at SSRN: http://ssrn.com/abstract=1162187
Although due to the decentralised nature of Anonymous it is conceptually and practically difficult to define a single 'official' website. However, the two main websites for Anonymous or at least portals at the time of writing seem to be http://anonops.net/ (and associated Twitter feed) and http://hbgary.anonleaks.ch/
Sean-Paul Correll *Operation:Payback broadens to "Operation Avenge Assange"* PandaLabs Blog 6 December 2010. Available at: http://pandalabs.pandasecurity.com/operationpayback-broadens-to-operation-avenge-assange/
Esther Addley and Josh Halliday WikiLeaks supporters disrupt Visa and MasterCard sites in 'Operation Payback' Guardian 9 December 2010. Available at: http://www.guardian.co.uk/world/2010/dec/08/wikileaks-visa-mastercard-operation-payback
Paul Mutton Operation Payback aborts attack against Amazon.com Netcraft 9 December 2010. Available at: http://news.netcraft.com/archives/2010/12/09/operation-payback-aborts-attack-against-amazon-com.html
Noam Cohen Web Attackers Find a Cause in WikiLeaks New York Times 9 December 2010. Available at: http://www.nytimes.com/2010/12/10/world/10wiki.html
Icelandic Modern Media Initiative. Website in English available at: http://immi.is/?l=en

[1] "Digerati" is a term coined in the early days of the publicly-available Internet to describe users who were highly skilled in the processing and manipulation of digital information. The term seems to have fallen out of use in recent times. See: http://en.wikipedia.org/wiki/Digerati