APC ISSUE PAPER

FREEDOM OF PEACEFUL ASSEMBLY AND FREEDOM OF ASSOCIATION AND THE INTERNET

Alex Comninos

INTRODUCTION

The internet, social networks and mobile phones enhance human freedoms to come together around social, political and economic issues, to build associations and networks, and to assemble online to advocate for and to defend human rights. This has been reflected in demonstrations and protests in the middle-east and North Africa;[1] anti-austerity protests in Greece, Italy and Spain; "Occupy" protests; advocacy and protests against the Stop Online Piracy (SOPA) and PROTECT IP[2] (PIPA) bills in the United States; student protests in Quebec and Chile; and protests against the Anti-Counterfeiting Trade Agreement (ACTA). At the same time, responses by governments to the exercise of these rights including online crackdowns;[3] violent crackdowns in Bahrain, Egypt, Libya and Syria; and new anti-protest legislation in the US and Canada[4] have highlighted new threats posed to the freedoms of association and peaceful assembly.

What does it mean to assemble or form associations online? How is freedom of assembly and association exercised on the internet? How can the internet affect freedom of association and assembly? What online challenges are currently presented to the exercise of the rights to freedom of association and freedom of assembly? How can these freedoms be protected in both online and offline spaces? This paper aims to catalyse debate around these questions.

The internet can augment the opportunities and capabilities of citizens and netizens to form associations,

1. Ramy Raoof "The internet and social movements in North Africa" *Global Information Society Watch 2011: Internet rights and democratisation* APC and HIVOS, 2011, www.giswatch.org/en/2011
2. PROTECT IP stands for the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property.
3. Alex Comninos "E-revolutions and cyber crackdowns: User-generated content and social networking in protests in MENA and beyond" *Global Information Society Watch 2011: Internet rights and democratisation* APC and HIVOS, 2011, www.giswatch.org/en/2011
4. Armina Ligaya "Now the UN slams Quebec's 'alarming' anti-protest laws in latest Canada criticism" *The National Post*, 18 June 2012, news.nationalpost.com/2012/06/18/un-slams-quebecs-alarming-anti-protest-legislation-bill-78

Alex Comninos is a scholar and researcher on the internet and information and communications technologies from a human rights perspective. He is a DAAD scholar and doctoral student in the Department of Geography, Justus Liebig University Gießen, Germany. He has an MSocSci in International Relations from the University of Cape Town.

APC ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

CONNECT YOUR RIGHTS! INTERNET RIGHTS ARE HUMAN RIGHTS

enhance the management and organisation of associations, and increase the membership and reach of associations. It provides new tools for those organizing peaceful assemblies, as well as the possibility of conducting assemblies in online spaces. In addition to being a powerful multiplier for the freedoms of association and peaceful assembly, the internet can also pose new threats to the exercise of these rights.

The rights to freedom of peaceful assembly and of association

The Universal Declaration of Human Rights (UDHR) states that "everyone has the right to freedom of peaceful assembly and association."[5] The International Covenant on Civil and Political Rights (ICCPR) states that "everyone shall have the right to freedom of association with others, including the right to form and join trade unions for the protection of [her or] his interests."[6]

Freedom of association and *freedom of peaceful assembly* have similar meanings and are often used interchangeably. Freedom of peaceful assembly is sometimes more narrowly defined as the freedom to assemble peacefully in a public place, and more specifically the right to protest peacefully. The United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kiai,[7] in his recent report to the Human Rights Council underlined that:

> ...while the rights to freedom of peaceful assembly and association are clearly interrelated, interdependent and mutually reinforcing, they are also two separate rights. They are indeed in most cases governed by two different types of legislation and...they face different challenges. This implies that they should be treated separately.[8]

Kiai recognises that "the rights to freedom of peaceful assembly and of association serve as a vehicle for the exercise of many other civil, cultural, economic, political and social rights."[9] He quotes a Human Rights Council resolution stating that these rights empower individuals to:

> ...express their political opinions, engage in literary and artistic pursuits and other cultural, economic and social activities, engage in religious observances or other beliefs, form and join trade unions and cooperatives, and elect leaders to represent their interests and hold them accountable.[10]

The exercise of these rights may be, as stated by the Human Rights Council, "subject only to the limitations permitted by international law, in particular international human rights law"[11] such as the ICCPR which states that:

> No restrictions may be placed on the exercise of this right other than those which are prescribed by law and which are necessary in a democratic society in the interests of national security or public safety, public order (ordre public), the protection of public health or morals or the protection of the rights and freedoms of others.[12]

