Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous

TOM SORELL*

Abstract

Traditional human rights concepts seem to fit Internet activity when it is broadly allied to conventional political mobilization and when it occurs in human rights-violating jurisdictions. Traditional concepts are strained, however, when Internet activity takes the unconventional form of 'hacktivism', and it occurs in human-rights respecting jurisdictions. Hacktivism is still activism but not always open or democratic activism. Unlike more familiar forms of activism, hacktivism can often be anonymous, sometimes gratuitously so, and can operate with a kind of impunity that its technology seems to afford. Hacktivism is sometimes also claimed to serve interests that transcend those of particular states, that is, the interests of the global population generally. But this claim is implausible if hacktivism is not accountable to anyone. Taking the cases of Wikileaks and Anonymous, I argue that some of the activities of these groups are highly questionable, and that forms of cyberactivism more strongly connected with public displays of protest and legally accountable disclosure are morally superior and cohere better with human rights. This line of thought is, admittedly, easier to articulate in the case of Wikileaks than in the case of Anonymous, whose free-form set of causes and swarm activity are not always attributable to a stable collective entity. The activities of these two groups are chosen for four reasons: because they are both prominent in hacktivism; because they together represent quite a lot of the spectrum of hacktivism; because they have operated at times in concert, and because, in the case of Wikileaks at least, the rationale for its activity is sometimes stated in the language of human rights.

Keywords: anonymity; cyberactivism; freedom of expression; impunity

Hacktivism is a form of political activism in which computer hacking skills are heavily employed against powerful commercial institutions and governments, among other targets. Hacktivism is not always open or democratic—even when it is practised in jurisdictions with strong democratic traditions. When hacktivism is directed against institutions that might also be the target of conventional political opposition, it need not be backed by consensus-building. It is not always easy to know how many people support a cause promoted by hacktivists, or whether even more than a few people do. Many hacktivists seem to be in their teens, and may have little political sophistication. The agents of hacktivism can espouse crude, and sometimes extreme, libertarian ideas: ideas without much of a following among voters in most

* Tom Sorell (t.e.sorell@warwick.ac.uk) is Professor of Politics and Philosophy, University of Warwick, and Director of the Interdisciplinary Ethics Research Group. Previously he was Co-Director of the Human Rights Centre and Professor of Philosophy, University of Essex.

Journal of Human Rights Practice Vol. 7 | Number 3 | November 2015 | pp. 391–410 DOI:10.1093/jhuman/huv012
Advance Access publication September 22, 2015

democratic countries. Perhaps most important, hacktivism is typically anonymous, and several cyber-personas can correspond to just one real activist. Although hacktivists often lack wide political support, they can enjoy significant power. Cyber-expertise can give hacktivists the ability to attack infrastructure, steal commercial secrets, expose classified government information, and spread malware to a large number of commercial, official or even private computers.

Some hacktivism springs from a hacker tradition of extreme irreverence and theatricality. Much of that irreverence started out by being apolitical, and it was once confined to an online hinterland (Bartlett 2014: Chapter 2). In its current forms, however, hacktivism has entered mainstream social media, such as Twitter, and, as we shall see, it has targeted the websites of organizations as varied as the Church of Scientology and the US Department of Defense. Protected by their anonymity, hacktivists can be less inhibited in expressing ideas or abuse, and can be much more impervious to criticism and debate, than people who hold similar beliefs but express and defend them publicly. In short, hacktivism can appear more shadowy, and more the work of fringe groups and outsiders, than traditional forms of activism.

Hacktivism is a kind of cyberactivism. There are many varieties of cyberactivist, but I shall argue that the power of some is illegitimate. Their power is therefore less legitimate than that of the typical democratic state, even when hacktivism is used in ways that seem to resemble ordinary political protest. Cyber-groups and lone cyber-vigilantes, though they appear in some lights to be the sort of agents that human rights ought to protect against the state, can also be among the rogue non-state actors that human rights theory sometimes takes a stand against.[1] Stateless, elusive, sometimes lawless, and almost always anonymous, hacktivists are particularly unaccountable in states that protect privacy and that recognize generously interpreted freedom of expression. They are particularly unaccountable, in other words, in human rights-respecting jurisdictions. These facts may require us to revise the conceptual scheme of human rights by rethinking the connection between being vulnerable and being an individual or a small group: in cyberspace, individuals and small groups can be very powerful.

1 A possible recent example of the activities of rogue non-state actors in cyberspace is the cyber-attack in November 2014 on Sony for its then impending release of the satirical film *The Interview*. Although the attack was attributed to the North Korean government, who were supposedly reacting against the clear modelling of the central character in *The Interview* on the North Korean head of state, the identity of the perpetrators is now in doubt (http://en.wikipedia.org/wiki/Sony_Pictures_Entertainment_hack). The attack was successful for a time in preventing the distribution of *The Interview* and it involved the leaking of commercially valuable information about Sony releases and embarrassing emails. The US government responded to the attack by imposing damaging sanctions on North Korea. If the attack was actually the work of independently operating hackers, as some commentators have suggested, we would have a good illustration of what the activity of rogue non-state actors in cyberspace might be like.

The rest of the article is divided into three sections. In the first, I briefly sketch some of the varieties of cyberactivism, acknowledging a spectrum according to the publicity or lack of publicity of the action. This spectrum stretches from, at one extreme, the action of conventional political parties partly operating from their websites to, at the other extreme, stealthy interventions by lone wolf hacktivist vigilantes. Toward the middle of the spectrum lie the activities of hacktivist groups. I shall consider the activities of two groups in particular: Wikileaks and Anonymous, primarily in human rights-respecting jurisdictions (see also Moore 2011). These groups are chosen because of their relative prominence in cyberactivism; because they together represent quite a lot of the spectrum of cyberactivism outlined in Section 1; and because they have operated at times in concert. Section 2 considers Wikileaks, and Section 3 Anonymous. Some of the activities of these organizations seem to lie outside those that are protected by human rights treaties, and both the organizations and some of their academic supporters claim a kind of exceptionalism for them that I shall argue they don't deserve.

