

**SPECIAL SELECTION OF ARTICLES
PRODUCED IN ADVANCE OF PUBLICATION**

Global Information Society Watch

2011

Global Information Society Watch 2011

Steering committee

Anriette Esterhuysen (APC)
Loe Schout (Hivos)

Coordinating committee

Karen Banks (APC)
Monique Doppert (Hivos)
Karen Higgs (APC)
Marjan Besuijen (Hivos)
Joy Liddicoat (APC)
Pablo Accuosto (APC)
Valeria Betancourt (APC)

Project coordinator

Karen Banks

Editor

Alan Finlay

Assistant editor

Lori Nordstrom

Publication production

Karen Higgs and Analía Lavin

Graphic design

MONOCROMO
info@monocromo.com.uy
Phone: +598 2 400 1685

Cover illustration

Matías Bervejillo

Proofreading

Valerie Dee and Lori Nordstrom

Financial partners

Humanist Institute for Cooperation with Developing Countries (Hivos)
Swedish International Development Cooperation Agency (Sida)

Printed in Goa, India
by Dog Ears Books & Printing

Global Information Society Watch
Published by APC and Hivos
2011

Creative Commons Attribution 3.0 Licence
<creativecommons.org/licenses/by-nc-nd/3.0/>
Some rights reserved.

ISSN to be delivered

APC-20111-CIPP-R-EN-PDF-0105
978-92-95096-14-1

Preface

Unlike any other medium, the internet enables individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders. Unlike any other technological development, it has created an interactive form of communication, which not only allows you to send information in one direction, but also to send information in many directions and receive an immediate response. The internet vastly increases the capacity of individuals to enjoy their right to freedom of opinion and expression, including access to information, which facilitates the exercise of other human rights, such as the right to education and research, the right to freedom of association and assembly, and the right to development and to protect the environment. The internet boosts economic, social and political development, and contributes to the progress of humankind as a whole; but it is especially an instrument that strengthens democracy by facilitating citizen participation and transparency. The internet is a “plaza pública” – a public place where we can all participate.

The past year has been a difficult time globally: whether the aftermath of the tsunami in Japan, unsteady global markets, post-election riots in Nigeria, civil war in Libya and a military clampdown in Syria. But there have been positive, and equally challenging, developments in countries such as Tunisia and Egypt. Throughout the year people around the world have increasingly used the internet to build support for human rights and social movements. This edition of Global Information Society Watch (GISWatch) offers timely commentary on the future of the internet as an open and shared platform that everyone has the right to access – to access content and to have access to connectivity and infrastructure.

Through the lens of freedom of expression, freedom of association and democracy, the thematic reports included here go to the heart of the debates that will shape the future of the internet and its impact on human rights. They offer, amongst other things, an analysis of how human rights is framed in the

context of the internet, the progressive use of criminal law to intimidate or censor the use of the internet, the difficult role of intermediaries facing increasing pressure to control content, and the importance of the internet to workers in the support of global rights in the workplace. Some call for a change of perspective, as in the report on cyber security, where the necessity of civil society developing a security advocacy strategy for the internet is argued. Without it, the levels of systems and controls, whether emanating from government or military superpowers, threaten to overwhelm what has over the years become the vanguard of freedom of expression and offered new forms of free association between people across the globe.

Many of these issues are pulled sharply into focus at the country level in the country reports that follow the thematic considerations. Each of these country reports takes a particular “story” or event that illustrates the role of the internet in social rights and civil resistance – whether positive or negative, or both. Amongst other things, they document torture in Indonesia, candlelight vigils in South Korea, internet activism against forgetting human rights atrocities in Peru, and the rights of prisoners accessing the internet in Argentina. While the function and role of the internet in society remains debated, and necessarily so, in many contexts these stories show that to limit it unfairly will have a harmful impact on the rights of people. These stories show that the internet has become pivotal in actions aimed at the protection of human rights.

GISWatch makes a valuable contribution to dialogue on freedom of expression, freedom of association and democratisation and seeks to inspire and support collaborative approaches. ■

Frank La Rue

UNITED NATIONS SPECIAL RAPPOREUR
ON THE PROMOTION AND PROTECTION OF THE RIGHT
TO FREEDOM OF OPINION AND EXPRESSION

Conceptualising accountability and recourse

Joy Liddicoat

Association for Progressive Communications

www.apc.org

Introduction

The modern foundations of international human rights rest on the Universal Declaration of Human Rights (UDHR) and the Charter of the United Nations (UN).¹ The UDHR affirmed human rights are universal, inalienable and interconnected. The human rights framework recognises both the right of states to govern and the duty of states to respect, protect and promote human rights. The global transformation of human rights from moral or philosophical imperatives into a framework of rights that are legally recognised between nations continued into the 21st century, but this basic framework has been reaffirmed by UN member states and remains the foundation of human rights today.² The internet has been used to create new spaces in which human rights can be exercised and new spaces in which rights violations can take place. This report looks at human rights concepts, the internet and accountability mechanisms for internet-related human rights violations.³

The human rights framework

The UDHR is not legally binding but has a powerful moral force among UN member states. Binding standards have been developed, including the International Covenant on Civil and Political Rights (ICCPR)⁴ and the International Covenant on Economic, Social and Cultural Rights (ICESCR).⁵ Together with the UDHR, these two standards have become known as the International Bill of Human Rights.⁶ Other international human rights standards followed, including the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment.⁷

1 The United Nations officially came into existence after ratification of the Charter on 24 October 1945.

2 The 1993 Vienna World Conference on Human Rights reaffirmed that human rights are indivisible and interrelated and that no right is superior to another. UN General Assembly (1993) *Vienna Declaration and Programme of Action*, Article 5. [www.unhcr.ch/huridocda/huridoca.nsf/\(symbol\)/a.conf.157.23.en](http://www.unhcr.ch/huridocda/huridoca.nsf/(symbol)/a.conf.157.23.en)

3 “Accountability mechanisms” range from international mechanisms, to litigation, to community action and lawful forms of protest.

4 The ICCPR includes rights related to the right to vote, freedom of expression, freedom of association, and the rights to a fair trial and due process.

5 The ICESCR includes rights related to the right to health, the right to education, the right to an adequate standard of living, and the right to social security.

6 Office of the High Commissioner for Human Rights (1996) *Fact Sheet No. 2 (Rev. 1) The International Bill of Human Rights*, United Nations, Geneva. www.ohchr.org/Documents/Publications/FactSheet2Rev.1en.pdf

7 Others include the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), the Convention on the Rights of the Child (UNCROC), and the Convention on the Rights of Persons with Disabilities (CRPD).

Accountability and remedies

When the UDHR was being negotiated, litigation was not seen as the appropriate way to seek remedies or accountability between nations (nor was there an international court system). New forums were established, including the Security Council, the Human Rights Committee and, more recently, the Human Rights Council. Accountability to these forums was primarily by way of periodic reporting. Once a state had ratified a treaty (such as the ICCPR) it agreed to periodically report on implementation, but ratification was also permitted with reservations. Some treaties adopted complaint procedures for individual complaints (which are known as optional protocols), but states are not obliged to submit to these. Each treaty has different standards for accountability. For example, states are obliged to implement economic, cultural and social rights as resources allow, through a system known as “progressive realisation”. Civil and political rights, on the other hand, must be implemented immediately and some, such as freedom from torture, can never be suspended or limited, even in emergency situations.

The premise underlying these forms of accountability is that states, as equal members of the international community of nations, will subject their conduct to the scrutiny of other states. In doing so states also agree to abide by recommendations or take into account observations made about matters within their own borders. States therefore agree to be publicly accountable for their human rights performance. This was a major transformation in the international community of states.

In practice, the effectiveness of these accountability mechanisms varies widely. Some treaty body processes⁸ are seen as very ineffective: the reporting processes are cumbersome, lengthy and time consuming for states and civil society groups alike. Some states simply do not file their periodic reports. For these and other reasons the treaty body processes are currently being reviewed.⁹ Other mechanisms, such as the Universal Periodic Review, are seen as much more effective.

This variability has implications for civil society groups, which must strategise carefully about the use of different or multiple mechanisms depending on a number of factors, including the issue, and whether the context is national or local. Multiple mechanisms might be used at the same time, over time, or not at all, depending on the particular issues and context.

8 Treaty body processes refers to the various mechanisms for oversight of implementation of treaties; for example, the Committee for the Elimination of All Forms of Discrimination Against Women oversees the CEDAW convention and the Human Rights Committee oversees the ICCPR.

9 www2.ohchr.org/english/bodies/HRTD/index.htm

The human rights framework also has limitations. As a forum of governments the UN is necessarily infused with politics. Agreed human rights standards are, generally, the product of the best possible political consensus. The result is often a minimum standard: the lowest common denominator of agreement. The international human rights system is still evolving, with the UN's mandate under constant scrutiny, and its utility questioned in the face of the modern horrors of human rights violations. In addition, the framework itself is not static. The UN system is evolving with new processes such as the Universal Periodic Review providing new opportunities for scrutiny and leadership. While changes may be positive, these take time to implement, requiring civil society organisations (CSOs) to develop or enhance capacity to engage and use them effectively while also trying to advance their issues and concerns.

Yet the UN – and the Human Rights Council in particular – remains the central global human rights forum. Opportunities for recourse against states, as ways to hold them accountable for human rights violations, must be considered taking into account both strengths and limitations of the international human rights framework. And today there are more processes for state accountability for human rights violations than have ever existed. These include:

- Scrutiny by treaty bodies
- Complaints to UN bodies under optional protocols
- Engagement with special procedures of the UN (for example, the Special Rapporteurs on Freedom of Opinion and Expression, Freedom of Association and Human Rights Defenders)
- State peer review in the Universal Periodic Review process
- Formal complaints to regional mechanisms, for example, the European Court of Human Rights, the Inter-American Court on Human Rights or the African Court on Human and People's Rights
- Complaints to or investigations by ombudspersons or national human rights institutions
- Litigation (where national constitutions allow for this or where international standards have been incorporated into domestic law).

As human rights violations in relation to the internet increase,¹⁰ questions arise about accountability and remedies. The implications for internet-related human rights violations cannot be considered without first looking at the internet-related forums in the UN.

