International Journal of Communication 8 (2014), Feature 2693–2703 1932–8036/2014FEA0002

Internet Privatization, WikiLeaks, and Free Expression

ANGELA DALY
European University Institute, Italy
Swinburne University of Technology, Australia

Introduction

In late 2010, the online nonprofit media organization WikiLeaks published classified documents detailing correspondence between the U.S. State Department and its diplomatic missions around the world, numbering around 250,000 cables. These diplomatic cables contained classified information with comments on world leaders, foreign states, and various international and domestic issues. Negative reactions to the publication of these cables came from both the U.S. political class (which was generally condemnatory of WikiLeaks, invoking national security concerns and the jeopardizing of U.S. interests abroad) and the corporate world, with various companies ceasing to continue to provide services to WikiLeaks despite no legal measure (e.g., a court injunction) forcing them to do so.

This article focuses on the legal remedies available to WikiLeaks against this corporate suppression of its speech in the U.S. and Europe since these are the two principle arenas in which the actors concerned are operating. The transatlantic legal protection of free expression will be considered, yet, as will be explained in greater detail, the legal conception of this constitutional and fundamental right comes from a time when the state posed the greater threat to freedom. As a result, it is not generally enforceable against private, non-state entities interfering with speech and expression which is the case here. Other areas of law, namely antitrust/competition, contract and tort will then be examined to determine whether WikiLeaks and its partners can attempt to enforce their right indirectly through these other means. Finally, there will be some concluding thoughts about the implications of the corporate response to the WikiLeaks embassy cables leak for freedom of expression online.

The Corporate Response

In the immediate aftermath of WikiLeaks' release of U.S. embassy cables and the accompanying condemnation from U.S. politicians, some companies stopped providing services to WikiLeaks. Broadly speaking, these were either payment-processing firms that refused to continue to process payments destined for WikiLeaks (Bank of America, MasterCard, PayPal, and Visa) or companies that technically supported WikiLeaks by hosting its website (Amazon.com's Amazon Web Services and EveryDNS) or by providing visualization software to see the leaked cables better (Tableau Software). In addition, Apple

removed from sale in its App Store an app created by Igor Barinov, a developer not associated with WikiLeaks, which was described as giving instant access to WikiLeaks material, with $1 from every app purchased given to WikiLeaks.

The corporations gave various reasons for why they had reacted this way. Some firms—such as Amazon.com, Bank of America, PayPal, Tableau Software, and Visa—claimed that WikiLeaks had violated their terms of services, usually claiming that what WikiLeaks was doing was illegal or that it did not have rights over the material it had put on its website. MasterCard specifically stated that it had ceased to provide services because WikiLeaks was engaging in illegal activity (although no legal or judicial authority had come to that conclusion). EveryDNS claimed that the wikileaks.org site had become the target of several distributed denial-of-service attacks, which EveryDNS claimed threatened the stability of its infrastructure. Apple gave no reason at all for removing the WikiLeaks app from its App Store.

Tableau Software claimed that, in addition to a potential violation of its terms of service by WikiLeaks, the company had stopped providing services to WikiLeaks after receiving a (nonbinding) request from Senator Joe Lieberman, the chairman of the Senate Homeland Security Committee, calling for organizations providing services to WikiLeaks to terminate their relationship with the website. Furthermore, although not acknowledged officially, *The Guardian* also claimed that Amazon was under "heavy political pressure" to stop hosting WikiLeaks (MacAskill, 2010).

WikiLeaks' Legal Recourse

Despite the withdrawal of the services outlined above, and although its functioning was made much more difficult, WikiLeaks was still accessible online at the time of these events through the use of mirror sites (such that even if WikiLeaks' original providers ceased to host it, it was still accessible) and mobile payment company Xipwire, which facilitated another route by which WikiLeaks could receive donations. Nevertheless, the continued blockade by the payment-processing firms appears to have had a devastating effect on WikiLeaks, because it suspended activities on its website in 2011, giving the reason that the blockade has "destroyed 95% of our revenue" (WikiLeaks, 2011). The situation improved somewhat in 2013 when the Icelandic Supreme Court ordered payment service Valitor to recommence processing payments to WikiLeaks, and MasterCard also reversed its position (WikiLeaks, 2013).