One of the general recommendations of the Special Rapporteur is "to recognize that the rights to freedom of peaceful assembly and of association can be exercised through new technologies, including through the Internet."[13] The Special Rapporteur has noted that the word "association" may also refer to online associations.[14] He also notes "the increased use of the Internet, in particular social media and other information and communication technology, as basic tools which enable individuals to organise peaceful assemblies. However, some States have clamped down on these tools to deter or prevent citizens from exercising their right."[15]

5. The Universal Declaration of Human Rights (UDHR), Article 20, http://www.un.org/en/documents/udhr
6. The International Covenant on Civil and Political Rights (ICCPR), Article 22, www2.ohchr.org/english/law/ccpr.htm
7. Maina Kiai is hereafter referred to as the "Special Rapporteur".
8. Maina Kiai *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Human Rights Council*, 21 May 2012, A/HRC/20/27 para 4, www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-27_en.pdf
9. Ibid, para 12.
10. Human Right Council *The rights to freedom of peaceful assembly and of association* HRC Resolution 15/21, 6 October 2010, A/HRC/RES/15/21, Preamble, www.ohchr.org/EN/Issues/AssemblyAssociation/Pages/SRFreedomAssemblyAssociationIndex.aspx
11. Ibid.
12. ICCPR, Article 22.
13. Kiai *Report of the Special Rapporteur*, para 84(4).
14. Ibid, para 52.
15. Ibid, para 32.

He further mentions a recent report by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, which recommended that all states should "ensure that internet access is maintained at all times including during times of political unrest."[16]

This paper investigates how freedom of peaceful assembly and of association can be exercised as well as infringed upon online. Firstly, it shall investigate new online threats to the freedoms of association and of peaceful assembly. Secondly, it will attempt to develop a human rights approach to the exercise of these freedoms that recognises the internet.

NEW THREATS TO FREEDOM OF ASSOCIATION AND OF PEACEFUL ASSEMBLY

Surveillance of assemblies and associations

There is a "profound connection between social networking and freedom of association", and "social networks such as Facebook and LinkedIn are simply the latest and strongest associational tools for online group activity building on the email and the web itself."[17] However as WikiLeaks' Julian Assange has noted, the internet is not only a force for openness and transparency, it is also potentially "the greatest spying machine the world has ever seen."[18] Frank La Rue has stated:

> ...the Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals' communications and activities on the Internet. Such practices can constitute a violation of the Internet users' right to privacy, and by undermining people's confidence and security on the Internet, impedes the free flow of information and ideas online.[19]

The internet thus presents new challenges to the freedoms of association and assembly. "Social networks and other emerging online activities receive increasing scrutiny from policy makers for privacy reasons."[20]

The internet augments opportunities for surveillance of associations and assemblies. Online communications can be easily intercepted by third-parties, including governments, corporations, and non-state actors. A plethora of data about associations and people generated on the internet passes through and is stored with intermediaries such as internet service providers and online content platforms like blogging websites, Facebook and Twitter.

We now form associations in ways that are different to the offline world. Social networking websites and mobile phones are changing how we conduct our associational life in the public and private spheres. Users of smartphones are for example "more willing to reveal private issues in public spaces."[21] Offline we selectively reveal information about our associational lives, in a conscious and controlled manner. Online one's real name, date of birth, network of friends and associational affiliations are often on a user's Facebook wall – accessible to all those with access, including friends, co-workers and employers. In sharing information online we exercise our rights to freedom of association and assembly. While this enhances our ability to express ourselves and to form associations, as well as enhances transparency, there is often a trade-off with regards to privacy or security.

Content platforms (e.g. Facebook) may for example share this information with third parties such as advertisers. New opportunities are created for infringements on the right to privacy as people can become subject to surveillance, or have their personal data used for reasons that were not originally intended. Information on social networks may potentially be mined by third-parties such as individuals or corporations, social networking applications, advertisers and governments. Users often agree to share their data with corporations. This is done by agreeing to

16. Frank La Rue *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* Human Rights Council, A/HRC/17/27, 16 May 2011, para 79, www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
17. Peter Swire "Social networks, privacy and freedom of association: How individual rights can both encourage and reduce uses of personal information" Center for American Progress, 28 February 2011, p. 2, www.americanprogress.org/issues/2011/02/social_networks_privacy.html
18. The Hindu "World's greatest spying machine" *The Hindu* April 2011, www.thehindu.com/opinion/editorial/article1602746.ece
19. Frank La Rue *Report of the Special Rapporteur* para 53.
20. Peter Swire "Social networks".
21. This is according to a study by researchers at Tel Aviv University, see "Are smartphones breaching our privacy?" *Hindustani Times* 12 May 2012, www.hindustantimes.com/technology/IndustryTrends/Aresmartphones-breaching-our-privacy/Article1-854604.aspx

the terms and conditions on social networking websites that users often do not read (rather one scrolls down and clicks "Accept"). In essence users are consenting to a social contract[22] with corporations that allow for certain invasions of privacy by allowing data to be collected, stored and shared with third parties. Users benefit from this because their associational life is subsidised by these economic activities, and they essentially get a "freebie" that greatly enhances their ability to communicate.