Human rights and the internet at the UN

Despite the centrality of human rights to the creation of the UN, the World Summit on the Information Society (WSIS),¹¹ the WSIS Geneva Declaration of Principles¹² and the Internet Governance Forum (IGF),¹³ discussions about accountability for human rights violations remain limited. Tensions have emerged given the openness of the internet, which has been both a factor in its success and a point of political contention in debates about internet governance.¹⁴ Early adopters of the internet and information and communications technologies (ICTs) reached for rights as a way to navigate these tensions by articulating their freedom to use and create online spaces, to assert their rights to communicate and share information, and to resist state or government interference with rights to privacy.¹⁵ The simple application of existing human rights standards was the starting point for civil society groups and, building on the work of the People's Communication Charter, the Association for Progressive Communications (APC) developed the first Internet Rights Charter in 2001-2002 (subsequently updated in 2006).¹⁶ In 2010, the Dynamic Coalition on Internet Rights and Principles released a Charter of Internet Rights and Principles and, in 2011, a more condensed set of ten principles.¹⁷

But further elaboration and clear explanation of how existing human rights standards apply seemed necessary. New charters and statements of principles have emerged in regional bodies (such as the Council of Europe) and nationally (for example, in Estonia and Finland).¹⁸ It is not yet clear if a new "Super Charter" will emerge or if a new model national law will be developed.

The internet-related aspects of freedom of expression and freedom of association have received some scrutiny in UN human rights mechanisms. The 2011 annual report of the Special Rapporteur on Freedom of Opinion and Expression¹⁹ was the first time the Human Rights Council had considered a report specifically focused on human rights and the internet. In 2010, the Human Rights Committee began a review of

11 World Summit on the Information Society, United Nations and International Telecommunication Union (2005) WSIS Outcome Documents. www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2316

12 Article 19 of the UDHR is cited in paragraph 4 of the Geneva Declaration of Principles (2003).

13 www.intgovforum.org

14 Cavalli, O. (2010) Openness: Protecting Internet Freedoms, in Drake, W. J. (ed) *Internet Governance: Creating Opportunities for All*, United Nations, New York, p. 15.

15 One of the more famous examples was John Perry Barlow's Declaration of the Independence of Cyberspace (February 1996). projects.eff.org/~barlow/Declaration-Final.html

16 www.apc.org/en/node/5677

17 www.internetrightsandprinciples.org

18 In relation to Estonia, see Woodard, C. (2003) Estonia, where being wired is a human right, *Christian Science Monitor*, 1 July. In relation to Finland, see Ministry of Transport and Communications (2009) *732/2009, Decree of the Ministry of Transport and Communications on the minimum rate of a functional Internet access as a universal service*. www.finlex.fi/en/laki/kaanokset/2009/en20090732

19 La Rue (2011) op. cit.

10 La Rue, F. (2011) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, 26 April, A/HRC/17/27, p. 8-15.

General Comment 34 (a key document which the Committee uses to interpret Article 19 of the ICCPR) and released its preliminary report in May 2011.²⁰ The new general comment includes specific reference to “electronic and internet-based modes of expression”.²¹ This will strengthen the mechanisms for recourse and reporting internet-related violations of freedom of expression under Article 19 by requiring states to include these in their reports. The final revised comment was released in June 2011 and should be available for use in periodic reporting and other accountability mechanisms by early 2012.

These various initiatives are welcome, but more work needs to be done to ensure the internet is a cross-cutting issue within all treaty bodies and human rights mechanisms. The topic of human rights, the internet and accountability mechanisms remains complex for a variety of reasons, including:

- The complexity of the internet ecosystem (for example, no single point of governance and network operation, diverse standard-setting systems, the role of internet intermediaries and platform providers, and so on) and the various connection points of that ecosystem with the human rights ecosystem (or lack of connection points).
- While there may be a single international human rights standard (for example, on freedom of expression) there is no single way and no single correct way to give effect to that standard.
- The diverse ways that human rights issues arise; for example, from privacy and surveillance, to the ICT production line (conflict minerals, the rights of workers), to content filtering, content blocking and harassment, arrest and detention of online human rights activists.
- Human rights violations may involve multiple and intersecting rights across different treaties and affect groups differently (such as women, sexual and gender minorities, people with disabilities, or racial and cultural minorities).
- The application of human rights standards to the fast-changing forms of connectivity (mobile is outpacing other forms of connectivity, for instance).²²
- The nebulous legal environments of many countries, including absence of the rule of law (or ineffective legal systems), lack of legislation and constitutional protections or, conversely, over-regulation and extensive direct or indirect censorship.²³

- The diverse human rights situations in diverse countries, especially within and between developed and developing countries.
- The actual and perceived limitations of human rights remedies where the state violates human rights or where non-state actors can act with impunity.
- The frequent need to obtain remedy or recourse quickly and the slow and cumbersome nature of most legal processes.
- The cost of litigation and the lack of access to this remedy for many individuals and groups.
- The geopolitics and how these play out in various forums.
- The multiple and sometimes conflicting mechanisms for remedy within countries (for example, in relation to content censorship, the intersections of defamation law, constitutional protections where these exist, and criminal or civil legislation for different types of material).

What future for accountability mechanisms?

Given these complexities it is perhaps no surprise that those discussing internet rights charters and principles have steered away from creating new accountability mechanisms – none appear to contain new complaints procedures. The question is, can the existing human rights framework provide adequate accountability mechanisms for internet-related human rights violations?

The answer is unclear. A mixed picture emerges from current practice. Some CSOs have been active in the Universal Periodic Review process.²⁴ Regional human rights mechanisms (such as the European Court of Human Rights) are receiving increasing numbers of complaints²⁵ together with strategic interventions in litigation by CSOs.²⁶ But no complaints have been received by the African Special Rapporteur on Freedom of Expression in relation to freedom of expression and the internet.²⁷ There have been few complaints to national human rights institutions, possibly because these have not yet adequately considered how to deal with internet-related complaints.²⁸ Civil litigation remains a primary way to gain recourse in many countries.²⁹

More research is needed to develop a better global picture of the use of these various mechanisms and monitor change. For example, some mechanisms may be best suited

20 Human Rights Committee (2011) *Draft General Comment No. 34 (upon completion of the first reading by the Human Rights Council)*, 3 May, CCPR/C/GC/34/CRP.6.

21 *Ibid.*, para 11.

22 See, for example, Southwood, R. (2011) *Policy and regulatory issues in the mobile internet*, APC. www.apc.org/en/node/12433; Horner, L. (2011) *A human rights approach to the mobile internet*, APC. www.apc.org/en/node/12431; and Cominos, A. (2011) *Twitter revolutions and cyber-crackdowns: User-generated content and social networking in the Arab Spring and beyond*, APC. www.apc.org/en/node/12432

23 For example, in relation to Turkey, see Johnson, G. (2011) *Censorship Threatens Turkey's Accession to EU*, unpublished research paper.

24 Universal Periodic Review (UPR), Thailand: Joint CSO Submission to the Office of the High Commissioner for Human Rights (March 2010), endorsed in whole or in part by 92 Thai organisations.

25 For a summary of recent European Court of Human Rights cases in relation to the internet and human rights see the European Court of Human Rights “New Technologies Fact Sheet” (May 2011).

26 For example, the Electronic Frontier Foundation and Privacy International.

27 Advocate Pansy Tsakula, personal communication to APC, 2011.

28 See, for example, New Zealand Human Rights Commission (2010) *Roundtable on Human Rights and the Internet*. www.hrc.co.nz

29 Kelly, S. and Cook, S. (eds) (2011) *Freedom on the Net 2011: A global assessment of the internet and digital media*, Freedom House, Washington.

to certain types of complaints and offer different remedies. Capacity building also may be needed to support civil society advocacy and strengthen the mechanisms to ensure judicial and other officers adequately understand internet-related human rights issues.

New avenues for global recourse and accountability mechanisms are emerging. The Special Rapporteur on Freedom of Expression has emphasised the need for effective remedies, including rights of appeal.³⁰ In addition, he noted that the internet has created more avenues for use of traditional remedies including the right of reply, publishing corrections and issuing public apologies.³¹ In one defamation case, for example, the settlement agreement included the defendant apologising 100 times, every half hour over three days, to more than 4,200 followers of his Twitter account.³²

A rights-based approach to the internet and human rights

The rights-based approach, or human rights approach as it is also known, was developed as a practical way to implement human rights standards. The rights-based approach was first articulated in the UN in 2002, when the Office of the UN High Commissioner for Human Rights convened an ad hoc expert committee on biotechnology. The committee noted this was a new and emerging area of human rights, with no specific human rights standards. To overcome this difficulty the committee decided to rely on a “rights-based approach” for its task, indicating that such an approach should:³³

- 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 a 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.

This approach has been extended into a wide range of areas, particularly those where no specific human rights standards seem to apply. The approach is increasingly being used to critique internet regulations on access to the internet, privacy, filtering³⁴ and the mobile internet.³⁵ The UN Special Representative on Business and Human Rights has also drawn on the rights-based approach to consider liability of transnational corporations for human rights violations. The resulting framework highlights the need for access to effective remedies, both judicial and non-judicial.³⁶

There is scope to use this approach in other areas, for example, with the mandates of various UN forums that focus on the internet. The recent appointment of a Special Rapporteur on Freedom of Association provides an opportunity to explore such an approach taking account of modern human rights movements, the use of the internet and ICTs to mobilise, and the special situation of human rights defenders seeking to improve democratic participation. New forms of accountability may yet emerge, as well as new remedies that relate specifically to the internet.

Conclusion

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. Diverse and complex factors interact to create this situation and it is difficult for CSOs to develop effective strategies. At the same time, new human rights standards and mechanisms are emerging in relation to freedom of expression and freedom of association, creating new opportunities for recourse. 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, and provide greater access to, and measurement of, accountability mechanisms. ■

30 La Rue (2011) op. cit., para 47.

31 Ibid., para 27.

32 www.thejournal.ie/malaysian-man-apologises-via-100-tweets-in-defamation-settlement-147842-Jun2011

33 High Commissioner for Human Rights (2002) *Report of the High Commissioner's Expert Group on Human Rights and Biotechnology: Conclusions*, OHCHR, Geneva, para 21.

34 Access (2011) *To Regulate or Not to Regulate, Is That the Question? A Roadmap to Smart Regulation of the Internet*, discussion paper released ahead of the OECD High-Level Meeting on the Internet Economy on 28-29 June 2011. www.accessnow.org/policy-activism/docs

35 See footnote 22.

36 Ruggie, J. (2011) *Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises. Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, 21 March, A/HRC/17/31, para. 26-31.

Towards a cyber security strategy for global civil society?

Ron Deibert

The Canada Centre for Global Security Studies and the Citizen Lab,
University of Toronto
www.citizenlab.org

Cyberspace is at a watershed moment. Technological transformations have brought about an architectonic change in the communications ecosystem. Cyber crime has exploded to the point of becoming more than a nuisance, but a national security concern. There is a seriously escalating arms race in cyberspace as governments scale up capabilities in their armed forces to fight and win wars in this domain. Telecommunication companies, internet service providers (ISPs), and other private sector actors now actively police the internet. Pressures to regulate the global network of information and communications have never been greater.

Although states were once thought to be powerless in the face of the internet, the giants have been woken from their slumber. How exactly governments react to these problems will determine the future of cyberspace – and by extension the communications platforms upon which global civic networks depend.