1. Kinds of cyberactivism and human rights

Cyberactivism has a presence in policy and academic literature under two different headings. The first is 'political activism': cyberactivism refers to a form of political mobilization (Chadwick and May 2003) that has only relatively recently become available through computer and smartphone technology. The second heading is 'security'. Cyberactivists are discussed as possible sources of cyberattacks—that is, as possible sources of data-destroying viruses, and as threats to the access and control systems of important civil infrastructure, even military equipment (Nissenbaum 2005; Cavelty 2012: 368). Some of what follows will have implications for security, but the main focus is on cyberactivism as the exercise of civil rights.

Although there are many possible ways of classifying cyberactivism, it is useful to distinguish between, on the one hand, cases in which the Internet is a platform and a medium for political action that is primarily manifested on the street, and, on the other hand, cyberactivism that is mainly carried out on the Internet. Hacktivism is of the latter kind. People associated with it can go public and appear on the streets from time to time, but it is mainly carried out by individuals operating in private, sometimes in secret, and relatively autonomously, albeit according to a shared timetable and a distinctive agenda.

Hacktivists are often concerned with the protection of the Internet as a relatively unregulated and unowned space. Traditionally this took the form of developing and sharing open-source computer code.[2] More recently it has turned to the protection of technology-based cultures that exist primarily on the Internet (Jordan and Taylor 2004: Chapters 1–3). A common preoccupation is with restrictions on downloading music and information, and the limits of anti-

2 For what is arguably a manifesto for cyberactivism see Barlow (1996).

hacking protections used by big businesses or public institutions (Jordan 2000; Jordan and Taylor 1998). A related and perhaps newer concern is with undoing the dominance of the commercial Internet service providers and Internet platforms, and creating alternatives (Milan 2013; Fenton 2012: 154).

Hacktivists can also exploit their technological expertise to challenge the power of companies, states and religious groups whose existence is primarily offline. The medium of hacktivism is often electronic penetration of a protected website or database and the extraction of information. It can be a matter of disabling the hardware or software of a target organization. Or it can take the form of defacing a website. None of these kinds of activity need be connected with street protests, though they are carried out collectively, and sometimes in the name of values—such as national self-determination and the rejection of censorship—that are also defended through street protests. Without a connection to values like these, collectively expressed, hacktivist actions would have little to distinguish them from hacking itself.

If one extreme of cyberactivism is the secret but coordinated electronic attack mounted by a few individuals, the other extreme might be marked by the public use of highly accessible Internet resources—the best known social networking platforms—for the coordination of highly visible mass protests on the streets. At this very public end of cyberactivism, a number of further distinctions can be made. There is a difference between a demonstration and a protest organized by a traditional political party or trade union that happens to have an online presence, and a demonstration or protest that originates from the posts of individuals on social networks (Bennett and Segerberg 2012). What we need to think of in this latter connection is a political event that arises from roughly the same mechanisms as a large-scale 'rave' or a more or less impromptu charity run: individuals self-organized into online interest groups, or simply with large numbers of online 'friends', decide to do something together in physical space to support some shared, possibly short-term, goal, or to stop or protest against some planned activity or measure, either on the part of a local jurisdiction or another civil society grouping.

Examples of cyberactivism along these lines after 2010 come from North Africa (the so-called Tunisian and Egyptian revolutions), Spain (the Indignados movement), Iceland (the kitchen tools protest) and the Occupy movement. The North African examples apart, many varieties of cyberactivism seem to be linked to the financial crisis, and to the perception that governments at the centre of it were subservient to the banks. In North Africa, there appeared to be a reaction against Islamicization as well as the immovability of traditional power structures and institutions, including, in Egypt, the army (Castells 2012).[3] Another, quite different, manifestation of the most

3 To what extent the North African movement was dependent for its success on Western hacktivists in particular and social media in general is a disputed question. Some writers make large claims for the role of Anonymous in the Tunisian revolution (Coleman 2014). Others stress

public cyberactivism is the formation of groups with cyber-expertise whose political platforms put the Internet at the service of democracy (Taylor 2014). The Pirate Party, which has had representatives in the European Parliament as well as the national parliaments of some EU member states, is an example (Erlingsson and Persson 2011). The Pirate Party not only uses the Internet as a channel for its own activity, but also as one of its main legislative topics. In particular, the Pirates oppose the erection of paywalls between individual users of the Internet and literary, musical and video content (Hintz and Milan 2009).[4]

The most public cyberactivism is clearly covered by traditional human rights protections.[5] The reason is that these forms of cyberactivism are essentially connected with street protests, democratic electoral processes, and channels of political communication available to private citizens; and street protests, democratic electoral processes and channels of political communication open to private citizens are paradigms of the things that traditional human rights instruments protect. For example, the International Covenant on Civil and Political Rights (ICCPR)[6] recognizes a range of relevant rights. Article 19 protects freedom of opinion and expression. Paragraph 2 of that article is very inclusive in its protection of the means of expression—so inclusive that it easily covers a kind of technology that came into being long after ICCPR was open for signature. Article 19, paragraph 2 says:

> Everyone shall have the right to freedom of expression; this right shall include the freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

Two further articles are connected with the other identifying marks of public cyberactivism. Article 21 specifically protects street protests, so long as they are peaceful. Finally, article 25 protects the right to direct participation and to democratic representation, including through free and universal elections, in national public life.

domestic blogospheres commenting on well-publicized offline events. For a review of some academic research, see Wihbey (2013).

4 A variety of more informal, less public and less mainstream organizations also try to keep the Internet from being commercialized by offering Internet platforms independent of the commercial giants in this area.

5 There is relatively little literature on the relation between the Internet and human rights. Among the most recent books is Jorgensen (2013). A broadly relevant book, now somewhat dated, is Hicks et al. (2000). Even earlier is Metzl (1996). The UN Human Rights Council adopted a resolution on the protection of online freedom of expression in July 2012; for commentary, see Park (2013). For a (now dated) discussion of freedom of expression on the Internet, mainly in relation to Canada, see Steeves (2000). For more recent discussion, mainly in connection with the United States, see Levmore and Nussbaum (2012).