According to Peter Swire, in social networking there exists a "tension between information sharing, which can promote freedom of association, and limits on information sharing, notably for privacy protection", which can in certain instances also protect the freedom of association. There needs to be a deeper understanding, further research and a human rights approach to how information sharing interacts with privacy protection. Many feel "research has not found an analysis of how the two fit together".[23]

Data about associations and assemblies can be mined and analysed with algorithms by government agencies, corporations and even criminals to draw inferences about associational affiliations. Online surveillance can happen "relationally", rather than directly. Relational surveillance refers to the fact that targets of surveillance can be monitored by analysing behaviour from vast amounts of data, for example, traffic data, search data or communications on social networks. Analysis can be conducted by data mining and algorithms to predict and identify "suspicious" activity – the conclusions of which are often inaccurate. Under relational surveillance, people are identified as "suspect" before they have even formed associations, merely by an analysis of their behaviour and their networks.[24]

Another feature of modern surveillance is that internet users are surrounded by "always on" internet devices. "The internet of things",[25] an internet with more devices than people on the planet, each with IP addresses[26] assigned to them, is fast becoming a reality. Laptops, mobile phones, netbooks, tablets, digital television sets, fridges and dishwashers can all increase our ability to be surveyed. These devices can be geo-located through GPS in the device or through the measurement of signals from mobile phone base stations and wireless hotspots, or through analysis of IP addresses. They also contain cameras, light sensors and motion sensors that can be eavesdropped on. CIA director David Petraeus recently commented that an "internet of things" would be "transformational", particularly with regards to its "effect on clandestine tradecraft", adding that this will prompt us to "change our notions of secrecy".[27]

Censorship and shutting down communications

Another threat to freedom of association and assembly is online censorship – the filtering and blocking of access to online content, as well as particular services and protocols. Censorship can be used to restrict freedom of assembly and association. Governments in many countries have been using filtering technologies for some time to block access to certain content and thus curtail freedom of expression and association. This is well documented, by for example the OpenNet initiative and Google Transparency.[28] While some countries, for example, China and Iran have developed their national firewall systems to block content, many countries use software developed in Western countries, for example the United States and

22. For more on this kind of social contract see Rebecca Mackinnon *Consent of the networked* Basic Books, 2012, consentofthenetworked.com
23. Peter Swire "Social networks".
24. Katherine J. Strandburg "Surveillance of emergent associations: Freedom of association in a network society" in *Digital privacy: Theory, technologies, and practices*. Ed. Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis and Costas Lambrinoudakis, Auerbach Publications, 2007, works.bepress.com/katherine_strandburg/11; Katherine J. Strandburg "Freedom of association in a networked world: First amendment regulation of relational surveillance" *Boston College Law Review* 49(171) 2008, papers.ssrn.com/sol3/papers.cfm?abstract_id=1136624
25. International Telecommunication Union *The Internet of things* ITU, 2005, www.itu.int/pub/S-POL-IR.IT-2005/e
26. "An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication." (Definition from en.wikipedia.org/wiki/IP_address).
27. Spencer Ackerman "CIA Chief: We'll spy on you through your dishwasher" *Wired Magazine* 15 March 2012, www.wired.com/dangerroom/2012/03/petraeus-tvremote
28. See opennet.net and google.com/transparencyreport

Canada, to block content and thus restrict freedom of expression and association.[29]

Another threat to associations and assemblies is geographic censorship. Most web platforms now have functionality that serves and withholds content on websites according to geographic location. This is often done for justifiable reasons, like for example a search engine providing relevant results to a search for a place or product based on the user's location. It is also used by streaming and media platforms to ensure that rights protected content is streamed only to regions where it is licensed. Geographic filtering technologies also provide new opportunities for governments to demand censorship of content in their countries. Twitter for example now filters out certain keywords in certain countries at the request of governments.[30]