Global civil society, now increasingly recognised as an important stakeholder in cyberspace governance, needs to step up to the challenge. A constitutive moment awaits. What is required is nothing less than a serious and comprehensive *security* strategy for cyberspace that addresses the very real threats that plague governments and corporations, addresses national and other security concerns in a forthright manner, while protecting and preserving open networks of information and communication. It is an enormous challenge but also a great opportunity that, if not handled well, could end up having major detrimental consequences for human rights online. Of course, “global civil society” is not an undifferentiated whole, but an amalgam of multiple and diverse local networks. Regardless of their differences, citizens who share an interest in democracy and human rights also share common interests in a secure but open global communications space. Those common interests can lay the basis for a civil society cyber security strategy.

Prior to laying out the elements of such a strategy, it is useful to take a step back and look at some major social forces that are shaping the domain of global communications. The internet’s de facto and distributed regime of governance – largely informal and driven up to now by decisions of like-minded engineers – has come under massive stress as a function of the internet’s continuing rapid growth. Not only have there been continuing exponential increases in users and deeper penetration into everyday life (a recent Cisco

report¹ said that by 2020, there will be 50 billion “things”, meaning devices, connected to the internet), but there has been a vast growth in the developing world, as millions of new digital natives come online. With these new digital natives come new values and interests that in turn are affecting internet governance, as governments like China, Russia and India exercise their influence. The latter are now key players in several internet governance forums, and have been collectively pushing for the legitimisation of nationalised controls, such as those over the domain naming system. They also have a shared interest in limiting the voices of civil society in these decision-making forums, an interest exemplified by the push to have the United Nations and the International Telecommunication Union (a state-based organisation) take the lead on internet governance. Civic networks need to be vigilant that such a strategy does not succeed.

Another major force shaping cyberspace arises out of technological innovation and economic factors that have created the architectonic shifts in the nature of the ecosystem of global communications. Whereas before the internet was largely a self-segmented and isolated network generally separate from other means of communication, such as television, telephony and radio, all of these media have integrated into a single system of planetary communications, which we call cyberspace. The integration of these media into a common space has happened at the same time that business models and service delivery mechanisms for information and communications have changed fundamentally, with the rise of social networking, cloud computing, and mobile forms of connectivity. This paradigm shift has upset the principles, norms and rules of what used to be just the “internet”, with implications for freedom of speech and access to information. Today, our data is entrusted to vast transnational information empires who act as gatekeepers and increasingly arbiters of what gets communicated, and what information is accessible or not. Market considerations can easily outweigh privacy and other rights concerns, and have already made largely irrelevant so-called “end-to-end” principles that once ensured network neutrality. Even something as benign as a spam filter gone wild can end up unintentionally disrupting political communications, as our research on Apple’s MobileMe filtering system² has shown.

More serious, however, are the ways in which the private sector is being pressured, compelled, and even *incentivised* to “police the internet” by governments looking to download their growing cyberspace controls. For example,

1 www.readwriteweb.com/archives/cisco_50_billion_things_on_the_internet_by_2020.php

2 opennet.net/apple-mobileme-brief

in Canada, the Stephen Harper government is introducing an Omnibus Crime Bill³ through parliament that would require ISPs and telecommunications companies to retain user data, process the data in ways that make it amenable to law enforcement and intelligence, and then share that data with law enforcement representatives – all without judicial oversight. Arrangements like these are not uncommon. Privacy researcher Chris Soghoian has made a career documenting⁴ how private sector actors not only facilitate access to information for law enforcement, but actually derive revenues from doing so. He has also documented extensive variation among these actors on the specifics of their data retention and privacy policies. As a result, citizens using different communications services can live in entirely different universes of rights.

The downloading of policing functions to the private sector – a phenomenon known as “intermediary liability” – extends to the protection of intellectual property. At a recent meeting⁵ on the internet economy organised by the Organisation for Economic Co-operation and Development (OECD) in Paris, the final communiqué argued that ISPs should take on more expansive roles chasing down copyright violators using their networks. Civil society stakeholders refused to sign on to the final communiqué largely in objection to this component. The OECD communiqué is but a reflection of a larger trend. In the United States (US), several ISPs and carriers have already taken on this responsibility as a voluntary arrangement. Across the industrialised world, it is considered standard practice for large carriers to “clean their pipes” of malicious networks and traffic that is associated with file sharing or similar “undesirable” activities. The bottom line of business now demands it.

Of course what is considered “intermediary liability” or a market imperative in Canada and the US differs quite fundamentally from Belarus, Iran, Viet Nam or China. In non-democratic countries, ISPs, telecom carriers and mobile operators are being asked to police political content, track dissidents, identify protesters, send threatening messages over their networks, and disable certain protocols used by adversaries – all as part of what my colleague Rafal Rohozinski⁶ and I have dubbed “next-generation controls”⁷ that we see emerging throughout the developing world. During the Arab Spring, for example, the Egyptian government took the drastic step of forcing ISPs to shutter the internet, and required the country’s main mobile phone operator, Vodafone, to send mass text messages encouraging pro-regime sympathisers to take to the streets to counter the protesters.

This shift towards intermediary liability is perhaps one of the greatest practical changes around internet governance in the last decade, particularly when considered in the context of growing cyberspace securitisation, of which it is a part.

The *securitisation* of cyberspace – a transformation of the domain into a matter of national security – is perhaps the most important factor shaping the global communications ecosystem today. Faced with the combined pressures above, and seemingly incessant and embarrassing large-scale data breaches, policy makers around the world are racing to develop cyber security strategies. Some are following the lead of the US, standing up within their armed forces dedicated cyber commands and laying out formal doctrines for cyberspace. Others are adopting less conventional means, including providing tacit support for pro-patriotic groups to engage in offensive cyber attacks in defence of their country, as seems to be the case in Iran, Syria, Russia, Burma and China.

Cyberspace securitisation includes a political economy dimension: there is a growing cyber industrial complex⁸ around security products and services that both responds to, but also shapes the policy marketplace. Corporate giants of the Cold War, like Northrup Grumman, Boeing and General Dynamics, are repositioning themselves for lucrative defence contracts, alongside an array of subterranean niche companies that offer computer network exploitation products and services. The global cyber arms trade⁹ now includes malicious viruses, zero-day exploits and massive botnets. An arms race in cyberspace has been unleashed, with international implications. For every US Cyber Command, there is now a Syrian or Iranian cyber army equivalent. For every “Internet Freedom in a Suitcase”,¹⁰ there is justification for greater territorialisation of cyberspace controls.

Cyberspace securitisation has also effectively *normalised* internet censorship. What was once the province of pariah states, like China and Saudi Arabia, is now quickly becoming the norm among liberal democracies and authoritarian regimes alike. Our OpenNet Initiative¹¹ project tracks internet filtering and information controls in more than 40 countries worldwide. But perhaps the best insight on the normalisation of internet restrictions comes from data provided by Google. As part of its Transparency Report,¹² Google now discloses requests from governments for user data or the removal of information on its websites and services, like YouTube. The data it released for the July–December 2010 period was perhaps most remarkable not so much for confirming the usual suspects, but rather for the way it revealed that censorship is now normal among democratic countries.

3 www.michaelgeist.ca/content/view/5808/135

4 www.dubfire.net/#pubs

5 www.oecd.org/document/59/0,3746,en_21571361_44315115_48173819_1_1_1_1_00.html

6 Rafal Rohozinski is a Senior Scholar at the Canada Centre for Global Security Studies at the Munk School of Global Affairs, University of Toronto. He is a co-principal investigator of the OpenNet Initiative and Information Warfare Monitor projects.

7 www.access-controlled.net/wp-content/PDFs/chapter-1.pdf

8 www.theglobeandmail.com/news/opinions/opinion/the-new-cyber-military-industrial-complex/article1957159

9 www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html

10 www.nytimes.com/2011/06/12/world/12internet.html?_r=1&pagewanted=all

11 map.opennet.net

12 www.google.com/transparencyreport

The governments of Germany, the United Kingdom, Brazil, Italy and others make thousands of take-down requests every year.¹³ Here too, as a complement to these new developments, internet censorship services – produced primarily in the West¹⁴ – have become a major commercial sector. When Canadian filtering software companies who provide services and products to Yemen, Kuwait and the United Arab Emirates are actually applauded¹⁵ for their efforts by the Canadian government, we can safely say that internet censorship has become a global norm.

Rohozinski and I have summed up these cumulative forces as the coming “perfect storm” in cyberspace. With threats seemingly multiplying, and mutually reinforcing tendencies like those above growing, the prospects of extreme solutions finding widespread acceptance are high. Whether it is a proposal for an entirely new internet (as former CIA director Michael Hayden recently argued)¹⁶ or the gradual metamorphosis of the existing open communications space into sovereign-controlled national internets, the securitisation wave is going to have major and potentially damaging consequences for civic networks. What is to be done?

First, as argued, there is an urgent need for the articulation of a cyber security strategy for civic networks. For many who would characterise themselves as part of global civil society, “security” is seen as anathema. In today’s world of exaggerated threats and self-serving hyperbole from the computer security industry, it is easy to dismiss security as a myth to be demolished, rather than engaged. Securitisation is associated with the defence industry, Pentagon strategists, and the cyber security military industrial complex. Many might question whether employing the language of security only plays into this complex and the growing might of cyberspace controls.

But the vulnerabilities of cyberspace are very real, the underbelly of cyber crime is undeniably huge and growing, an arms race in cyberspace is escalating, and major governments are poised to set the rules of the road¹⁷ that may impose top-down solutions that subvert the domain as we know it. Dismissing these as manufactured myths propagated by the power elite will only marginalise civic networks from the conversations where policies are being forged.

Civic networks need to be at the forefront of security solutions that preserve cyberspace as an open commons of information, protect privacy by design, and shore up access to information and freedom of speech, while at the same time address the growing vulnerabilities that have produced a massive explosion in cyber crime and security breaches.

How can security and openness be reconciled? Aren’t the two contradictory? Not at all. The answer lies in the internet itself. As my colleague Jonathan Zittrain has forcefully argued, there are open and generative self-healing and protective mechanisms that are a part of the everyday functioning of the internet itself. Zittrain’s views are backed up by a recent European security study which explained how the open and decentralised organisation that is the very essence of the ecosystem is essential to the success and resilience of the internet.¹⁸ What is remarkable, in other words, is that the internet functions precisely in the *absence* of centralised control and *because* of the thousands of distributed, loosely coordinated monitoring mechanisms. While these decentralised mechanisms are not perfect and can occasionally fail, they should be bolstered and enhanced as part of a coherent distributed security strategy. Bottom-up, “grassroots” solutions to the internet’s security problems are consistent with principles of openness, avoid heavy-handed centralised controls, and provide checks and balances against the concentration of power in cyberspace. Part of a civil society security strategy should be to find ways to facilitate cooperation among the existing, largely scattered security networks while simultaneously making their actions more transparent and accountable.