6 International Covenant on Civil and Political Rights, 16 December 1966 (entered into force 23 March 1976).

There is no doubt that the rights guaranteed by these articles, or at least rights corresponding to these articles, exist and are regularly exercised in many of the liberal jurisdictions associated with cyberactivism. These include Spain, Iceland, and (in the case of the Occupy movement) the UK and the USA. On the other hand, questions can be raised about the strength of those rights in states whose governments have not abided by ICCPR after ratification. Tunisia was an early (1969) ratifier of ICCPR but, prior to 2011, was a notoriously human rights-violating country. Even after 2011, freedom of expression has been seriously curtailed in the Draft Constitution (see Human Rights Watch 2015). Similar remarks apply to Egypt. Although it ratified ICCPR after Tunisia did, it did not abide by articles 19, 21 and 25 before its revolution, and its adherence to article 25 after its revolution is pretty doubtful.

Then there are (the very few) countries that have not yet ratified ICCPR. An example is the People's Republic of China (hereafter 'China'). Although it signed ICCPR in 1998, China has yet to ratify it. Much more importantly, it is far from complying with the relevant obligations. China remains a one-party state, lacks free elections, operates policies of censorship and summary arrest for dissidents, and has been accused of persecuting religious and other minorities. So the constituency[7] for ICCPR is very likely indeed to include Chinese political dissidents and devotees of religion in China. It also includes a very large group of Internet users who have been prevented from expressing heterodox political and other views, and whose access to uncensored sources of information, primarily in the West, has been systematically blocked.[8]

Although the central civil rights of freedom of expression, freedom of assembly and participation in the democratic system are not respected in the

7 I use the term 'constituency' to mean the group who at a time most need the protection of a human right. For example, prior to 2001, Afghan women were part of the constituency for Convention on the Elimination of Discrimination against Women, but Swedish women were not. See Sorell and Landman (2006).

8 In China, access is or has been prevented to websites discussing any of the following: the Dalai Lama, the 1989 crackdown on Tiananmen Square protesters, and Falun Gong, the banned spiritual movement. Again, Internet traffic is monitored for the occurrence of a lengthening list of keywords that are used to profile suspect Internet postings and searches. Social networking sites are blocked. As early as 2008, bans were imposed on Facebook, YouTube and Twitter. In late 2012 new regulations were introduced requiring Internet users to identify themselves to service providers, and requiring Internet providers to delete banned material and to inform the authorities of such postings. These regulations were apparently intended to bring under control mobile phone-based Internet activity. In addition to overseeing very intensive censorship of the Internet, the Chinese government employs people to pose as ordinary Internet users and post pro-government material. Until recently it also tried to introduce into all new computers a kind of spyware called Green Dam: officially its purpose was to restrict exposure to pornography, but actually it worked to expose visits to sites with political content. The Chinese government has also blocked virtual private networks, which permit encrypted personal communication. Most of these actions are in contravention of article 19. The Green Dam initiative would clearly violate ICCPR article 17, which protects privacy, if it were implemented.

jurisdictions just mentioned, there is no doubt that the relevant rights protections apply. As we have been saying, the manifestations of the most public cyberactivism are street protests, which are paradigms of human rights-protected activity. The connection of some protected activism with the Internet makes no significant difference to which rights are in question. In the case of the most public cyberactivism, the new technology is only a new medium for organizing mass protests: it has not ushered in mass protests for the first time or radically altered their public manifestations. People are still appearing in numbers on the streets, and still making visible protests about issues that the wider public can recognize and understand. The new technology may recruit people who would not otherwise have been activists, and it may afford novel and efficient communication between like-minded individuals, but it neither excludes nor supersedes participation by other individuals who do not use the Internet.

What is more, street protests expose cyberactivists to all the dangers of crowd violence, arbitrary arrest and surveillance by the authorities that entirely conventional mass demonstrations have traditionally involved. These forms of willing public exposure to the authorities show a kind of deference to democracy in human rights-respecting jurisdictions and a willingness to build a culture of open protest in human rights-violating jurisdictions. Some of these features legitimize cyberactivism in ways that the appearance on demand of busloads of party or union activists cannot. And those same features seem to give the most public cyberactivism a moral and political authority that hacktivism lacks. Or so I will argue.

2. New challenges to human rights concepts from cyberactivism: Wikileaks

Two important and related hacktivist groups are Wikileaks and Anonymous. I shall suggest that while some of the objectives of these groups can be and are pursued by human rights activists and institutions, some of the distinctive means adopted by hacktivists are subversive of central tenets of human rights, at least as traditionally understood. Hacktivist groups are not the only actors who disturb human rights thinking; lone wolf hacktivists are also anomalous, and challenge the usual understandings in human rights of which agents are weak and which are powerful.

Wikileaks is an online media organization that publishes leaked, secret information (Sifry 2011: 171).[9] Its practice is not only to publish stories based on the documents released to it, but also the documents themselves, sometimes in huge quantities. It collects its leaks through electronic drop boxes that it has helped to design to protect the anonymity of its sources. So its work is partly journalistic and partly technological. The information it has released concerns a wide variety of countries, but its best publicized leaks have been of

9 In a mainly very good discussion of Wikileaks, Micah Sifry (2011) distinguishes three different models of Wikileaks activity: (1) as a 'wiki-fied conduit for raw information dumps'; (2) 'tight editorial control and production' as in the production of the 'Collateral Murder' video; and (3) collaborations with established, mainstream organizations.

US government and US military material, some of them on a vast scale. Perhaps its most impressive disclosure is of a film that appears to prove that on at least one occasion the US military was guilty of targeting non-combatants during the most recent war in and occupation of Iraq. In the case of the recent release of US diplomatic cables, Wikileaks cooperated in their publication with two mainstream newspapers, *The Guardian* in London, and *The New York Times*.

A striking aspect of the self-description of Wikileaks (2011) is its mention of human rights:

> The broader principles on which our work is based are the defence of freedom of speech and media publishing, the improvement of our common historical record and the support of the rights of all people to create new history. We derive these principles from the Universal Declaration of Human Rights. In particular, Article 19 inspires the work of our journalists and other volunteers. It states that everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. We agree, and we seek to uphold this and the other Articles of the Declaration.