In practice, WikiLeaks suffered an attack on its freedom of expression, and, arguably, its users also experienced violations in terms of their freedom to receive information as a result of these corporations' behavior. The next section examines the legal options open to WikiLeaks and its partners to challenge this state of affairs, with a jurisdictional focus on the United States and Europe, because most of the actors involved—whether government, corporate, civil society, or individuals—are located in these regions.

Free Expression

Free expression is protected by the First Amendment to the U.S. Constitution and by Article 10 of the European Convention on Human Rights (ECHR). The First Amendment has traditionally been conceived

of as a right enforceable against the U.S. government, as opposed to a right enforceable against private parties such as corporations. Indeed, one way in which the U.S. and European conceptions of free speech differ is that, in the United States, not only is the First Amendment not enforceable against private entities such as corporations but such entities are entitled to free expression as well. The European approach centers more on the individual, 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.

Under the U.S. regime, WikiLeaks enjoys the protection of the First Amendment, guaranteeing free speech, and receives this protection even if an illegal act was committed by, for example, the person who leaked the information containing the embassy cables to WikiLeaks. However, this protection is only effective against prosecution by the U.S. government. The case at hand does not involve direct governmental interference with WikiLeaks' free expression, but rather interference from other private entities, at least some of which seems to be motivated by extrajudicial pressure from the U.S. government to act in this way. However, the lack of formalization of the U.S. government's conduct here, and its indirect and subtle nature, would appear to make a direct case against the government impossible—or, at the very least, extremely difficult.

The corporations cutting off services to WikiLeaks are also likely entitled to exercise their right to free expression by, for example, deciding to no longer provide their services to WikiLeaks. Not only would a direct action against the corporations be impossible according to the current conception of the First Amendment, but their conduct may also enjoy protection.

The limitations of this conception of the right to free expression in the Internet environment have been recognized in the literature. Yemini (2008)—writing in the context of the net neutrality debate but with conclusions on this issue that 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 (U.S.) 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 the right to free expression, subject to regulation on that basis, or indeed proceedings for infringement of the right. Yet much of the applications layer of the Internet is similarly owned and controlled by private entities that can exert their power in ways that are not in accordance with free expression.

The situation in Europe differs somewhat. Article 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 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 programs against the terms of the tenancy agreement. In this case, the European Court of Human Rights found that the applicants' freedom to receive information via satellite broadcast, which formed part of Article 10, had been violated, because the

state, Sweden, had "failed in their positive obligation to protect that right." 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 that refused to host WikiLeaks. However, because the WikiLeaks website migrated to different servers and mirror sites of WikiLeaks appeared in other locations on the Internet, these attempts to shut down WikiLeaks and prevent users from accessing the information contained in the leaks did not work. The fact that users could still see this information suggests too that the court would not find that users' rights to receive information had been violated. In any event, again through the ECHR apparatus, the corporations cannot be directly censured for their actions.

Indeed, the situation in both the United States and Europe indicates that it would be highly problematic for WikiLeaks to defend legally its right to free expression. As Birnhack and Elkin-Koren (2011) have observed, whereas the U.S. government would be standing on "shaky legal ground" regarding interference with WikiLeaks for publishing this material due to First Amendment protection, 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—and one less susceptible to legal challenge.

The issue of the inadequacies of the legal protection of free expression online extends beyond the scope of this particular incident involving WikiLeaks, and even beyond the net neutrality debate. The fact of private entities' control over the Internet in developed jurisdictions such as the United States and Europe and their ability to affect in whatever way the information disseminated over it gives general cause for concern over civil liberties online. As MacKinnon puts it, "What is troubling and dangerous is that in the Internet age, public discourse increasingly depends on digital spaces created, owned and operated by private companies" (2010, para. 4).

Other Legal Regimes

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 are explored in the next section. Private law may prove more fruitful than the legal protections of free expression, because the relationship between Internet users (whether organizations such as WikiLeaks or individuals) and the 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.