Part of the civic strategy must also include a serious engagement with law enforcement – another traditional anathema for civil society. Law enforcement agencies are often stigmatised as the Orwellian bogeymen of internet freedom (and in places like Belarus, Uzbekistan and Burma, they are), but the reality in the liberal democratic world is more complex. Many law enforcement agencies are overwhelmed with cyber crime, are understaffed, lack proper equipment and training, and have no incentives or structures to cooperate across borders. Instead of dealing with these shortcomings head on, politicians are opting for new “Patriot Act” powers that dilute civil liberties, place burdens on the private sector, and conjure up fears of a surveillance society. What law enforcement needs is not new powers, it needs new resources, capabilities, proper training and equipment. But alongside those new resources should be the highest standards of judicial oversight and public accountability. Civic networks can articulate the differences between powers and resources, and highlight the importance of public accountability to liberal democracy as an example to the rest of the world without alienating what could be an important natural ally.

The same basic premise of oversight and accountability must extend to the private sector as well. Civic networks are inherently transnational and are because of this best equipped to monitor globe-spanning corporations who own and operate cyberspace. Persistent public pressure, backed up by credible evidence-based research and campaigns – like the Electronic Frontier Foundation’s (EFF) privacy

13 www.washingtonpost.com/blogs/blogpost/post/web-censorship-moves-to-democracies-the-west/2011/06/27/AGPi4xnH_blog.html

14 opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

15 opennet.net/blog/2011/07/canadian-government-lauds-uae-internet-service-provider-pervasively-censors-political-r

16 www.nextgov.com/nextgov/ng_20110706_1137.php

17 arstechnica.com/tech-policy/news/2011/05/france-attempts-to-civilize-the-internet-internet-fights-back.ars

18 www.lightbluetouchpaper.org/2011/04/12/resilience-of-the-internet-interconnection-ecosystem

scorecard¹⁹ – are the best means to ensure the private sector complies with human rights standards worldwide. Going further, however, civic networks should make the case that government pressures to police the internet impose costly burdens on businesses that should be conceded only with the greatest reservations and proper oversight. Such self-interest-based arguments will have much greater traction with the private sector than either pleas for magnanimity or pressures of naming and shaming ever will.

Lastly, civic networks need to be players in the rule-making forums where cyberspace rules of the road are implemented. This is not an easy task. There is no one single forum of cyberspace governance; instead, governance is diffuse and distributed across multiple forums, meetings and standard-setting bodies at local, national, regional and global levels. The idea of civil society participation in these centres of cyberspace governance varies widely, and is alien to some. Civic networks will need to monitor all of these centres of governance, open the doors to participation in those venues that are now closed shops, and make sure that “multi-stakeholder participation” is not just something paid lip service to by politicians, but something meaningfully

exercised by networks of citizens. The civil society rejection of the OECD final communiqué is a model in this regard.

The idea of *security* is most closely associated with the tradition of *realpolitik*, and the denizens of the national security apparatus. Global civil society, on the other hand, is most often associated with respect for rights, democracy, diversity and openness. As the securitisation of cyberspace builds momentum, it may be tempting for civic networks to either concede the terms of the security debate to the national security community, or resist it altogether. That would be a mistake. There is a long-standing and very powerful tradition of *liberal security*, associated with distributed checks and balances, respect for individual rights, and decentralisation. What is urgently required now is the translation of that tradition to the domain of cyberspace, and the practical application of its principles by citizens worldwide. Otherwise, the great gains in networking that have produced an explosion in global civil society over the last decades could gradually evaporate. ■

19 www.eff.org/pages/when-government-comes-knocking-who-has-your-back

Internet intermediaries

Joe McNamee

European Digital Rights (EDRI)

www.edri.org

Introduction

The purpose of this report is to look at the increasing trend for internet intermediaries to be used to police and enforce the law on the internet and even to mete out punishments. As well as undermining the fundamental rights of freedom of communication, privacy and right to a fair trial, this approach is serving to create borders in the online world, undermining the very openness that gives the internet its value for democracy and, indeed, for the economy.

This issue is becoming increasingly important due to four different trends, which are developing simultaneously and synergetically. These are:

- The increased technical possibilities for online surveillance by internet access providers. The use of some of these possibilities is required by legal obligations such as the 2004 Communications and Law Enforcement Act (CALEA)¹ in the United States (US) and the European Union's (EU) Data Retention Directive.²
- The increased business interest that larger access providers see in blocking or limiting access to certain online content, as illustrated by recent discussions in both the US and Europe on "net neutrality".
- A concerted push at an intergovernmental level to legitimise and spread privatised enforcement measures.³
- Mergers of access providers and media companies, and distribution agreements between content providers and intermediaries where the contract includes obligations for the intermediary to undertake policing/punishment measures.⁴

Limitations of intermediary liability

The need for an open internet was recognised by both the US and the EU at the end of the 1990s. The US adopted the Digital Millennium Copyright Act (DMCA) in 1998, offering significant "safe harbours" to internet intermediaries for unauthorised content on their networks, while the EU adopted the E-Commerce Directive in 2000, which took a horizontal

approach to safe harbours for all forms of illegal and unauthorised content. The public policy objectives on both sides of the Atlantic were clear, namely to maintain an open internet. This was seen as necessary to allow the economy to take full advantage of the internet and, as a collateral benefit, freedom of expression and almost unrestricted access to information. The benefits of such an approach can be seen in the economy⁵ and in the effect of the internet in opening closed societies right around the world.

Nonetheless, despite this comparatively robust legal framework, weaknesses appeared almost from the start. This particularly in Europe, where the wording of the E-Commerce Directive is too vague (due to the political compromises that were made during the adoption process) to allow intermediaries to feel completely secure, resulting in significant infringements on the right to communication. In 2004, a study by the Dutch NGO Bits of Freedom tested twelve hosting providers, nine of which deleted innocent material as a result of an obviously bogus "notice" sent from a Hotmail account set up solely for that purpose. This experience was duplicated by a team of United Kingdom (UK) academics,⁶ also in 2004 (although it should be pointed out that this project did find the DMCA's process comparatively robust), and Dutch firm ICTRecht in 2009. Unilateral actions by internet providers have now effectively shifted their core activities from hosting providers to internet access providers, who have started "blocking" content, very often outside the rule of law. This started in the UK in 2004, supported by the Internet Watch Foundation, and spread to Denmark, Sweden and Finland in the ensuing years, as well as into the mobile environment, thanks to an agreement brokered by the European Commission.⁷ It is worth noting the heavy overlap between parts of the internet access market most opposed to net neutrality and the parts most favourable to voluntary internet blocking.

Operators that have been at the forefront of "voluntary" internet blocking – such as British Telecom, Telenor, Virgin and the mobile industry in general – have also been the loudest voices opposed to net neutrality. In January 2011, British Telecom announced plans to charge certain online video providers more for prioritised traffic,⁸ as did Telenor,⁹ while Virgin Media announced plans to launch a deep packet

1 en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act

2 eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

3 See, for example, article 5.3 of the Anti-Counterfeiting Trade Agreement at www.ustr.gov/webfm_send/2379

4 www.bof.nl/2011/01/04/vrijie-internettoegang-ook-in-nederland-onder-vuur

5 eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

6 pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf

7 ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3153

8 www.wired.com/epicenter/2011/01/bt-rejects-accusations-of-net-neutrality-breach-sort-of

9 www.dn.no/forsiden/etterBors/article2067200.eco

inspection of the traffic of 40% of its customers in 2010.¹⁰ Similarly, there have been multiple examples of mobile industry efforts seeking to exploit and reinforce their control over access to their clients, such as the blocking of voice over internet protocol (VoIP) applications.¹¹ This creates a situation where these providers are eager to accept demands from regulators for so-called “self-regulatory” blocking measures as, in the long term, it will be difficult for regulators to sustainably argue that access providers should be voluntarily interfering in traffic for public policy reasons but not for business reasons.

The beginning of large-scale privatised enforcement

At the moment there appears to be a “tipping point”, with governments apparently feeling that the openness that gives the internet its economic value is now so unbreakable that unfettered meddling by intermediaries for the protection of (mainly) intellectual property can be actively promoted.¹² They are not only promoting this approach internally, and not only in countries with strong democratic traditions, but across the globe, potentially blocking off markets and legitimising privatised surveillance and control on communication in totalitarian and highly controlled regimes. As a result, there has been a veritable rash of international-level measures which seek to encourage or coerce intermediaries – many with their own long-term vested interests in this – to filter, block and punish alleged online infringements.

In November 2010, the negotiating parties published the final text of the Anti-Counterfeiting Trade Agreement (ACTA). Although significantly improved from earlier versions, the section of the agreement on intellectual property enforcement circuitously talks about maintaining an internet service provider (ISP) liability regime which preserves “the legitimate interests of rights holders” and obliges parties to “endeavor to promote cooperative efforts within the business community to effectively address trademark and copyright or related rights infringement”¹³ – a footnote in a leaked draft explaining that “an example of such a policy is providing for the termination in appropriate circumstances of subscriptions and accounts in the service provider’s system or network of repeat [alleged, presumably] infringers.”

In February 2011, the World Intellectual Property Organization (WIPO) tried and failed¹⁴ to launch a discussion¹⁵ on internet intermediary liability for trademark infringements.

This was followed in June 2011 by a side-event at a WIPO event in Geneva on the “role and responsibility of internet intermediaries in the field of copyright” which, interestingly, included no internet intermediaries at all! WIPO has also recently commissioned and published two independent studies on intermediary liability.¹⁶ It has successfully tabled a workshop proposal for the Internet Governance Forum in Nairobi in September 2011 to discuss “thought-provoking ideas” such as in ACTA, the US Combating Online Infringements and Counterfeits Act (COICA) (which requires “blocking” by internet intermediaries) and the EU Intellectual Property Rights Enforcement Directive (whose use for mandatory internet blocking and surveillance is currently being assessed by the European Court of Justice).¹⁷

In June 2011, the Organisation for Economic Co-operation and Development (OECD) adopted its Communiqué on Principles for Internet Policy Making.¹⁸ Under the heading “limit internet intermediary liability” it calls for states to undertake multi-stakeholder processes to “identify the appropriate circumstances under which internet intermediaries could take steps to educate users, assist rights holders in enforcing their rights or reduce illegal content” (this communiqué itself was the subject of a multi-stakeholder process that civil society rejected).¹⁹ The text avoids supporting network neutrality and instead meaninglessly refers to maintaining “appropriate” quality. It also pointedly avoids even a single reference to “due process”, opting for the less restrictive and legally meaningless “fair process” instead.