The reference is to the Universal Declaration of Human Rights (UDHR) rather than ICCPR. Although article 19 in each instrument is about the freedom of expression, the UDHR version corresponds only to paragraph 1 of ICCPR, and includes nothing about the ways in which the right to free expression is limited by other rights. As we shall see, the interpretation of free expression as a free-standing right better fits Wikileaks practice than its declared support for the Universal Declaration as a whole.

What is the relation of Wikileaks practice to the ethics of leaking? Leaking is the act of an insider who, in the public interest, reveals sensitive information about his or her organization, information that those in charge of the organization do not want revealed. It is consistent with the purposes of leaking that the organization is merely embarrassed by the disclosure, say because it reveals a difference between its officially expressed aspirations and its practice. But in the cases that give leaking the character of a public service, the leaked information reveals that the organization is guilty of wrongdoing of some kind, with harmful consequences for the general public, whom the leaked information is supposed to reach. A leak may also be directed at authorities who are in a position to reverse or punish the wrongdoing or compensate those harmed. The more serious and widespread the harm revealed, the more the leaking is morally justified and maybe even obligatory. On the other hand, the less serious it is, and the more the aim of leaking is simply to embarrass, the less morally justified it is. For example, a leak from within government or the military of an official's romantic emails might be at the frivolous

end of the spectrum, while a leak showing that a government department knew and did nothing about a manageable health risk to the public probably lies at the other end.

The ethics of leaking is important to assessing Wikileaks' (2011) rationale for its disclosure of secret information:

> Publishing improves transparency, and this transparency creates a better society for all people. Better scrutiny leads to reduced corruption and stronger democracies in all society's institutions, including government, corporations and other organisations. A healthy, vibrant and inquisitive journalistic media plays a vital role in achieving these goals. We are part of that media.
>
> Scrutiny requires information. Historically, information has been costly in terms of human life, human rights and economics. As a result of technical advances particularly the Internet and cryptography—the risks of conveying important information can be lowered. In its landmark ruling on the Pentagon Papers, the US Supreme Court ruled that 'only a free and unrestrained press can effectively expose deception in government'. We agree.

Many of these claims are disputable when applied to Wikileaks' own activity. First, not all Wikileaks disclosures reveal deception, still less the sort of deception brought into the open by the Pentagon papers. For example, in the case of the leaked US diplomatic cables, many revelations were simply of diplomats' opinions and assessments of governments or officials in the countries where they were based. Diplomacy, although often a context for private discussion, is not necessarily a departure from open government, since, at least in theory, those to whom the diplomats report are highly accountable, and since diplomatic efforts at reconciliation or the formulation of policy are known and agreed by all concerned to work better when they are pursued behind closed doors.

Again, it is hard to see the strong public interest in disclosing even some of the alleged highlights of the cables. Among the items that made it into *The Guardian* summary of the highlights was the far from startling revelation that British diplomats had given American diplomats a 'master class in negotiating with the Iranians' and that a member of the British royal family had made inappropriate comments about one of the security services (Leigh 2010). These are tabloid titbits rather than leaking of great moral importance. It is true that other information—for example concerning Saudi support for an attack on Iran—is far more than a titbit, but in that case it is hard to know what a *Guardian* reader in the UK, a *New York Times* reader in New York, or even a Saudi Internet user could have done with it. The information is perhaps most useful to the Iranian government, but then that is hardly one of the intended beneficiaries of Wikileaks. The target audience is supposed to be ordinary

people, who are supposed to use the information they get from Wikileaks to hold governments to account (Sifry 2011: 173).[10] Since Saudi citizens are not able easily to hold their government to account, and since the Iranian government is not ordinary people, the value of the disclosure seems primarily journalistic: it is news.

Once more contrary to its own self-description, not all Wikileaks information is leaked. Instead of being provided by insiders, some of it is stolen by outsiders and then given to Wikileaks. For example, internal emails from an American security intelligence company, Stratfor, that were relatively recently disclosed, came to Wikileaks not from company employees but from the cyberactivist group Anonymous. How Anonymous came to choose this company as a target is unclear, and, as in the case of some of the material included in the diplomatic cables, it is quite a varied set of emails, some of no obvious public interest at all. More significantly, however, some of those published contained identifying information and therefore exposed employees and others to cyber-hostility or worse from those who are likely to vilify organizations targeted by Wikileaks and Anonymous. Equally significantly, Wikileaks published this material despite its stated commitment to UDHR, and despite the UDHR containing a right to privacy (article 12) that clearly encompasses personal emails, especially when their publication harms the reputations of innocent people.

It is striking that the disclosure of personal emails and identifying information by Wikileaks has sometimes not been condemned by human rights organizations. For example, in its online comments on Wikileaks, Human Rights Watch (2010) expresses reservations about naming human rights defenders, but seems to ignore violations of the right to privacy of named Stratfor employees. Amnesty International (2010) does acknowledge the wider range of violations of privacy, but it appears unconcerned with the disclosure of information that merely embarrasses officials.[11] I have argued that some embarrassing disclosure that is not in the public interest is not justified by the ethics of leaking, and much information that is merely embarrassing furthers no public interest by being disclosed.

Both Amnesty International and Human Rights Watch object to the excessive use by governments of security classifications that render some of the information revealed by Wikileaks officially secret. I am sympathetic to those objections, but not all information that is kept secret is protected for the mere convenience of governments or at the whim of officials. Keeping the content of diplomatic exchanges secret is a practice that probably has the status of customary international law, and it probably reduces the posturing that perfectly

10 Sifry quotes from two recent essays by Julian Assange that suggest that far from leaking to energize the public, its purpose was to make the organizations attacked paranoid, brittle and unable to function. For further discussion, see Brevini et al. (2013).

11 Other civil society groups have taken a similar line. See Whalen (2010).

open diplomacy would inevitably involve. Secret diplomacy frees officials from having to strike official poses and speeds up dispute resolution. So it is or can be morally justified on balance, notwithstanding its conflict with the value of making the actions of government transparent to the governed.

I turn now to Wikileaks' claims to engage in processes of democratic accountability, given the organization's own secrecy, and given the way that its failure to disclose information about itself contributes to an objectionable kind of impunity. To develop these claims, let us consider differences between Wikileaks and some of the media organizations it cooperates with.