Another trend is the blocking of access to the internet, cell phone networks, or particular online services and protocols to restrict the ability of people to assembly peacefully. During the "Arab spring" it is well documented that governments completely blocked internet access, or slowed it down to a trickle in order to try to restrict freedom of peaceful association. Examples can be found from Google's Transparency website which has recorded the blocking of internet access in Egypt, Libya and Syria during protests. In Egypt, during the "January 25" protests, internet access was blocked for a number of days.[31]

Western governments which have often espoused the use of ICTs for freedom of association assembly have also blocked access to the internet and cell phone networks, or publicly considered such measures to restrict assemblies. In San Francisco the government-owned corporation, the Bay Area Rapid Transit Authority (BART) shutdown the underground mobile network base-stations along the transport routes in order to pre-emptively restrict communications between peaceful protesters protesting against the killing of an unarmed homeless man by BART security.[32] During the London riots, the British government summoned representatives from Facebook, Twitter and Research in Motion (Blackberry) in order to discuss the possibility of restricting access to these services during social unrest.[33] Although the UK riots were not peaceful assemblies, the use of these tools remain important in all kinds of protests – they allow people to report incidents of violence, to convey information about violent or unsafe hotspots and to coordinate safe routes away from violent activity as well as to contact emergency services or coordinate ad-hoc emergency assistance.

Government and corporate responses to online anonymity

Frank La Rue, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, in his report states:

> The right to privacy is essential for individuals to express themselves freely. Indeed, throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously. The Internet allows individuals to access information and to engage in public debate without having to reveal their real identities, for example through the use of pseudonyms on message boards and chat forums.[34]

Despite this, some governments and corporations are becoming increasingly intolerant of online anonymity and are seeking to legislate or create policies that prevent the use of anonymous monikers on online platforms, or require users to register with personally identifying information.

29. Helmi Noman and Jillian C. York "West censoring East: The use of Western technologies by Middle East censors, 2010-2011" *OpenNet Initiative* March 2011, opennet.net/west-censoring-east-the-use-western-technologies-middleeast-censors-2010-2011
30. Martin Carstens "Twitter changes its policy on global censorship" *memeburn* 27 January 2012, memeburn.com/2012/01/twitter-changes-its-policy-on-globalcensorship
31. See google.com/transparencyreport and an analysis of this data in Raoof "The internet and social movements" and Comninos "E-revolutions".
32. For an overview of the operation in protest against BART see: "The War and Peace Report" (news show), Democracy Now!, 16 August 2011, www.democracynow.org/2011/8/16/stream; and "Vince in the Bay, Disorderly Conduct – Operation BART Recap" (podcast), 17 August 2011, www.blogtalkradio.com/vinceinthebay/2011/08/17/disorderly-conduct—operation-bart-recap-1
33. Ravi Somaiya, "In Britain, a meeting on limiting social media" *The New York Times* 25 August 2011, www.nytimes.com/2011/08/26/world/europe/26social.html?_r=1&src=tp
34. Frank La Rue *Report of the Special Rapporteur*

Some would argue that there are dangers presented by anonymous communication online. Trust, for example, is an issue in anonymous communication. If the source of information is anonymous its reliability may be in question. Another problem is *astroturfing* – the creation of multiple fake identities to emulate grassroots movements and then post material arguing for a political or economic objective. Astro-turfing software, which can manage multiple fake identities, can apparently now be purchased from specialised software companies.[35] The manipulation of online associations through astroturfing presents new challenges to freedom of association and assembly. Some argue that anonymity increases the capacities of cyber-criminals, who can use this anonymity to commit crimes.[36] However, anonymity cannot and should not, as Randi Zuckerberg, ex-marketing director of Facebook has suggested, just "go away".[37] Despite calls by some authorities – the British Police for example – to end the use of anonymous monikers on online platforms,[38] online anonymity needs to be protected. Restrictions on online anonymity would have chilling effects on freedom of association and assembly.

There are legitimate reasons for people not to use their real names online. Anonymity provides an enabling environment for people to seek help with problems that have a social stigma like drug addiction, illnesses such as HIV-AIDS, or sexual abuse. Pseudonyms or monikers may also be a useful way for women, children and vulnerable groups to avoid cyberbullying or real-life violence in response to their online activities as well as to seek confidential help after becoming victims of violence or abuse. In some countries certain types of sexuality are criminalised or people with sexualities deviating from the "norm" are subject to violence and abuse. Some lesbian, gay, bisexual, transgender and intersex (LGBTI) people face the risk of violence or punitive measures including imprisonment or execution. Online anonymity is an important tool for LGBTI communities to associate safely.