Competition Law

Competition law (or "antitrust") may provide some respite to WikiLeaks by pursuing either the payment-processing firms as a cartel or oligopoly or by alleging an abuse of Apple's dominant position.

Regarding the payment-processing firms' (Visa, MasterCard, PayPal, and the Bank of America) refusal to process payments for WikiLeaks, if what WikiLeaks has stated is true, then the companies' action to block funds to WikiLeaks has dramatically reduced the possibility of donating to the organization, with devastating effects for WikiLeaks' functioning. Although the initiative to Xipwire to facilitate payments to WikiLeaks indicates no or low entry barriers to this market, this may be proved to be an entirely insignificant gesture because WikiLeaks still cannot receive adequate remuneration for its activities.

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 when combined, can be demonstrated by the legal proceedings against the two companies in both the United States and the European Union for anticompetitive behavior due to their large market shares. Furthermore, in light of Visa and MasterCard 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 U.S. influence over the blocking of payments from European citizens to a European organization—that is, WikiLeaks.

Indeed, in July 2011, DataCell (a service provider assisting WikiLeaks) filed a complaint with the European Commission alleging that the "coordinated action" of the payment-processing firms constituted a violation of European competition law (DataCell, 2011).

DataCell argued that the refusal by the payment-processing firms to grant it access to their respective payment card networks was anticompetitive, because they constituted a cartel harming competition contrary to Article 101 of the Treaty of the Functioning of the European Union (TFEU) and/or because they abused an individual or collective dominant position, contrary to Article 102 TFEU.

However, the European Commission issued a preliminary decision in late 2012 to the effect that the Commission would not pursue this matter any further since it believed that "[t]he likelihood of establishing the existence of an infringement of Articles 101 or 102 TFEU in this case appears limited" (European Commission, 2012, p. 5). The Commission considered that, regardless of whether the group of firms formed a cartel, or had an individual or collective dominant position, their conduct was not anticompetitive since their conduct only meant that DataCell was not permitted to process payments to WikiLeaks, but could continue its services for other customers. Even if DataCell exited the relevant market (for payment facilitation services) because it refused to agree not to provide WikiLeaks with services and so was not permitted to process other payments, this was unlikely to have negative effects for competition overall on that "global and fragmented" market (p. 9). Furthermore, the Commission accepted that the payment-processing firms probably had an objective justification for restricting competition under Articles 101 and 102 TFEU, namely to "eliminate the risk of criminal liability or harm to the schemes' brands" (p. 14), presumably from the association with WikiLeaks' controversial (yet not actually illegal) activities. Implicit in the Commission's reasoning is the idea that competition law does not protect competitors *per se*: so long as the market overall was competitive, then DataCell's potential exit from it was not of particular concern, even at the hands of enormous corporations.

No action concerning alleged anticompetitive behavior on the part of the payment-processing firms has been taken to date in the United States.

In addition, no action has been taken against Apple, but the monopolistic position of the company over its App Store and its removal of the WikiLeaks app in the wake of the controversy over the U.S. embassy cables leak may constitute anticompetitive behavior. Unless users of Apple's iPad, iPhone, and iPod Touch platforms jailbreak the device, they can only run programs approved by Apple and available via the App Store. Jailbreaking one of these devices would be prima facie illegal in the United States under the Digital Millennium Copyright Act (DMCA) as violating copyright law; however, jailbreaking a smartphone has been recognised as an exception to the DMCA anti-circumvention rules, but jailbreaking tablets does not fall within this permission (Hofmann and McSherry, 2012) . Nevertheless, this 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 favor 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.

Apple would need to be shown to be a dominant entity. It has complete control over the apps that appear in its App Store even if the apps are created by other companies or individuals, and so the company 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 phone devices has been ruled to be legal in the United States (but not for iPads) and is permitted in the EU, consumers can also choose to run apps on their Apple devices from Apple's competitors. 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 that Apple's market share is large enough for it to be considered dominant, then perhaps its refusal to allow the WikiLeaks app could be characterized as an abuse of this dominant position—in particular, a refusal to deal or supply.