Privatised policing in practice

So what does all of this mean on a practical level? As this approach is generally outside the rule of law, implementations tend to be very ad hoc. Across Europe, internet hosting providers and social networks delete material which they fear could result in them being liable, based on random criteria. As seen in the 2004 Bits of Freedom study, the same content will be deleted or left online depending on the unpredictable internal practices of the companies in question. Dutch social networking site Hyves will automatically delete anything if users with ten different IP addresses click the “report material” button. Remarkably, the European Commission has actively encouraged hosting providers to change their terms of service to give them an unfettered ability to delete anything they want.²⁰ Similarly, internet providers who started “blocking” websites accused of containing child abuse material are now being asked and sometimes required to introduce blocking measures for other content.

10 technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6989510_ece

11 www.ft.com/cms/s/0/1ce4e1c8-1fd7-11de-a1df-00144feabdc0.html#axz1STK17d9n

12 The draft PROTECT IP Act in the US was accused of allowing “the government to break the Internet addressing system” and “breaking the Internet infrastructure” by a group of 108 professors in a recent public letter on this proposed legislation. blogs.law.stanford.edu/newsteed/files/2011/07/PROTECT-IP-letter-final.pdf

13 www.ustr.gov/webfm_send/2379

14 www.cciinet.org/index.asp%3Fsid=5%26artid=213%26evflg=False

15 www.wipo.int/edocs/mdocs/sct/en/sct_25/sct_25_3.pdf

16 www.wipo.int/copyright/en/internet_intermediaries/index.html

17 European Court of Justice Case C70/10

18 www.oecd.org/dataoecd/40/21/48289796.pdf

19 www.edri.org/files/CSISAC_Press_Release%20_0628011_FINAL.pdf

20 www.edri.org/edriagram/number8.15/edri-euroispa-notice-takedown-comission

In Ireland, the former monopoly internet provider Eircom has agreed to become judge, jury and executioner on accusations of illegal downloading – cutting off consumers repeatedly accused of infringements²¹ and blocking websites²² accused by music industry interests of facilitating infringements. The Spanish “Sinde” law offers an interesting mix of rule of law and extra-judicial coercion. Under that approach, the plaintiff requests extra-judicial action from the internet provider first and, afterwards, if the internet provider wants to incur the expense of pursuing a court case, a judicial procedure is foreseen. In the US, the large ISPs that have been lobbying hard for the right to throttle bandwidth for their own commercial benefit have kindly offered to throttle bandwidth to users who have been repeatedly accused of copyright violations.

In addition to their business interest in this anti-net neutrality approach, the changing nature of the business (demonstrated *inter alia* by Comcast’s purchase of NBC and Verizon’s recent move to movie distribution)²³ creates new incentives for this approach. Smaller access providers will be increasingly “squeezed” – they are obliged to incur the cost of implementing technologies to be able to interfere with internet traffic in the absence of the economies of scale that would permit this to be done in a cost-effective way, or in a way which could be used for non-net neutral purposes.

In addition to the threats to citizens’ ability to access the internet at all, to access an open and neutral internet, and to access material “voluntarily” or accidentally blocked by their ISP, there are also increasing efforts to use the structure of the internet itself as a law enforcement tool. The EU and the US, for example, have an ongoing project to discuss the revocation of domain names (on which the US claims wide-ranging jurisdiction)²⁴ and IP addresses²⁵ (the regional registry for Europe, the Middle East and parts of central Asia is located in the Netherlands). While the US approach is partly based on law, with COICA and the PROTECT IP (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property) Act²⁶ planned to regulate the blocking and revocation of domain names, a non-legislative approach is also followed in some circumstances, such as regarding unlicensed online pharmacies. In the EU, blocking is regulated by law in some countries (France and Italy, for example), without law in others (the UK and Sweden) and with and without law in others, depending on the subject (such as in Denmark and, possibly in the future, the UK). Revocation of domain names, on the other hand, is generally without a legal framework.²⁷

Conclusion

The promotion of a closed internet regulated outside the rule of law undermines efforts of Western governments to support the democratising potential of the internet in closed and totalitarian regimes. The imposition of unreasonable jurisdiction claims over parts or all of the IP address allocation and domain name systems creates dangers for the integrity of the global internet. The outsourcing of policing of the internet and imposition of punishments by internet intermediaries contradicts basic democratic values and our democratic societies’ view of the rule of law. The outsourcing of these activities to large corporations who have a publicly stated vested interest in the development and imposition of a non-neutral internet creates an online environment which is diametrically opposed to the openness of the internet. This openness gives us the democratic – and the economic – value of the internet and is too important for governments to simply take for granted and to experiment with as if it were insignificant. Our social interaction is increasingly online and freedoms which were previously unquestioned are now increasingly at the whim of private companies: our freedom of expression, our freedom of assembly, our privacy and our right to due process and presumption of innocence.

Next steps

- Activists should demand that the spirit and the letter of constitutional²⁸ and human rights²⁹ be respected
- The dangers of pushing world regions or individual countries into developing “splinternets” to avoid EU/US jurisdiction should be recognised.
- Positive positions of international organisations should be publicised as much as possible.³⁰
- Positive political statements on the need to keep the internet open should be publicised and promoted.³¹
- The contradictions between calls for an open internet in certain countries and support for a privately regulated and closed internet domestically should be highlighted.
- More attention should be given to the economic damage of moving from an innovative, competitive and open internet to a closed non-neutral internet. ■

21 www.theregister.co.uk/2009/02/03/eircom_agrees_to_three_strikes_enforcement

22 www.theregister.co.uk/2009/02/23/rma_demands_irish_isps_block_access_to_piracy_sites

23 www.nytimes.com/2011/07/17/opinion/sunday/17sun3.html?partner=rssnyt&emc=rss

24 digitizor.com/2011/07/06/us-jurisdiction-com-net-websites

25 www.theregister.co.uk/2010/04/27/eu_cybercrime

26 en.wikipedia.org/wiki/Protect_IP_Act

27 www.theregister.co.uk/2011/05/18/nominet_wrestles_with_net_cop_role

28 Such as the US First Amendment.

29 Such as Articles 8 and 10 of the European Convention on Human Rights and Article 19 of the International Covenant on Civil and Political Rights.

30 www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

31 www.physorg.com/news/2011-02-clinton-renews-internet-access.html

E-revolutions and cyber crackdowns: User-generated content and social networking in protests in MENA and beyond

Alex Comminos

Justus Liebig University Giessen

www.comminos.org

Introduction

The recent protests and uprisings in Tunisia and Egypt have both been called “Twitter revolutions” and “Facebook revolutions” due to the widespread use of user-generated content (UGC) disseminated over social networks like Facebook and Twitter by protesters, activists and supporters of the protests, as well as by those following the events around the globe. This report investigates the usage and role of UGC and social networking websites in the recent protests and uprisings in the Middle East and North Africa (MENA), as well as other cases outside of the region.

In addition to being effective tools for communication and coordination by protesters, UGC and social networking have also been used by governments in response to these protests, often to crack down on protesters. Content and social networking platforms are areas of contestation between protesters and governments not necessarily balanced in favour of protesters.

UGC refers to internet content (text, images, videos and sound clips) that is created and uploaded to the internet by users, usually for no explicit financial gain, but rather for enjoyment or passion. UGC is created usually by amateurs, rather than professionals. It includes blogs, video clips, audio clips (podcasts), as well as comments on internet forums or “status updates” on social networks like Facebook or micro-blogging platforms like Twitter. In MENA, UGC created on mobile phones enabled protesters or witnesses to report on events live and to communicate with others and spread their message. Social networks like Facebook and the micro-blogging platform Twitter were used to disseminate this content.

Twitter and Facebook revolutions?

Can the uprisings in Egypt and Tunisia, as well as others in the MENA region, be called Twitter or Facebook revolutions? Was social networking unique to these protests? Has similar usage been seen before elsewhere? Was UGC, created on mobile phones and distributed over platforms like Facebook or Twitter, among the causes of these uprisings?

The usage of mobile phones, social networking websites and UGC in protests in MENA is not unprecedented. Twitter was used in protests in Moldova and Iran in 2009 and both cases were referred to by some as Twitter revo-

lutions.¹ The popular ousting of President Joseph Estrada in the Philippines in 2001 was referred to as an “SMS revolution” due to the use of text messages to mobilise protests. It was described as “arguably the world’s first ‘e-revolution’ – a change of government brought about by new forms of ICTs.”²

Many feel that the role of UGC and social networking should not be overstated,³ that these were not the cause of protests and uprisings in any MENA country. The causes involve a combination of decades of repression, political and economic marginalisation, the long-term structural decay of effectiveness and legitimacy in some state institutions, and soaring food prices, along with a desire by citizens for political representation and participation and the recognition of their human rights. On the ground, popular sentiments, grassroots organising and allegiance of the state security forces are important factors.

ICT access in MENA

Calling the uprisings in Tunisia and Egypt Twitter or Facebook revolutions overlooks information and communications technology (ICT) access in these countries. In 2009 in Tunisia and Egypt there were only 34.1 and 24.3 internet users per 100 inhabitants respectively. In Egypt only 7% of inhabitants are Facebook users, while 16% are Facebook users in Tunisia. From the ICT access and usage figures listed in Table 1, there is little correlation between ICTs and the level of unrest.

Throughout MENA social networking users generally comprise a minority of the population. Claims that UGC speaks for the demonstrators must be taken critically. The usage of the internet in developing countries is often disproportionately urban. Media attention is generally drawn to urban protests, for example, Cairo, Alexandria, Tunis, Tripoli and Benghazi. Use of UGC and social media also often reflects income and literacy biases.

- 1 The term was applied by Evgeny Morozov to the Moldovan protests in 2009. See Morozov, E. (2009) Moldova’s Twitter Revolution, *Net Effect*, 7 April. neteffect.foreignpolicy.com/posts/2009/04/07/moldovas_twitter_revolution; see also his other posts, More analysis of Twitter’s role in Moldova, *Net Effect*, 7 April. neteffect.foreignpolicy.com/posts/2009/04/07/more_analysis_of_twitter_role_in_moldova and Moldova’s Twitter revolution is NOT a myth, *Net Effect*, 10 April. neteffect.foreignpolicy.com/posts/2009/04/10/moldovas_twitter_revolution_is_not_a_myth Morozov has since criticised the Western media’s haste to apply the term to Iran and protests and uprisings in MENA, as well as admitting that he might have hastily applied the term to Moldova. He writes about it in his 2011 book, *The Net Delusion: The Dark Side of Internet Freedom*, Public Affairs, New York.
- 2 Cout, J. (2001) *People Power II in the Philippines: The First E-Revolution?*, Overseas Development Institute. www.odi.org.uk/resources/details.asp?id=3147&title=people-power-ii-philippines-first-e-revolution
- 3 The debate between techno-sceptics and techno-idealists with regards to the role of ICTs in Tunisia and Egypt is well outlined in Vargas, J. A. (2011) Egypt, the Age of Disruption and the “Me” in Media, *The Huffington Post*, 7 February. www.huffingtonpost.com/jose-antonio-vargas/egypt-age-of-disruption-me-in-media_b_819481.html; see also Kravets, D. (2011) What’s fueling Mideast protests? It’s more than Twitter, *Wired Magazine*, 28 January. www.wired.co.uk/news/archive/2011-01/28/middle-east-protests-twitter.