Restrictions on private associations can have chilling effects on freedom of association, and thus so do restrictions on anonymity online. Laws against online anonymity can have unintended consequences that can outweigh the benefits, for example endangering the privacy, information security, and property of netizens. In 2007 South Korea introduced regulations that required citizens to register with their real name and resident registration (ID) number to use the internet, as well as to use South Korean websites. After a few incidents in which personal information was leaked there has had to be a revision of this system. In July 2011, personal information including resident registration numbers of up to 35 million websites was stolen by hackers. In November 2011, a database of names, emails and other personal information from an online game was hacked and the personal details of 13 million South Koreans including resident registration numbers and passwords were leaked online. There are also reports of an online market for South Korean resident registration numbers, which are bought by people wishing to play online South Korean games that require these numbers to play. South Korea is now considering repealing the regulations governing the online real-name system as well and is also considering measures to stop online companies from collecting and storing resident registration numbers.[39]

35. John Herrman "Online astroturfing gets sophisticated" *smartplanet* 23 February 2011, www.smartplanet.com/blog/thinking-tech/online-astroturfing-gets-sophisticated/6349; Kit Dotson "Generating crowds: Astroturfing propganda software and social media collide" *siliconAngle* 21 February 2011, siliconangle.com/blog/2011/02/21/generating-crowds-astroturfingpropaganda-software-and-social-media-collide
36. See for example a discussion of this: Jonathan Lusthaus "Trust in a World of Cybercrime" *Global Crime* 13(2) May 2012, pp. 71–79. The author argues that anonymity presents both opportunities and challenges as it provides them with a guise to commit criminal acts, however cybercriminals also need to develop trust and build reputation with clients, thus making anonymity a cost as well as a benefit for them.
37. Adam Clark Estes "Randi Zuckerberg's ill-timed statements about anonymity online" *The Atlantic Wire* 3 August 2011, www.theatlanticwire.com/technology/2011/08/randizuckerbergs-ill-timed-statements-about-anonymityonline/40808
38. Adrian Chen "Clueless British police suggest Twitter require realnames" *Gawker* 26 August 2011, gawker.com/5834776
39. Graham Cluley "Data stolen from 35 million South Korean social networking users" *Naked Security* July 28 2011, nakedsecurity.sophos.com/2011/07/28/data-stolen-from-35-million-south-korean-social-networking-users; Yoon Ja-young "Online ID system faces overhall" *Korean Times* 23 December 2011, www.koreatimes.co.kr/www/news/biz/2011/12/123_101459.html; Kate Jhee-Yung Kim "Lessons learned from South Korea's Real-Name Policy" *Korea IT Times* 17 January 2012, www.koreaittimes.com/story/19361/lessons-learned-south-koreas-real-nameverification-system

Online protests

New forms of online protests are not well covered by national legislation and human rights law. Much legislation has not defined what is a legitimate and legal online protest and what is not. Human rights instruments also do not clearly address these issues. Human rights instruments and many constitutions explicitly protect the freedom of peaceful assembly and thus the right to conduct peaceful and lawful protests. It seems common sense that violence cannot occur on the internet, but rather occurs through the internet (e.g. the internet can be used as a tool to identify victims of violence and coordinate violent activities, but internet content cannot itself physically harm anyone). Destruction of property as well as the theft of private information or money can of course also happen online. Human rights instruments need to clearly address what forms of online protest are legitimate, and should be protected.

An often used form of online protest in the past two years has been distributed denial of service (DDoS) attacks. DDoS attacks involve the continuous flooding of a website by many users with useless information. This can cause the website to slow down or go offline. DDoS must be conducted from a large number of computers in order to be effective. The first well-known use of DDoS was in 1997 and targeted Mexican government and corporate websites in protests in sympathy with the Zapatistas in Mexico and the repression they and agriculturalists experienced in the Chiapas area, which included being victims of paramilitary violence. In the last two years there have been various protests in the form of DDoS – this included DDoS against a UK law firm in response to threatening letters sent to alleged file sharers; DDoS of Mastercard, VISA and Paypal in response to these companies cutting off donations and funding to Wikileaks; and DDoS of Sony servers in protest against a court case filed by Sony against computer science enthusiast George Hotz for the development of a software to unlock Sony Playstation gaming consoles and allow modifications. There are also many examples of DDoS attacks on government websites in the Middle East and North Africa region during the Arab spring. During the recent Formula 1 (F1) Grand Prix in Bahrain, there were DDoS attacks against F1 sites in protest against the event being held there despite the worrying human rights situation. In 2011 there were arrests and court cases in the Netherlands, Spain, Turkey, United Kingdom and US for participation in DDoS.