In the EU, a refusal to supply, although not explicitly listed in Article 102 of the TFEU (which prohibits abuse of a dominant position), has been recognized as an abusive practice in the case law. First, 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 over which Apple is dominant also must be defined; this could be the market for providing apps for Apple devices. Indeed, for Apple devices that have not been jailbroken, Apple is the only player in this market, whereas for Apple devices that have been jailbroken, other app providers exist. Thus, an analysis would have to be made of the extent to which Apple is dominant by looking at market share. Alternatively, the market for apps could be considered a submarket, in which consumers who have purchase the main product—for example, an iPad—are locked in to the submarket of 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 submarket.

On the assumption that Apple is dominant in both markets or at least dominant in the (sub)market for apps (which would seem prima facie to be the case), its decision to cease providing access to the WikiLeaks app could be characterized as an anticompetitive refusal to deal. Since the WikiLeaks app was initially available through the App Store and was then suspended, Apple's action would 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 because the WikiLeaks app was being sold through the App Store, with $1 from each download being donated to the WikiLeaks organization.

However, alternative means of distribution, even if they fall into different markets, do exist—the app could be distributed through the Android Store, for instance. In *Bronner*, the availability of such alternatives led to the finding that there was not an essential facility, and the same conclusion might be reached here. In any event, an "objective justification" for what might otherwise be anticompetitive conduct on Apple's behalf might be found again regarding liability for possibly illegal activities and/or the damage to Apple's brand that making such an app available might cause, like in the DataCell scenario.

The U.S. judiciary has developed the concept of refusal to supply, which in some cases constitutes an infringement of the Sherman Act. In light of the decision in *Verizon v. Trinko,* the U.S. courts might follow a similar approach to their European counterparts in assessing the anticompetitive behavior of Apple *vis-à-vis* the WikiLeaks app.

Thus, competition law may, in theory, be able to provide remedies to WikiLeaks and its partners that would go some way toward correcting the infringements of its freedom of expression. Yet the European Commission's preliminary decision in the DataCell case demonstrates the difficulties of relying on competition law alone to provide solutions to what is essentially an issue of free expression. This case also demonstrates the Commission's willingness to defer to the payment-processing firms' concerns about their liability and public image from association with WikiLeaks. In any event, these scenarios show that the existence of a monopolistic or oligopolistic market worsens the circumstances for exercising the right to free expression on the Internet; in such a market, users are even more restricted in seeking an alternative provider in the form of a genuine competitor to the company or companies acting in a way to restrict their free expression online.

Contract and Tort

There may be avenues open to WikiLeaks to seek redress for the infringements to its right to free expression in contract and tort due to the private law nature of the agreements it had with the corporations providing it with services.

In the U.S. context, Benkler (2011) recognizes 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" (p. 369).

Benkler also considers the possibility of a U.S. tort action—in particular, the behavior 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 for the payment-processing organizations, because their ceasing to provide services to WikiLeaks was evidently aimed at preventing WikiLeaks from receiving donations that fund the organization.

In 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, harmonizing, 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 constitutionalization 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 that protects fundamental rights. In proceedings in such jurisdictions, WikiLeaks could argue that its right to free expression has been infringed by these service providers breaching their contracts with WikiLeaks; and a court adjudicating the breach ought to decide the case in a way that 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.

In practice, contract law has proved the most fruitful for WikiLeaks and its associated providers. Alongside the complaint to the European Commission over the alleged anticompetitive behavior of the payment-processing firms, WikiLeaks and DataCell initiated proceedings in Denmark for an alleged violation of Danish merchant law due to the termination of the payment services and refusal to reinstate them (the forum being chosen seemingly due to the fact that Teller, a company licensed to process transactions on behalf of Visa and MasterCard, is based in Denmark). In addition to this, as mentioned at the beginning of this piece, DataCell successfully challenged the suspension of financial services by Valitor (formerly Visa Iceland), with the Icelandic Supreme Court holding that Valitor must honor its contract with DataCell and recommence processing card payments destined for WikiLeaks or else face a penalty of almost US$7000 per day (Valdimarsson, 2013).