The Guardian and *The New York Times* are large organizations with published addresses. Their journalists sign their articles. Both newspapers have engaged in big journalistic exposures, sometimes based on leaks. Some of these exposures, as we have just seen, have been carried out in conjunction with Wikileaks, but others have been the work of the newspapers themselves. This means they do not have to be taught investigative journalism by their cyber-collaborators. Both *The Guardian* and *The New York Times* have a significant online presence, and both have global reputations for reliability. One way this reputation is ensured is by having a large staff. This enables the two newspapers to check stories, and also to edit them in ways that make large amounts of information digestible by their audiences. A further feature of the two organizations is that they are highly exposed where they are headquartered to libel laws and to laws prohibiting hacking, even in the service of bona fide investigative journalism. When they make mistakes, they sometimes voluntarily and sometimes by court order say so publicly. The same is true when they or their journalists are guilty of fraud or of some other kind of criminal activity. In these last respects, *The Guardian* and *The New York Times* follow an accepted practice familiar in other Western media organizations. The BBC, for example, is active not only in publicizing its own journalistic mistakes, but also the wrongdoing of its employees outside journalism, most recently the sexual abuse perpetrated by its star presenters from the 1960s and 70s.

Wikileaks is systematically different from these mainstream organizations. Although it says quite a lot about its convictions on its website, it displays no masthead identifying its editors, and, apart from Julian Assange, few people connected with the organization have ever been named. This might make sense if those running Wikileaks were based in human rights-violating jurisdictions, but it is known that much Wikileaks technology is based in Scandinavia, where there is no tradition of censorship or government interference in the media. Since Wikileaks does not necessarily go in for disclosures that are more far-reaching than those of its mainstream collaborators, it is entirely unclear why it is so shadowy. On the contrary, its secrecy about itself detracts from both the credibility of its news and the credibility of its adherence to human rights. It detracts from the credibility of its news because no one knows whether it has the resources to check the information it publishes. Though it claims to check all its information before publishing, it does not

back up this claim with an indication of numbers of people, or their competence, or the methods by which information is tested for accuracy and authenticity. This would be bad enough in a media organization with a relatively local coverage, but Wikileaks publishes leaks about the powerful in a wide array of countries. Again, its secrecy about itself seems to call into question its self-proclaimed belief in transparency. It has not been quick to report allegations of wrongdoing by its own employees. On the contrary, it has avoided doing so. For example, it did not publicize charges of sexual assault against Assange in Sweden. It has also failed to comment on the irony of Assange's seeking refuge from the Swedes and the UK authorities trying to extradite him in the embassy of a state—Ecuador—with a very poor record of protecting human rights in general and the freedom of expression, in particular.[12]

Wikileaks' secrecy is puzzling. It is not as if media organizations have some special exemption from scrutiny because they are usually ranged against human rights-violating governments. Media organizations can even be instruments of the state; they can also be human rights violating non-state actors in their own right. To give one example, media organizations had a well documented role in encouraging the Rwanda genocide (Thompson 2007). Indeed, three people connected with *Radio télévision libre des mille collines* have been convicted of genocide offences by the International Criminal Tribunal for Rwanda (2003). And, at the less extreme end, people in media organizations have been guilty of fraud and of hacking.[13] Wikileaks, too, is associated with hacking through its publication of emails hacked by Anonymous.

More problematic than its double standards about transparency is the fact that its secrecy promotes legal impunity. Far from exposing itself to libel action or prosecution for hacking, as *The Guardian* and *The New York Times* do, Wikileaks appears to position itself exclusively in the legal no-man's-land of cyberspace. But this calls into question the democratic character of its supposed role in holding the powerful to account. For it is arguably part of holding the powerful to account in a democracy that institutions and individuals within a democracy all submit to the same scheme of law. Holding to account is partly holding to account under law, and even those whose democratic activity is civil disobedience submit voluntarily to arrest and even imprisonment by the jurisdiction that they disobey. There is no such submission from a position of anonymity in cyberspace.

I now consider two replies to the objection that Wikileaks seeks and exercises an unacceptable legal impunity. First, it might be replied in defence of Wikileaks that while it does not expose itself to law in any liberal jurisdiction, it still abides by international law, including human rights law. This, however, is far from evident. First of all, human rights law presupposes the rule of

12 The irony has not been lost on Amnesty International (2012).

13 As in the Leveson Inquiry in the UK. For discussion, see Mair (2013). For the hacking scandal that led to Leveson, see Keeble and Mair (2012).

domestic law, for it is governments that are parties to international human rights treaties, and they fulfil their obligations under these treaties partly through domestic legislation. Second, domestic law that prohibits hacking, and that protects the reputations of people and also their private communications from disclosure is not only consistent with human rights but required by human rights. So Wikileaks' violations of this law are inconsistent with its adherence to human rights. It is true that article 19 of UDHR does not mention the limitations of the right to free expression that are to be found in the corresponding article of ICCPR, but human rights is nothing if not holistic, and it is quite contrary to its spirit to take the narrower UDHR formulation as the definitive one. In any case, disclosures from a space outside all democratic jurisdictions do not seem to be democratic acts. To be democratic, they need to be exposed to the laws of democracies.

The second reply on Wikileaks' behalf depends on reinterpreting what I have been calling impunity as a deliberate repudiation of national allegiances, and as the seizure of a distinctively cosmopolitan space (Tambini 2013; Sifry 2011: 173–4). This reply is easiest to understand in the light of the tensions between Wikileaks and its conventional media partners over what should be published, and what should be 'redacted', that is, expunged, from leaked cables for the sake of national security. Whose national security were offline organizations obliged to take account of? They were *legally* obliged to take account of the national security of their own local jurisdictions, sometimes over the protests of Julian Assange, who wanted them to test the legal boundaries. Since *The Guardian* and *The New York Times* worked jointly on redaction, a kind of mid-Atlantic 'national interest' was reflected in their redactions: text was suppressed if it endangered US *or* UK troops and officials. But another Wikileaks partner was the Pakistan *Dawn* newspaper, which took over the *Guardian–Times* redactions when it reprinted the Wikileaks material. Pakistan's national government had been heavily criticized domestically for colluding militarily with the USA, and the *Guardian–Times* redactions did not take account of Pakistani sensitivities. Should *Dawn* have redacted the Wikileaks cables from scratch, to reflect Pakistani national security and have ignored the *Guardian–Times* redactions? If we say 'no' we seem to be endorsing a double standard. If we say 'yes', we endorse publicity that will lead to harm to some government's officials and troops.