Is DDoS a form of peaceful assembly? Is it a form of peaceful and lawful protest? Many argue that partaking in a DDoS attack can be an act of protest — the online version of a sit-in. A DDoS attack will usually only take down a website for a short amount of time, until the attacks cease — like protesters outside a building stopping business activities from happening until the protest ends. DDoS does not alone generally compromise the security of a site and allow for the stealing of information unless the target site is hacked and exploited while it is weakened. Due to its similarity to offline forms of protests some have argued that DDoS is a legitimate form of protest. Others have argued that criminalizing such protest activity can have negative consequences for democracy.[40]

In 2011 after a court case involving DDoS attacks against the airline Lufthansa for their involvement in the deportation of illegal immigrants, politically motivated DDoS attacks were recognized in a German court as a legitimate form of protest rather than a crime. DDoS of course cannot be legitimately used for criminal purposes, for example extortion. A German court has recently ruled that using DDoS for extortion could involve sentences of up to 10 years in prison. A distinction needs to be drawn between a DDoS attack conducted by people and attacks conducted by "botnets" controlled by hackers — networks of "zombie" computers that have been infected with viruses or malware. Botnets do the bidding of their "herders," which can be anything from sending spam or stealing information to conducting DDoS attacks. Botnets harm both their targets and the unwilling owners of zombie machines and can thus clearly infringe on freedom of expression and association. People using DDoS tools should be assessed differently from those using botnets.

It has also been argued by many that DDoS may infringe on other peoples' rights to freedom of expression (e.g. publishing information on websites) and access to

40. James Ball "By criminalising online dissent we put democracy in peril" *The Guardian* 1 August 2011, Www.guardian.co.uk/commentisfree/2011/aug/01/onlinedissent-democracy-hacking

information (e.g. retrieving information from websites). While DDoS should not be criminalised as a form of protest, it may need to be balanced against other rights in assessing the effects of such protests.

CONCLUSION: A HUMAN RIGHTS-BASED APPROACH TO FREEDOM OF ASSOCIATION AND ASSEMBLY AND THE INTERNET

The Special Rapporteur on the freedom of peaceful assembly and of association, has recognised that:

> The word 'association' refers, inter alia, to civil society organizations, clubs, cooperatives, NGOs, religious associations, political parties, trade unions, foundations or even online associations as the Internet has been instrumental, for instance, in 'facilitating active citizen participation in building democratic societies'.[41]

He has also recommended "to recognize that the rights to freedom of peaceful assembly and of association can be exercised through new technologies, including through the Internet."[42] The report however lacks a detailed focus on the conceptualisation of freedom of association and of peaceful assembly online.

> As he has mainly received information regarding allegations impacting civil society's work since the inception of his mandate, and due to the word limit, [his report has primarily focused] on this type of association, but will address others when relevant. This will not prevent him from focusing on other forms of associations in his future reports.[43]

This should serve as an invitation to international organisations, governments, activists, human rights defenders, scholars, and lawyers concerned with the internet and human rights to more deeply conceptualise how these rights are exercised online, as well as the relationships between the internet and these rights. The examples of new challenges to freedom of association and assembly above, and the lack of clarity in national legislation and human rights instruments as to how freedom of association and freedom of peaceful assembly should be approached in relation to the internet point to the need for human rights organisations, civil society, activists and governments to adopt a human rights approach and to better conceptualise what these freedoms mean in the internet age.

Human rights apply online just as they do offline. This is why "internet rights are human rights" is the message of APC's Connect Your Rights Campaign. Freedom of association and assembly should be protected online, the same way they are protected offline. Nonetheless the nature of communications in the online and offline worlds are quite different, and these differences need to be understood in order to correctly identify where these freedoms are exercised and what threats to these freedoms may be posed.

41. Kiai *Report of the Special Rapporteur*, para 52, citing La Rue *Report of the Special Rapporteur*, para 1.
42. Kiai *Report of the Special Rapporteur*, para 52.
43. Ibid.

Distinguishing between online assembly and online association

Freedom of expression and freedom of association are perhaps better applied to the online world, as this is done by using the metaphors of speech, print, and networks of people. To understand assembly online we apply the metaphor of a physical gathering or meeting, or of a protest. It is hard to identify however exactly when something becomes an assembly online, rather than an association or a series of communications.