Conclusion

The corporate response to WikiLeaks' release of U.S. embassy cables highlights the fact that the current conceptions of free expression are inadequate for the Internet context, where expression depends on an increasingly privatized sphere. Constitutional and treaty protections of free expression—such as the First Amendment to the U.S. Constitution and Article 10 of the European Convention on Human Rights—cannot provide appropriate protection against violations by corporations. Although other areas of law, may

provide some relief to WikiLeaks, these systems cannot do so entirely, especially since the protection of fundamental rights is not their objective—or at least not their main objective.

Pragmatically, entities such as WikiLeaks retain the possibility of jurisdiction shopping for the most favorable (virtual or physical) climate for online free expression—for example, by using servers based in such a jurisdiction and engaging the services of companies 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.

References

Benkler, Y. (2011). A free irresponsible press: WikilLaks and the battle over the soul of the networked fourth estate. *Harvard Civil Rights-Civil Liberties Law Review*, *46*(2), 311–397.

Birnhack,M., & Elkin-Koren, N. (2011, February 20). WikiHunt and the (in)visible handshake. *openDemocracy*. Retrieved from http://www.opendemocracy.net/michael-birnack-niva-elkin-koren/wikihunt-and-invisible-handshake

DataCell. (2011, July 2). Legal action by DataCell and WikiLeaks against Visa and MasterCard [Press release]. Retrieved from http://www.datacell.com/news/2011-07-02/legal_action_by_datacell_and_wikileaks_against_visa_and_mastercard

European Commission. (2012, October 25). Letter to DataCell regarding Case COMP/39921 – Datacell/Visa & Mastercard. Retrieved from https://wikileaks.org/IMG/pdf/EUPreliminaryDecision1.pdf

Hofmann, M., & McSherry, C. (2012, November 2). The 2012 DMCA Rulemaking: What we got, what we didn't, and how to improve the process next time. *EFF.org*. Retrieved from https://www.eff.org/deeplinks/2012/11/2012-dmca-rulemaking-what-we-got-what-we-didnt-and-how-to-improve

Istituto Chemioterapico Italiano S.p.A. and Commercial Solvents Corporation v. Commission, Joined Cases 6/73 & 7/73, 1974 E.C.R. 223, [1974] 1 C.M.L.R. 309.

Khurshid Mustafa and Tarzibachi v. Sweden (2008, December 16). EctHR

MacAskill, E. (2010, December 2). WikiLeaks website pulled by Amazon after US political pressure*. The Guardian.* Retrieved from http://www.theguardian.com/media/2010/dec/01/wikileaks-website-cables-servers-amazon

MacKinnon, R. (2010, December 3). WikiLeaks, Amazon and the new threat to Internet speech. *CNN.com*. Retrieved from http://edition.cnn.com/2010/OPINION/12/02/mackinnon.wikileaks.amazon

Oscar Bronner GmbH & Co. KG v. Mediaprint Zeitungs- und Zeitschriftenverlag GmbH & Co. KG, Case C-7/97, 1998 E.C.R. I-7791, (1999). 4 C.M.L.R. 112.

United Brands Co. v Commission for the European Communities, Case 27/76 [1978] ECR 207.

Valdimarsson, O. R. (2013, April 25). Iceland's top court orders Valitor to process Wikileaks payments. *Bloomberg*. Retrieved from http://www.bloomberg.com/news/2013-04-24/iceland-s-top-court-orders-valitor-to-process-wikileaks-payments.html

Verizon Communications v.Law Offices of Curtis V. Trinko, LLP 540 U.S. 398. (2004).

WikiLeaks (2011, October 24). Banking blockade. Retrieved from http://wikileaks.org/Banking-Blockade.html

WikiLeaks. (2013, July 3). MasterCard breaks ranks in WikiLeaks blocade. Retrieved from https://wikileaks.org/MasterCard-breaks-ranks-in.html

Yemini, M. (2008). Mandated network neutrality and the First Amendment. Lessons from Turner and a new approach. *Virginia Journal of Law and Technology, 13*(1), 1–38.