TABLE 1. ICT access in MENA

Country	Mobile cellular subscriptions per 100 inhabitants	Fixed internet subscriptions per 100 inhabitants	Estimated internet users per 100 inhabitants	Fixed broadband subscriptions per 100 inhabitants	Facebook users	Facebook users per 100 inhabitants
Algeria	93.8	...	13.5	2.3	1,138,240	3.00
Azerbaijan	87.8	5.9	27.4	1.1	184,660	2.00
Bahrain	177.1	10.0	53.0	9.6	232,960	29.00
Egypt	66.7	2.8	24.3	1.3	5,651,080	7.00
Iran	70.8	...	11.1	0.5	no data	no data*
Iraq	64.1	...	1.1	0.1	254,840	less than 1
Israel	125.8	...	63.1	25.8	308,760	40.00
Jordan	95.2	3.9	26.0	3.2	954,580	15.00
Kuwait	129.9	...	36.9	1.5	525,000	17.00
Lebanon	56.6	...	23.7	5.3	969,240	23.00
Libya	148.5	12.0	5.5	1.0	191,120	3.00
Mali	34.2	0.2	1.9	0.0	44,360	less than 1
Mauritania	66.3	...	2.3	0.3	33,700	1.00
Morocco	79.1	1.5	41.3	1.5	2,158,680	7.00
Oman	139.5	2.8	51.5	1.4	156,200	5.00
Palestine	28.6	...	32.2	5.0	no data	no data
Qatar	175.4	10.4	40.0	10.4	405,100	24.00
Saudi Arabia	174.4	7.3	38.0	5.2	2,489,320	9.00
Sudan	36.3	0.4	no data	no data*
Syria	45.6	3.6	20.4	0.2	no data	no data*
Tunisia	95.4	4.0	34.1	3.6	1,708,700	16.00
UAE	232.1	30.5	75.0	15.0	1,689,300	36.00
Yemen	35.3	1.9	10.0	0.2	107,520	less than 1

* Denotes lack of data due to the US comprehensive economic embargo on Iran, Sudan and Syria. There is no official Facebook data for these countries due to the trade embargo – technically they are not supposed to be offered Facebook, which is a US product.

Sources: International Telecommunication Union 2009 (www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx) and Social Map (geographics.cz/socialMap, Statistics are from May 2011)

Nonetheless, many protesters used UGC to express popular demands. Linkages were demonstrated between the mobilisation of demonstrators by social media as well as off-line (on-the-ground) mobilisation.⁴

UGC and social networking in MENA

The terms “Twitter revolution” or “Facebook revolution” may not be accurate. The assertions that “the revolution will be tweeted” and “the revolution will be streamed” have more credence in the cases of Egypt, Tunisia, Syria, Bahrain and Libya. Many used mobile phones to organise demonstrations and to spread their messages. UGC and social networking platforms play an important role in protests and political transitions, but not necessarily a decisive one.

Before investigating the usage of UGC, the context of its use in MENA will be examined by looking at internet freedom in the region.

Internet freedom in MENA

In November 2005, Reporters Without Borders (RSF) listed fifteen “enemies of the internet”, four of which were in

MENA: Libya, Saudi Arabia, Syria and Tunisia. In 2010, RSF listed twelve enemies of the internet, including Saudi Arabia, Egypt, Syria and Tunisia. In March 2011, only Saudi Arabia and Syria were “enemies of the internet”, although Bahrain, Belarus, Egypt, Libya, Tunisia and the United Arab Emirates (UAE) were listed as “under surveillance”. Saudi Arabia, Syria and Egypt had netizens in prison.⁵

Internet filtering is common in MENA. The OpenNet Initiative reports that Bahrain, UAE, Qatar, Oman, Saudi Arabia, Kuwait, Yemen, Sudan and Tunisia used Western technologies to block internet content, “such as websites that provide sceptical views of Islam, secular and atheist discourse, sex, GLBT [gay, lesbian, bisexual and transgender content], dating services, and proxy and anonymity tools.”⁶

5 Reporters Without Borders (2005) The 15 enemies of the Internet and other countries to watch, *Reporters without Borders*, 17 November. en.rsf.org/the-15-enemies-of-the-internet-and-17-11-2005,15613.html; Reporters without Borders (2010) Web 2.0 vs Control 2.0, *Reporters Without Borders*, 12 March. en.rsf.org/IMG/pdf/Internet_enemies.pdf; Reporters Without Borders (2011) *Internet Enemies*, Reporters without Borders. march12.rsf.org/i/Internet_Enemies.pdf

6 Noman, H. and York, J. C. (2011) *West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011*, OpenNet Initiative. opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

4 Meier, P. (2011) Civil Resistance Tactics Used in Egypt’s Revolution #Jan25, *iRevolution*, 27 February. irevolution.net/2011/02/27/tactics-egypt-revolution-jan25

According to a 2007 study of Arab media, “the impact of censorship across the region is mixed.” Despite persistent censorship, “governments have not been able to silence dissent on the internet.”⁷

The use of UGC and social networking in protest in MENA

Mohammed Bouazizi was a poverty-stricken Tunisian vegetable trader from the small town of Sidi Bouzid who had been repeatedly harassed by the police, who often asked him for bribes and confiscated his wares. In the last encounter they beat him. After being denied an appointment with a local government official to discuss this harassment, he doused himself with fuel and set himself alight in a public square. He died in hospital weeks later.

News of Bouazizi inspired protests in Sidi Bouzid, elsewhere in Tunisia, and throughout MENA. Initially television and print media were slow to pick up on the story. Often state media in MENA avoided reporting on it. Some internet content (like YouTube) was blocked at the time by the Tunisian internet filter. Facebook, which was not blocked at the time, became an important platform for spreading news of Bouazizi and the Sidi Bouzid revolt. Twitter was also instrumental in covering the protests.

Around the globe, many used Twitter and Facebook as a first port of call for information about Tunisia. UGC about events in Tunisia served to inspire people throughout the region. Egyptian activist Gigi Ibrahim, upon witnessing the downfall of Tunisian President Zine al-Abidine Ben Ali, tweeted: “The Tunisian revolution is being twitterised...history is being written by the people #sidiBouzid #Tunisia.”⁸

In Egypt, Facebook and Twitter were used to announce and publicise the planned protests on 25 January 2011. Facebook groups such as We are all Khaled Said⁹ and the 6th of April Youth Movement¹⁰ called for demonstrations. The plans and message of the protest were also disseminated through conventional means like word of mouth, photocopies and emailing of a PDF file explaining the plans for the protests.¹¹

Facebook was used to announce protests in other countries in the MENA region. Many protests in 2011 were supported by Facebook pages, events and groups. UGC

communicated the messages of protesters nationally, regionally and globally, and provided live coverage, news and opinions. On Twitter, protests (both online and offline) had their own Twitter hash tags. The Twitter hash tags #SidiBouzid, #Jan25, #Jan30, #Feb14, #Feb17 #Mar11/#ksa/#tal3mrak,¹² #Yemen/#Yamen, #Kuwait, and #Syria were used for protest in Tunisia, Egypt, Sudan, Bahrain, Libya, Saudi Arabia, Yemen, Kuwait and Syria respectively.

UGC acted as a conduit for news around unfolding events not covered by or outside the reach of the conventional media. Micro-blogging and picture and video sharing over mobile phones became avenues to disseminate and consume news about protests. The nexus of UGC and mobile phones is an important tool for protesters to inform the world of their demands, the events surrounding the actual protests, and the nature of police, military and civilian responses. UGC often offers views and perspectives that state-run and conventional media do not offer, as well as images that other media cannot record. In Syria, where access by international journalists has been almost completely restricted, mobile phone videos have become one of the few ways to report on protests.

State responses to UGC and social networking

Many have commented on the power of social media in the hands of protesters and activists. What of state responses to UGC and social networking during the protests? How have UGC and social networking websites been used by incumbent regimes in response to protests?

Goliath and the mouse? Twitter revolutions and cyber crackdowns

An online campaign by the International Society for Human Rights (ISHR) depicts challenged incumbent leaders gripped by fear of the revolutionary potential of ICTs. The presidents of Iran, Zimbabwe, Venezuela and Cuba, Colonel Muammar Gaddafi of Libya and North Korea's Kim Jong-il, are portrayed cowering in near paralytic fear of a computer mouse, jumping on furniture and hanging from chandeliers and curtains in an attempt to flee.¹³ The real balance of power in the electronic terrain, however, is not necessarily in favour of the mouse. The campaign could have been balanced with other images: boots crushing mice, keyboards and mobile phones after being identified as threats for spreading content. Or perhaps the regime's technicians unplugging the mice, terminating lines of communication.

UGC and the infrastructures through which it flows are areas of contestation between protesters and pro-incumbent

7 Hofheinz, A. (2007) Arab Internet Use: Popular Trends and Public Impact, in Sklar, N. (ed) *Arab Media and Political Renewal: Community, Legitimacy and Public Life*, IB Tauris, New York, p. 60.

8 Gigi Ibrahim (@Gsquare86) 17:28:11 Jan 14 2011 twitter.com/gsquare86. Tweet curated in Nunns, A. and Idle, N. (2011) *Tweets from Tahrir*, OR Books, New York.

9 See Anonymous, “We are all Khaled Saeed”, www.facebook.com/ElShaheed as well as “We are all Khaled Said: Working against torture and inhuman treatment of Egyptians in their own country. Standing up against corruption in Egypt”, www.elshaheed.co.uk. The pages were created in response to the murder of Khaled Said. Said was beaten to death by police after being caught in an internet café attempting to upload footage of Egyptian police selling drugs.

10 See “6th of April Youth Movement - ليريد ا 6 بابيش طرح”, www.facebook.com/shabab6april

11 See a copy in English and Arabic in Madrigal, A. (2011) Egyptian Activists' Action Plan: Translated, *The Atlantic*, 27 January. theatlantic.com/international/archive/2011/01/egyptian-activists-action-plan-translated/70388. Interestingly, the document stated not to use Twitter, Facebook or other websites for dissemination as “[t]hey are all monitored by the Ministry of the Interior.”