Offline it is hard to distinguish exactly between the act of associating and the act of assembling, or between associations or networks and assemblies. Online this becomes more difficult. Consider a few examples of assembly and association on the internet:

1. A Facebook Group, based around a particular interest, for example women in ICT in Uganda

2. An online forum for discussion of a nervous system disorder called Charcot-Marie-Tooth

3. A discussion around a Twitter hashtag, about protests in Bahrain during the Formula 1 Grand Prix (#F1)

4. An internet relay chat channel (chat room) called #SOPA where issues around internet legislation like SOPA and PIPA are discussed, and advocacy campaigns and protests are organised

5. An email petition against the Anti Counterfeiting and Trade Agreement (ACTA).

One could say that the Facebook group (1) and the web forum (2) are associations or networks of people coming together around certain issues, and the Twitter hashtag (3), IRC chat (4) are online assemblies or meetings of people, and the email petition (5) is an online protest, thus a peaceful assembly. But it would not be easy to classify these examples absolutely. The Facebook group, the forum or the twitter hashtag for example can also serve as a meeting place and could be counted as an assembly. If the discussion was frequent it would be more of an assembly, if the discussion was less frequent, it would be less so. An internet relay chat room is more easily conceived of as a meeting or assembly of people, but it may also be an association of people or group of associations and networks pursuing common interests.

The intricacy with which the concepts of association and assembly are intertwined, and the difficulty in cleaving them apart perhaps suggests that these two rights need to be dealt with by means of an integrated approach which acknowledges their similarities and interdependence, and that the exercise of these rights face the same challenges and opportunities.

Joy Liddicoat of APC summarises the challenges and opportunities for extending accountability and recourse to human rights to the online world

> There are more opportunities at global levels for recourse for human rights violations than ever before. Yet these appear largely underutilised in relation to the internet and human rights... At the same time, new human rights standards and mechanisms are emerging in relation to freedom of expression and freedom of association... Taking a rights-based approach to the internet and human rights may provide a way to negotiate these complex issues, to build broad consensus on the application of human rights standards.[44]

A rights based approach to the internet and human rights "is a practical way to implement human rights standards" to areas of human rights "where no specific rights standards seem to apply".[45] A rights based approach was first articulated in an ad-hoc committee of the Office of the UN High Commissioner for Human Rights. It was indicated that such an approach should:[46]

- Emphasise the *participation* of individuals in decision making
- Introduce *accountability* for actions and decisions, which can allow individuals to complain about decisions affecting them adversely
- Seek *non-discrimination* of all individuals through the equal application of rights and obligations to all individuals
- *Empower* individuals by allowing them to use rights as leverage for action and legitimise their voice in decision making
- Link decision making at every level to the *agreed human rights norms* at the international level as set out in the various human rights covenants and treaties.

Protecting freedom of peaceful assembly and of association on the internet requires a rights based approach that acknowledges the right to freedom of association is dependent on the protection of other rights. Freedom of peaceful assembly and of association are threatened when other rights are threatened, for example freedom of expression and opinion and freedom from surveillance/the right to privacy. In environments in which freedom of expression is threatened, in which people are threatened with negative consequences for expressing certain opinions online, freedom of association is threatened. In environments in which the right to privacy is threatened – one in which users are lead to believe that their communications are subject to surveillance by governments, corporations, criminal or other actors – freedom of association is also threatened.

Associations cannot be formed online if the electronic space is blocked, and people cannot assemble online if the networks themselves are blocked or not allowed to function. In addition, people also cannot associate or assemble online if their communications and networking is rendered insecure, or if there are invasions on their privacy. The internet must create an enabling environment that protects freedom of association. In order to do this, the privacy of individuals and the security of their information/ data needs to be protected.

Some rights are more important to certain people and less important to others in their exercise of freedom of association. For example privacy may be more important to activists under repressive regimes. Some people may value the right to freedom of expression more than the right to be able to form private associations. Some assemblies of people may wish to remain anonymous and in a private space because of the issues that they deal with, which may involve stigma in society for example, associations and assemblies dealing with alcohol and drug addiction, victims of violence or sexual abuse, LGBTI issues, or organisations for sex workers and HIV positive people. Nonetheless maximum protection for all these different rights concerns should be provided in all contexts, without assuming different preferences for the different actors involved. In protecting the rights to freedom of association and assembly online, different online and social contexts must be considered so as to afford the maximum protection for everybody's right to freedom of association and assembly.

44. Joy Liddicoat "Conceptualising accountability and recourse" *Global Information Society Watch 2011: Internet rights and democratisation* APC and HIVOS 2011, www.giswatch.org/en/2011
45. Ibid.
46. High Commissioner for Human Rights *Report of the High Commissioner's Expert Group on Human Rights and Biotechnology* OHCHR, Geneva 2002, para 21. Cited in Liddicoat "Conceptualising accountability".