This dilemma, which arises from Wikileaks' and *Dawn*'s dependence on better-resourced media organizations in particular jurisdictions, raises the question of whether Wikileaks compromised its possible function of conducting journalism from a global rather than a national perspective, the distinctive perspective supposedly afforded by an Internet-based journalistic organization. As Carl Shirky (Tambini 2013: 247) puts it:

> Appealing to national traditions of fairplay in the conduct of news reporting misunderstands what Wikileaks is about: the release of

> information without regard to national interest. In media history up to now, the press is free to report on what the powerful wish to keep secret because the laws of a given nation protect it. But Wikileaks is able to report on what the powerful want to keep secret because the logic of the internet permits it.

The implication here is that Wikileaks forfeits the distinctive cosmopolitan approach that the Internet affords it when it condones a national interest-based redaction policy. But this is highly tendentious. When the names of government officials or the details of military operations are edited out, that is not necessarily a case of the powerful wanting to keep something secret and the less powerful—journalists—colluding with the powerful, as Shirky claims. The less powerful may themselves think that publishing names is wrong. They may think that even if the people whose identities are concealed are not 'innocent', they are nevertheless personally vulnerable and are often representing governments, rather than acting in their own right: exposing them will not necessarily hold governments to account, and may expose them personally to great danger for no good reason.

So an argument for restraint in disclosure can be based on considerations other than the national interest. But it is hard to see how the Wikileaks' theory of popular action based on their disclosures is supposed to work if national interest is always supposed to be irrelevant. Wikileaks revelations are supposed to make people hold governments to account, in particular—at least according to their website—hold their *own* governments to account. Many citizens will think that the interest of their own nation has to be protected by their governments where the means are not too brutal and where national interest is weighty, and not equated merely with the government interest. Such people will not be helped to criticize their governments by Wikileaks if national interest is always understood as a biasing or contaminating influence.

3. New challenges to human rights concepts from cyberactivism: Anonymous

From many different directions, then, Wikileaks theory and practice is open to question, and if Wikileaks is the prototype of the online media organization of the future, then either human rights law will have to change to accommodate new media behaviour or online media organizations will have to drop their pretensions, if any, to comply with human rights law.

Other cyberactivist organizations are also hard to accommodate in traditional human rights theory and practice. Our chosen example is Anonymous.[14] As we

14 Anonymous as a group of hackers—strictly only a small proportion of Anonymous participants have sophisticated computer skills—emerged from the social interactions occurring in 4chan, a popular online image board that is perceived as one of the most offensive sites on the Internet. Before 2008, Anonymous was mainly associated with pranks—trolls—played online and intended to reveal personal or embarrassing information about specific people. In

have already seen, Anonymous has provided material to Wikileaks: notably emails it extracted from the security firm Stratfor by hacking (Fitzpatrick 2012). More than that, it has taken Julian Assange's side against the Swedish Prosecutor's attempt to extradite Assange from the UK in connection with an alleged sex offence. Anonymous attacked the website of the Swedish Prosecutor's office, presumably as a kind of protest against the extradition, and it launched denial of service attacks against Visa and Mastercard when these companies withdrew payment processing services from Wikileaks (BBC News 2010). More recently, Anonymous has fallen out with Wikileaks over the latter's decision to put some of its material behind a paywall (Santo 2012). It is possible, then, that cybersabotage by Anonymous in defence of Wikileaks will cease.

The problems with Anonymous do not end with its being mercurial and partial in its use of cybersabotage. It has many other peculiarities, some of which raise the question of whether it has enough unity even to count as a single organization. One of the images which it uses to identify itself illustrates the problem: it is a headless suit with a question mark in the place where a face might be. This is supposed to convey the idea that Anonymous is headless—in the sense of being collaborative rather than hierarchical. It is a protest movement rather than an organization with a programme or manifesto, but the targets of the protest are varied, and there is no obvious theme to them. Scientology, surveillance, security, censorship, paedophilia—these are some of its bêtes noires. But it also adopts causes that are far more particular and local. It 'doxed' or named in a vilifying way an individual it alleged was the cyber-bully behind a Vancouver teenager's suicide (Warren and Keneally 2012). And it recently posted a video that appears to have incriminated a group of teenagers in a small American town who were later convicted of the rape of an under-age girl (Democracy Now 2013).

Not every case of doxing appears to have identified the right person. In the case of the cyber-bully, it appears the wrong person was named at first, and then a second person was accused (Shaw 2012). If the wrong person was in fact identified, Anonymous is clearly guilty of a serious injustice. In the case of Stratfor, as we saw earlier, emails of identified people were released without it being clear that they had done anything wrong. This sort of exposure also appears to be flatly unjustifiable. Then there is the Swedish Prosecutor's office

January 2008, Anonymous started to launch trolls and lulz (cuttingly, often offensively, humorous Internet posts) against the Church of Scientology, mostly in response to the church's attempt to get Tom Cruise's promotional video for Scientology removed from the Internet. Soon after the first rounds of pranks Anonymous raised the bar and launched distributed denial of service (DDoS) attacks against Scientology's website and started also to disseminate incriminating information about Scientology itself. This helped Anonymous to get in touch with some of the church's dissidents and to bring to the fore the church's attitude to censorship and the breach of human rights. For a recent discussion, see Milan (2012). For a more recent, book-length account, see Olson (2013).

(Gross 2012). Anonymous seems to have been involved in a denial of service attack on its website as well as those of several other Swedish organizations, apparently in retaliation for the prosecution of Julian Assange, whom Anonymous identifies or once identified with Wikileaks. If Anonymous was indeed responsible, then it is guilty of confusing the investigation by the Swedish government of a complaint under criminal law against Assange personally with the persecution of Wikileaks. The Swedish courts can hardly be blamed for pursuing a complaint, and it prejudges the facts to take Assange's side. Moreover, there is no record of Swedish criminal prosecutions being unfair as a rule, or that Assange would readily be handed over to the US authorities if they requested his extradition, as Assange himself alleges. In fact it is quite unclear what Assange has to fear from going to Sweden to face charges. Moreover, and crucially, Assange is not identical with Wikileaks, and it is highly likely that the women who accuse him of sexual assault in Sweden have nothing whatever against either the organization or its tactics.