12 Tal3mrak means literally “May god prolong your life” and is used to address the wealthy and powerful respectfully in the Gulf region. It is also used sarcastically to make fun of rich and powerful figures and has been used to make fun of the king of Saudi Arabia around the Arab world. See Shibab-Eldin, A. (2011) #Tal3mrak: A Hashtag Challenges Saudi Arabian King, *The Huffington Post*, 31 August. www.huffingtonpost.com/ahmed-shihabeldin/tal3mrak-a-hashtag-challe_b_941231.html

13 The campaign cannot be found anymore on the ISHR website (www.ishr.org), but it can be found in many other places online, for example at Duncan (no surname given) (2010) ISHR Scared Dictators and The Mouse, *The Inspiration Room*, 24 September. theinspirationroom.com/daily/2010/ishr-scared-dictators-and-the-mouse

groups, not necessarily balanced in favour of those creating content for protest.

Some governments used internet filters to block content during the protests. In Tunisia, Egypt, Libya, Syria and allegedly Gaza there were state crackdowns on UGC and the internet in general through internet blackouts and slowdowns.¹⁴

The Mubarak regime virtually shut down all Egyptian access to the internet from midnight 27/28 April until 2 February 10:30 GMT.¹⁵ In Libya, the internet was blocked to most Libyans from the beginnings of the protests in areas under Gaddafi control.¹⁶ Hours after the internet had gone back up, Egyptian security forces arrested, detained and harassed bloggers and Facebook and Twitter users who had shared content or publicised and attended events.

In Tunisia, the Ben Ali regime stole usernames and passwords for Facebook, Twitter and online email accounts by injecting Java scripts into the content of these pages before they were sent to end-users.

Twitter and Facebook have been used by security and intelligence agencies to identify and locate activists and protesters. In North Sudan, where Facebook groups announced protests against the regime, the government actively monitored social networking websites. When protests did happen, many potential demonstrators found police waiting for them and were arrested.¹⁷

In Azerbaijan, influenced by events in Egypt, a number of Facebook pages and groups called for protests in early 2011. An opposition activist was arrested and charged with possession of narcotics. Many believe he was detained for comments he made on Facebook calling for Egypt-style protests.¹⁸ Amnesty International called the charges a “pretext to punish Jabbar Savalan for his political activism and to discourage other youth activists from exercising the right to freedom of expression.”¹⁹

Crackdowns on internet communications during protests were not only witnessed in MENA in 2011, but also in the United States (US) and United Kingdom (UK). In response to protests in the UK, the government has asked for cooperation from Research in Motion (RIM) – the creators of the Blackberry smartphone – to provide it with encryption

keys in order to be able to eavesdrop on the Blackberry Messenger service (BBM). The UK government has summoned Twitter, Facebook and RIM to a meeting discussing ways to restrict the use of social media during civil unrest.²⁰ The San Francisco Bay Area Rapid Transit (BART) authority (a state-owned transport corporation) shut down mobile phone access at subway stations as a response to planned protests against the killing of a homeless man by the BART Police.²¹

Problems presented by the use of UGC in struggles for democracy and human rights

Social media and surveillance

As WikiLeaks' Julian Assange recently noted, the internet is not only a force for openness and transparency, “it is also the greatest spying machine the world has ever seen.”²² Social networking platforms often link an online identity to a real name, home town, occupation, interests, pictures, and network of friends – providing many opportunities for surveillance.

Information on social networks may potentially be mined by third-party applications and advertisers. Facebook's API,²³ which is a language or set of commands for retrieving information from Facebook, is openly accessible by anyone turning their account into a developer account. The API makes it easy to obtain and analyse such information.²⁴

Mobile phones and geolocation

Facebook and Twitter, as well as mobile phone applications, offer geolocation functionality, which may add location to a user's content. The position of a mobile phone can be tracked by mobile operators, and potentially by governments or third parties. Under certain circumstances the use of the mobile internet can actually enhance the surveillance capabilities of repressive regimes.

Removal of UGC from social networks

Facebook policies can often result in the Facebook pages of political activists being shut down. The “We are all Khaled Said” Facebook page, which was used (among others) to call for protests on the 25 January revolution in Egypt, was actually opened in June 2010 but was quickly shut down by Facebook. This was because the user who opened the

14 Global Voices (2011) Syria: Reports of Internet Blackout, *Global Voices*, 3 June. globalvoicesonline.org/2011/06/03/syria-reports-of-internet-blackout-occupied-palestine (2011) Latest Updates on #Gaza | #GazaBlackOut”, *Occupied Palestine*, 10 August. occupiedpalestine.wordpress.com/2011/08/10/latest-update-on-gaza-gazablackout. The Gaza case may have been an accident, or an attempt to stop a planned terror attack, but it still may represent a crackdown on the internet during protests and unrest.

15 Internet access during the Egyptian revolution can be graphed on Google Transparency (transparency.google.com); see is.gd/VwQM29. The web was not entirely blocked: the ISP Nour, which ran the stock exchange, was functional. The web more correctly slowed to a microscopic trickle into Egypt.

16 See Google Transparency for Libya from mid-February on at is.gd/XKhhkC and is.gd/TWtIS

17 Meier, P. (2011) Civil Resistance: Early Lessons Learned from Sudan's #Jan30, *iRevolution*, 31 January. irevolution.net/2011/01/31/civil-resistance-sudans-jan30; Babington, D. (2011) Sudan's cyber-defenders take on Facebook protesters, *Reuters*, 30 March. reuters.com/article/2011/03/30/us-sudan-internet-feature-idUSTRE72T54W20110330.

18 Krikorian, O. (2011) Azerbaijan: Blowing Up in Their Facebook, *Global Voices Advocacy*, 10 March. advocacy.globalvoicesonline.org/2011/03/10/azerbaijan-blowing-up-in-their-facebook/.

19 Cited in *Ibid*.

20 Somaia, R. (2011) In Britain, a Meeting on Limiting Social Media, *The New York Times*, 25 August. www.nytimes.com/2011/08/26/world/europe/26social.html?_r=1&src=tp

21 For an overview of the operation in protest against BART see: The War and Peace Report (news show), 16 August 2011, *Democracy Now!* www.democracynow.org/2011/8/16/stream-and-vince-in-the-bay-disorderly-conduct-operation-bart-recap - Operation BART Recap (podcast), 17 August 2011, www.blogtalkradio.com/vinceinthebay/2011/08/17/disorderly-conduct-operation-bart-recap-1

22 The Hindu (2011) World's greatest spying machine, *The Hindu*, 6 April. www.thehindu.com/opinion/editorial/article1602746.ece.

23 API originally stood for Advanced Programming Interface, but is now more commonly known as Application Programming Interface. An API is “a particular set of rules and specifications that software programs can follow to communicate with each other. It serves as an interface between different software programs and facilitates their interaction, similar to the way the user interface facilitates interaction between humans and computers.” en.wikipedia.org/wiki/Application_programming_interface

24 Moderated, of course, by the user's privacy settings.

account – “El Shaheed” – was not using a real name. Facebook’s terms of service prohibit the use of fake names or monikers.

In the UK in April 2011 a group of students from University College London called UCL Occupation, protesting over fee increases and cuts to higher education funding, claimed that in twelve hours Facebook had deleted over 50 Facebook profiles of activists in the UK.²⁵

Guy Aitchison, a student at UCL and blogger for openDemocracy.net, said:

These groups are technically in violation of Facebook’s terms of agreement (...). But the timing – on the royal wedding and May Day weekend – is deeply suspicious. (...) [T]his purge of online organising groups could be linked to the wider crackdown on protest by authorities in Britain. Either way, it is a scandalous abuse of power by Facebook to arbitrarily destroy online communities built up over many months and years [which] provide a vital means for activist groups to communicate with their supporters.²⁶

Facebook officially responded to UCL Occupation with the following explanation and advice:

Facebook profiles are intended to represent individual people only. It is a violation of Facebook’s Statement of Rights and Responsibilities to use a profile to represent a brand, business, group, or organization. (...) If you would like to continue representing your organization on Facebook, we can convert your profile to a Page.²⁷

In Palestine a page calling for a “Third Palestinian Intifada” was shut down. It was seen by some as hate speech and reported to Facebook.²⁸ Many wondered why all other Arab countries were allowed to have pages dedicated to a “day of rage” against their governments, but one was not allowed for a protest against Israeli occupation.

These examples demonstrate that it is not users of the platforms, but the social networking or content platforms themselves, that have ultimate control of their content.

Reliability and veracity of UGC

UGC can be used for misinformation and propaganda. UGC presents problems with regards to the reliability and veracity of information. A famous example from MENA was that of the “lesbian Syrian blogger” who turned out to be a married

US man.²⁹ This ended up being counterproductive for the protest movement and fuelled rumours of foreign intervention in protests, propagated by the Syrian government. Social networks can be mechanisms for spreading rumour and falsehood. As there is usually no moderation of this content, it is the responsibility of the user to critically examine the veracity of UGC.

Sockpuppetry and astroturfing

“Sockpuppets” are an important problem in UGC. Wikipedia defines a sockpuppet as “an online identity used for purposes of deception within an online community” and, in earlier usage, “a false identity through which a member of an Internet community speaks with or about himself or herself, pretending to be a different person.”³⁰ “Astroturfing” is using sockpuppets on a larger and organised scale, designed to fake the appearance of grassroots or “netroots” movements (conventionally the word “astroturf” refers to synthetic grass). Astroturfing can disseminate views that appear to be legitimate and spontaneous, but are actually campaigns by political or commercial identities.³¹

Members of the hacktivist collective Anonymous claim to have discovered the existence of an advanced astroturfing software allegedly commissioned by the US Air Force.³² This software can create online identities with corresponding social networking profiles on multiple platforms, which can create content with identities that appear contingent to previous posts, as well as according to culture, age or gender. This software is also a surveillance platform, as “fake friends” on social networks to monitor unsuspecting users.³³ The possible existence of this software raises important concerns about the nexus of UGC and astroturfing.

Conclusion

UGC, social networks and mobile phones are not unequivocally tools for the benefit of protesters, but rather a part of a contested terrain used by both governments and protest movements in societal conflicts and transitions. Social networking sites like Facebook and Twitter could be used to spy on protesters, find out their real-life identities and make arrests and detentions.

These dilemmas will remain relevant in Egypt and Tunisia now that political transitions have started. Egypt and Tunisia both remain under military rule. Democracy and freedom to create and distribute content will not necessarily prevail. Neither will the role of UGC and social networking sites cease to be of relevance.