RECOMMENDATIONS TO THE SPECIAL RAPPORTEUR, THE HUMAN RIGHTS COUNCIL AND TO OTHER BODIES CONCERNED WITH HUMAN RIGHTS INSTRUMENTS

International human rights instruments need to be further developed to incorporate the explicit protection of freedom of peaceful assembly and of association online, as well as the protection of the right to use ICTs to associate and peacefully assemble offline. Human rights practitioners should take cognisance of existing, non-binding internet rights charters developed by civil society organisations which offer some pointers as to how the rights to freedom of peaceful assembly and association may be protected online.[47]

The Internet Rights and Principles Charter states in section 7, "Freedom of Online Assembly and Association", that:

- Everyone has the right to form, join, meet or visit the website or network of an assembly, group or association for any reason.
- Access to assemblies and associations using ICTs must not be blocked or filtered.

The APC Internet Rights Charter under Theme 2: "Freedom of expression and association" suggests the importance of the following rights online:

- "2.1 The right to freedom of expression. Freedom of expression should be protected from infringement by government and non-state actors. The internet is a medium for both public and private exchange of views and information across a variety of frontiers. Individuals must be able to express opinions and ideas, and share information freely when using the internet.
- 2.2 The right to freedom from censorship. The internet must be protected from all attempts to silence critical voices and to censor social and political content or debate.
- 2.3 The right to engage in online protest. Organisations, communities and individuals should be free to use the internet to organise and engage in protest.

The APC charter under Theme 5: Privacy surveillance and encryption states the importance of the following rights:

- 5.1 The right to data protection. Public or private organisations that require personal information from individuals must collect only the minimal data necessary and for the minimal period of time needed. They must only process data for the minimal stated purposes...[48]
- 5.2 The right to freedom from surveillance. People should be able to communicate free of the threat of surveillance and interception.
- 5.3 The right to use encryption. People communicating on the internet must have the right to use tools which encode messages to ensure secure, private and anonymous communication.

Respecting these rights and freedoms would be a good start towards protecting freedom of peaceful assembly and association online.

In light of the human rights instruments outlined in the paper, the internet rights charters outlined above, and new online threats to peaceful assembly, it is the author's view that freedom of peaceful assembly and association should include:

- Freedom of online assembly and association: the freedom for individuals and groups to form associations online and assemble online to pursue common interests.
- Freedom to use the internet for peaceful assemblies and for associations: the freedom for individuals and groups to use the internet and other ICTs to form associations and organise peaceful assemblies.

47. For an overview of these see Dixie Hawtin "Internet charters and principles" *Global Information Society Watch 2011: Internet rights and democratisation*, APC and HIVOS 2011, www.giswatch.org/en/2011

48. This right continues with: "Collection, use, disclosure and retention of this information must comply with a transparent privacy policy which allows people to find out what is collected about them and to correct inaccurate information. Data collected must be protected from unauthorised disclosure and security errors should be rectified without delay. Data must be deleted when it is no longer necessary for the purposes for which it was collected. The public must be warned about the potential for misuse of data supplied. Organisations have a responsibility to notify people when the information has been abused, lost, or stolen."

- **Freedom to protest online**: the freedom for individuals and groups to use the internet and other ICTs for peaceful online protests that respect the rights of others.

- **Freedom to use the internet for protest in physical public spaces**: the freedom for individuals and groups to use the internet and other ICTs for peaceful protests in physical public spaces that respect the rights of others.

- **Freedom of private and anonymous online assembly and association**: the freedom to use the internet and ICTs to form private associations and conduct private assemblies, in an environment in which the right to privacy is respected, and the right to use encryption and security applications to secure data, as well as anonymity to protect one's privacy is respected.

ASSOCIATION FOR PROGRESSIVE COMMUNICATION

Internet and ICTs for social justice and development

APC is an international network of civil society organisations founded in 1990 dedicated to empowering and supporting people working for peace, human rights, development and protection of the environment, through the strategic use of information and communication technology (ICTs).

We work to build a world in which all people have easy, equal and affordable access to the creative potential of ICTs to improve their lives and create more democratic and egalitarian societies.

www.apc.org info@apc.org

Commissioned by the Association for Progressive Communications (APC)

Conducted with support from the Swedish International Development Cooperation Agency (Sida).

FREEDOM OF PEACEFUL ASSEMBLY AND FREEDOM OF ASSOCIATION AND THE INTERNET

June 2012

APC-201206-CIPP-I-EN-DIGITAL-156
ISBN: 978-92-95096-65-3

ISBN 978-92-95096-65-3