As in the case of Wikileaks, Anonymous hides the identity of those associated with it. Its online actions are not attributed to individuals, and, in their relatively rare offline protests, Anonymous associates conceal their faces with Guy Fawkes masks. As in the case of Wikileaks, anonymity promotes impunity and a kind of outsider status in relation to the democracies that Anonymous sometimes attacks. Again, the partisanship and capriciousness of Anonymous actions partly undermines them. Here the 'headlessness' of Anonymous may be at work. If carrying out an Anonymous action is just a matter of carrying out an action in the name of Anonymous, with no one being more authoritative than anyone else about what Anonymous stands for, then perhaps Anonymous *has* no distinctive issues. This may be the other side of the coin of having no manifesto, no leadership and no mechanism for induction and expulsion. But in that case, hacktivism surely verges on a kind of anarchic hoodlum-like behaviour. This, too, is a challenge for human rights thinking, since low-level criminality performed by loosely associated individuals is not a protected form of protest or an exercise of the freedom of association. To be protected by human rights, the values embraced by activism have to work as elements of a recognizable way of life under democratic institutions. Sometimes cyberactivism merely plays out online new forms of allegiance to values that fit into liberal forms of social organization. These are the values that human rights are at home with. When other values are in play things are not so clear.

Other values sometimes *are* in play. Anonymous inherits from its 4chan roots not only a willingness to send up or see the funny side of anything, but also a strong anti-feminist, even misogynist, and homophobic tendency among many of its overwhelmingly male and geeky members.[15] It is possible

15 This criticism is strongly emphasized in a recent article in *The Nation* by Andrew Chen (2014).

to write off these anti-women and ant-gay tendencies as cases of an underlying irreverence (in this case directed at left-wing orthodoxies) that unifies all of Anonymous activities. It is possible also to look at this irreverence as a usefully disruptive force in morality and politics (Coleman 2014), one that can revive and refresh liberalism (Coleman 2013). These approaches fit in with a kind of apologism for Anonymous, but it will already be clear that I reject them (see also Chen 2014).

Hacktivism is sometimes illiberal not only in its lawlessness and anonymity, but also in the space it affords to an activism engaged in by individuals who are otherwise isolated from one another. Revolutionary Marxism sometimes took the form of 'cells' of activists, carrying out their own actions in ignorance of the members of other cells and their plans. Cyberactivism seems to take this model one step further, since with sufficient technical expertise a lone individual with a computer can do damage to states that in the past only groups could do. Some 'members' of Anonymous and other hacktivists must be more or less autonomous, hacking sites and planting viruses, organizing cybersabotage and sharing information about how these things are done—all from a teenager's bedroom in the suburbs of the UK, Sweden or the USA. These are non-state actors that human rights theory and practice may also have to come to terms with in the future. Alone and loosely connected, never in a chain of command, these individuals may turn out to be far stronger than the inventors of human rights ever thought was possible for individuals. Their strength may also make states vulnerable in ways that human rights theory and practice have never anticipated.

Traditionally, human rights addressed the vulnerabilities to state action of the relatively weak. Cyberactivism in particular and cyber-expertise in general redistributes these vulnerabilities. States and large commercial organizations as well as individuals working for them can become vulnerable to individuals or small groups. Sometimes these new vulnerabilities rebalance power relationships that are very oppressive; but sometimes they do not. Sometimes cyberexposures or cyberattacks are petty or malicious and fail to be justified by any public interest. Sometimes they circumvent the enforcement of law that is human rights compliant. Almost always they are done in secrecy and with impunity. Although they are not always very harmful, cyber-actions against the state can be expensive and disabling and can weaken the operation of human rights-respecting practice. This is because states are not only a threat to, but the protectors of, human rights. Since many welfare-distributing interactions between states and individuals in developed countries take place over the Internet, cyber-vulnerabilities on the part of states not only limit state abilities to misuse their power: they limit state abilities to realize human rights. Denial of service attacks not only make human rights-realizing activity less efficient; responding to them consumes funds that are needed to mobilize help for the weakest people, both domestically and internationally.

Compared to the most public cyberactivism, lone wolf hacktivism and swarm hacktivism run a big risk of being based on misinformation and of

being carried out illegitimately. The old adage that there is safety in numbers seems to be borne out in the cyberworld: the more or less arbitrary selection of causes of individual hacktivists might receive at least some critical consideration from others if hacktivist actions were carried out by groups of independent minded individuals and consensus—rather than by a swarm. This would start to move hacktivism toward a more democratic method of action. The alternative of whimsical and unpredictable doxing or cyberattack arguably brings politics too close to the sphere of gaming, sometimes at the expense of human rights.

Acknowledgements

I wish to thank George Lucas for comments and encouragement and Richard Aldrich for several opportunities to present these ideas. An early version of this article was given to several audiences. I wish to thank Mariarosaria Taddeo for the initial invitation.

References

Amnesty International. 2010. Wikileaks and Freedom of Expression. http://www.amnestymena.org/en/magazine/issue16/wikileaks.aspx?articleID=1020 (referenced 4 May 2015).

———. 2012. Is Assange a Hypocrite over Ecuador? Press release me let me go—Amnesty International UK Blogs. http://www.amnesty.org.uk/blogs/press-release-me-let-me-go/assange-hypocrite-over-ecuador (referenced 4 May 2015).

Barlow, J. P. 1996. The Declaration of the Independence of Cyberspace.

Bartlett, J. 2014. *The Dark Net*. London: Heinemann.

BBC News. 2010. Anonymous Hacktivists say Wikileaks War to Continue. 9 December.

Bennett, W. L., and A. Segerberg. 2012. The Logic of Connective Action. *Information, Communication & Society* 15(5): 739–68.

Brevini, B., A. Hintz, and P. McCurdy (eds). 2013. *Beyond Wikileaks: Implications for the Future of Communications, Journalism and Society*. Basingstoke: Palgrave Macmillan.

Castells, M. 2012. *Networks of Outrage and Hope*. Cambridge: Polity.

Cavelty, M. 2012. Cybersecurity. Available at Social Science Research Network (SSRN): http://ssrn.com/abstract=2055122 (referenced 21 July 2015).

Chadwick, A., and C. May. 2003. Interaction between States and Citizens in the Age of the Internet: 'E-Government' in the United States, Britain and the European Union. *Governance* 16(2): 271–300.

Chen, A. 2014. The Truth about Anonymous' Activism. *The Nation*. 11 November.

Coleman, G. 2013. *Coding Freedom*. Princeton University Press.

———. 2014. *Hacker, Hoaxer, Whistleblower, Spy*. London: Verso.

Democracy Now. 2013. Hacker Group Anonymous Leaks Chilling Video in Case of Alleged Steubenville Rape Cover-Up. 7 January.

Erlingsson, G., and M. Persson. 2011. The Swedish Pirate Party and the 2009 European Parliament Election: Protest or Issue Voting? *Politics* 31(3): 121–8.

Fenton, N. 2012. *The Internet and Radical Politics*. In J. Curran, N. Fenton and D. Freedman, *Misunderstanding the Internet*: 149–76. Abingdon: Routledge.

Fitzpatrick, A. 2012. Wikileaks Partners with Anonymous, Releases Security Firm's Emails. 27 February.

Gross, G. 2012. Swedish Websites Down after Anonymous Threats. *Computer World*. 5 October. http://www.computerworld.com/article/2492053/security0/swedish-websites-down-after-anonymous-threats.html (referenced 5 May 2015).

Hicks, S., E. Halpin, and E. Hoskins (eds). 2000. *Human Rights and the Internet*. London: Palgrave Macmillan.

Hintz, A., and S. Milan. 2009. At the Margins of Internet Governance: Grassroots Tech Groups and Communication Policy. *International Journal of Media & Cultural Politics* 51(1–2): 23–38.

Human Rights Watch. 2010. Q&A: Human Rights and the Wikileaks Cable Release.

———. 2015. Tunisia: Essential Background.

International Criminal Tribunal for Rwanda. 2003. Three Media Leaders Convicted for Genocide. Press release. 3 December.

Jordan, T. 2000. *Cyberpower: The Culture and Politics of Cyberspace and the Internet*. London: Routledge.

Jordan, T., and P. Taylor. 1998. A Sociology of Hackers. *The Sociology Review* 46(4): 757–80.

———. 2004. *Hacktivism and Cyberwars: Rebels with a Cause?* London: Routledge.

Jorgensen, R. 2013. *Framing the Net: The Internet and Human Rights*. Cheltenham: Edward Elgar.

Keeble, R., and J. Mair (eds). 2012. *The Phone-Hacking Scandal: Journalism on Trial*. Bury St Edmunds: Abramis.

Leigh, D. 2010. US Embassy Cables Leak Sparks Global Diplomatic Crisis. *The Guardian*. 28 November.

Levmore, S., and M. Nussbaum (eds). 2012. *The Offensive Internet*. Cambridge, MA: Harvard University Press.

Mair, J. (ed). 2013. *After Leveson? The Future for British Journalism*. Bury St Edmunds: Abramis.

Metzl, J. 1996. Information Technology and Human Rights. *Human Rights Quarterly* 18(4): 705–46.

Milan, S. 2012. Wikileaks, Anonymous and the Exercise of Individuality: Protesting in the Cloud. In Brevini, Hintz, and McCordy (eds), *Beyond Wikileaks*: 191–208.

———. 2013. *Social Movements and their Technologies: Wiring Social Change*. Basingstoke: Palgrave Macmillan.

Moore, A. 2011. Privacy, Security and Government Surveillance: Wikileaks and the New Accountability. *Public Affairs Quarterly* 25(2): 141–56.

Nissenbaum, H. 2005. Where Computer Security Meets National Security. *Ethics and Information Technology* 7(2): 61–73.

Olson, P. 2013. *We are Anonymous*. London: Heinemann.

Park, S. 2013. The United Nations Human Rights Council's Resolution on Protection of Freedom of Expression on the Internet as a First Step in Protecting Human Rights Online. *North Carolina Journal of International Law and Commercial Regulation* 38(4): 1129–57.

Santo, M. 2012. Hacker Group Anonymous Vows to Sever Ties After Wikileaks Erects Paywall. 13 October.

Shaw, G. 2012. Hacker Group Releases Online Record of Second Alleged Amanda Todd Stalker. 17 October.

Shirky, C. 2010. Half-Formed Thought on Wikileaks & Global Action. http://www.shirky.com/weblog/2010/12/half-formed-thought-on-wikileaks-global-action/ (referenced 5 May 2015).

Sifry, M. 2011. *Wikileaks and the Age of Transparency*. London: Yale University Press.

Sorell, T., and T. Landman. 2006. Justifying Human Rights: The Roles of Domain, Audience and Constituency. *The Journal of Human Rights* 5(4): 383–400.

Steeves, V. 2000. Privacy, Free Speech and Community: Applying Human Rights Laws to Cyberspace. In Hicks, Halpin, and Hoskins (eds), *Human Rights and the Internet*: 187–99.

Tambini, D. 2013. National Security and Cosmopolitan Ethics. In N. Coudry and A. Pichevski (eds), *Ethics of Media*: 232–52. London: Palgrave Macmillan.

Taylor, A. 2014. *The People's Platform*. London: Metropolitan Books.

Thompson, A. (ed). 2007. *The Media and the Rwanda Genocide*. Oxford: Pluto Press.

Warren, L., and M. Keneally. 2012. The Internet Vigilantes: Anonymous Hackers' Group Outs Man. *Daily Mail*. 16 October.

Whalen, J. 2010. Rights Groups Join Criticism of Wikileaks. *Wall Street Journal*. 9 August.

Wihbey, J. 2013. The Arab Spring and the Internet: Research Roundup. Journalists Resource. http://journalistsresource.org/studies/society/internet/research-arab-spring-internet-key-studies (referenced 21 July 2015).

Wikileaks. 2011. What is Wikileaks? http://www.wikileaks.org/About.html (referenced 4 May 2015).