25 UCL Occupation (2011) Over 50 political accounts deleted in Facebook purge, *UCL Occupation*, 29 April. blog.ucloccupation.com/2011/04/29/over-50-political-accounts-deleted-in-facebook-purge

26 Aitchison, G. (2011) Political purge of UK Facebook underway, *OurKingdom*, 29 April. www.opendemocracy.net/ourkingdom/guy-aitchison/political-purge-of-uk-facebook-underway

27 UCL Occupation (2011) Facebook forced to respond to our campaign for restoration of accounts, *UCL Occupation*, 29 April. blog.ucloccupation.com/2011/04/29/facebook-forced-to-respond-to-our-campaign-for-restoration-of-accounts

28 Neroulis, N. (2011) Jews Pressure Facebook over Palestinian Intifada Page, *The Huffington Post*, 31 March. www.huffingtonpost.com/2011/03/30/jews-pressure-facebook-ov_n_842741.html

29 Al Hussaini, A. (2011) Lesbian Blogger is Married American Man, *Global Voices*, 13 June. globalvoicesonline.org/2011/06/13/syria-lesbian-blogger-amina-is-a-married-american-man

30 [en.wikipedia.org/wiki/Sockpuppet_\(Internet\)](http://en.wikipedia.org/wiki/Sockpuppet_(Internet))

31 en.wikipedia.org/wiki/Astroturfing; see also Monbiot, G. (2011) The need to protect the internet from ‘astroturfing’ grows ever more urgent, *The Guardian*, 23 February. www.guardian.co.uk/environment/georgemonbiot/2011/feb/23/need-to-protect-internet-from-astroturfing

32 Bright, P. (2011) Anonymous speaks: The inside story of the HBGary hack, *ars technica*, 15 February. arst.ch/09q

33 Anonymous (n. d.) Operation Metal Gear, *AnonNews*. anonnews.org/?p=press&a=item&i=752

UGC is still being used actively in Egypt and Tunisia to expose violations of the security forces. In Egypt, the military recognised the power of Facebook and made a Facebook page after the fall of Mubarak to try to garner support and make peace with the protesters.

The transition in Egypt and Tunisia is still unfolding – elections need to be planned, political parties organised, reorganised and new ones formed. These processes cannot be conducted today without the internet and ICTs.

Some issues the online activist needs to bear in mind include:

Anonymity and monikers

User-generated content can, if not used carefully, expose content creators to surveillance. Many UGC platforms do not allow for anonymity. In light of the concerns raised above about astroturfing and sockpuppetry, anonymity is not ideal for activism, especially if the source of the activism is not known. Nonetheless, in the context of repressive regimes, the protection afforded by anonymity does have its merits.

Anonymity cannot and should not, as Randi Zuckerberg, ex-marketing director of Facebook has suggested, “go away.”³⁴ Despite calls by some authorities – the British Police for example – to end the use of anonymous monikers on platforms like Twitter,³⁵ many platforms will not do this. There are legitimate reasons (including personal security) for activists not to use their real names. Content creators should be informed about the possibilities of creating content anonymously and securely and decide whether to use real names or monikers. If anonymity is chosen, creators of content must be aware that small things like a network of real-life friends, one picture or an accidental use of geolocation could expose a user’s identity.

Safe and informed use of social networking

UGC and social networking present the challenge of balancing activism with privacy and online safety. Different platforms offer different strengths and weaknesses regarding the often diverging goals of activism and privacy: Facebook does not allow for anonymity, and the use of monikers is not permitted, while Twitter does allow monikers.

Facebook users need to be aware of the range of possible privacy settings and their implications. Privacy settings can protect users, but minimal privacy settings in certain conditions may be useful for online activism to build and coordinate communities, and spread content virally.

Each platform for the creation and dissemination of UGC, as well as each social networking website, has terms and conditions which users should be aware of. Users should also be aware of the national legal and regulatory environments governing privacy and the internet in the countries in which these UGC platforms are hosted.

Backup and mirroring of content

At the end of the day, it is the social networking platform or content platform on which the content is hosted that has the ultimate control over their online content. Unless, of course, users have this content backed up or mirrored (duplicated on another website).

There are alternatives to Facebook

It would be beneficial if activists were afforded access to social networking tools that they could exercise more control over, especially with regards to the hosting of their content, and their privacy and anonymity.

There are alternatives to social networking platforms such as Twitter or Facebook. The social networking platform Diaspora is nodal and peer-to-peer. Users can host their own identities or “pods”, and choose from a range of hosts to host their pod on.

Self-hosted or smaller social networking platforms have many advantages. However, they may not be able to invest as much in security as their larger counterparts. Even big “brand” social networks can experience problems securing private data.

UGC under surveillance

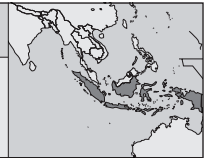
If the avoidance of state surveillance is required, certain practices should be followed wherever possible when disseminating UGC. Platforms offering end-to-end encryption should be defaulted to wherever possible. Facebook, Twitter and other social networking applications, web-based email and web-based applications should always be accessed through HTTPS encryption if it is available (by typing https:// instead of http:// before a web address).³⁶ HTTPS will help avoid the stealing of usernames and passwords as well as eavesdropping. Anonymising tools such as proxies, virtual private networks (VPNs) and Tor can also be used for protecting the identity of content creators, as well as for circumventing filtering and censorship. Tor has been particularly helpful in protecting activists and journalists in the MENA region.³⁷ ■

34 Bosker, B. (2011) Facebook’s Randi Zuckerberg: Anonymity Online “Has to Go Away”, *The Huffington Post*, 27 July. www.huffingtonpost.com/2011/07/27/randi-zuckerberg-anonymity-online_n_910892.html

35 Chen, A. (2011) Clueless British police suggest Twitter require real names, *Gawker*, 26 August. gawker.com/5834776

36 The Electronic Frontier Foundation has a plug-in for Firefox which can be downloaded from its website (www.eff.org/https-everywhere). The plug-in will instruct the browser to always connect to HTTPS (if available) when viewing a website.

37 Zahorsky, I. (2011) Tor, Anonymity and the Arab spring: An Interview with Jacob Appelbaum, *Peace and Conflict Monitor*, 1 August. www.monitor.ucepe.org/innerpg.cfm?id_article=816



Technology and protest in Indonesia

The ways that human rights activists have employed new technologies have shaped the political upheavals that have punctuated Indonesia's recent history. Probably the best-known example is the footage of human rights abuses in East Timor during the late 1990s, which was televised globally and became one of the key factors in garnering international support for Timor-Leste's independence.¹

The experience of the 1998 political uprising that overthrew the Suharto regime also showed the power of digital video in generating extensive socio-political changes by mobilising people in support of a new government. In the build-up to the end of the regime, footage of the shootings of Trisakti University students in Jakarta, much of which was "amateur" footage, was broadcast on television inside and outside Indonesia. These images sparked sentiments of national solidarity, leading to mass student protests in several cities across Indonesia, denouncing the New Order regime.

However, today, without the same momentum of mass direct action on the streets that characterised the end of the 20th century in Indonesia, the ways that video can be used to affect change are more ambiguous. Realising that they cannot rely on the foreign press to expose humiliating human rights violation cases, campaigners push their videos through other avenues – such as EngageMedia, YouTube and Facebook – where, instead of relying on news corporation producers, activists can become the producers and distributors themselves. But in becoming more independent, their responsibilities also shift, particularly when it comes to contextualising video information.

This report is concerned with what activists can do with video to improve the situation in West Papua and Indonesia more broadly: to stop human rights abuses, to bring perpetrators to justice, to prevent torture, and to end violence. Our approach is to compare the production and distribution of videos documenting incidents of abuse in order to deepen activist understanding of the mechanics of online distribution of video that has the purpose of social change. This focuses on the work of EngageMedia as one organisation investing in making this distribution not only more effective, but more mindful and secure.

Human rights abuses in West Papua and elsewhere

Indonesia ratified the UN Convention Against Torture in 1998, the same year the brutality of the New Order regime was meant to end. However, the Asian Human Rights

Commission says, today "torture is in fact encouraged as a mean[s] of interrogation and intimidation by the police and the military."² Because military personnel enjoy special immunity from being tried in civilian courts, acts of torture continue to go unpunished.

Amnesty International reports that in recent years there have been a number of cases of intimidation and attacks against human rights defenders and journalists in Indonesia. Many of these cases have occurred in the province of West Papua, given "special" autonomy by the Megawati government in 2001. West Papua is one of the least accessible places in Indonesia and one of the richest in natural resources.

This report does not have the scope to cover the struggle for self-determination in West Papua. Suffice to say that allegations of torture in the region are hardly new. Since it became part of Indonesia in the 1960s, there has been both a resilient separatist movement and a strong military presence.³ Amnesty International has documented how victims and witnesses in Papua have few available legal remedies to make complaints.⁴ Perhaps more than anywhere else in Indonesia, human rights violations in West Papua have gone unchecked for decades.

As recently as July 2010, Tama Satrya Langkun, a Jakarta-based anti-corruption activist, was severely beaten by unknown persons in an apparent move to silence him. That same month, Ardiansyah Matra, a journalist covering corruption and illegal logging in Papua, was found dead in the province. Despite police investigations, no one has yet been held accountable for these attacks.

Documenting torture

On 30 May 2010, Indonesian military personnel tortured Tunaliwor Kiwo, a Papuan farmer, and his neighbour, using a number of methods, including clamping their genitals, burning them with an iron rod, trying to suffocate them with

2 Asian Human Rights Commission (2010) Indonesia: Video of the military torturing indigenous Papuans surfaced, press release, 17 October. www.humanrights.asia/news/press-releases/AHRC-PRL-021-2010

3 For background on the issues in West Papua, see Drooglever, P. (2009) *An Act of Free Choice: Decolonisation and the Right to Self-Determination in West Papua*, Oneworld Publications, Oxford.

4 See the following reports: Amnesty International Papua Digest, January 2011. www.amnesty.org.uk/uploads/documents/doc_21212.pdf; Open letter on unchecked police abuse in Nabire district, Papua (Index ASA 21/024/2009), 30 November 2009. www.amnesty.org/en/library/info/ASA21/024/2009/en; Unfinished business: Police accountability in Indonesia (Index ASA 21/013/2009), 24 June 2009. www.amnesty.org/en/library/info/ASA21/013/2009/en; Amnesty International's briefing to the UN Committee Against Torture (Index ASA 21/003/2008), 15 April 2008. www.amnesty.org/en/library/info/ASA21/003/2008/en

1 KUNCI Cultural Studies Center and EngageMedia (2009) Video Activism and Video Distribution in Indonesia. www.engagemedia.org/videochronic

plastic bags and pulling out their fingernails with pliers. The incident was recorded on a soldier's mobile phone. The ten-minute torture video was released to the public on 18 October 2010, after being leaked to activists. The video was distributed on several websites including the Asian Human Rights Commission (AHRC) site from October and received international attention. Since then, the AHRC has reported attacks on their website along with the sites of several other groups who featured the torture video, including Survival International, West Papua Media Alerts, the Free West Papua Campaign, Friends of People Close To Nature and West Papua Unite. The video also appeared on YouTube.

Many questions arise from this incident, including whether or not this is part of a military culture in which such actions are not considered criminal. Why would a perpetrator want to take pictures of their crime? It is hard to believe that with the ease of upload/download technologies, a soldier would not understand how quickly a video such as this could be disseminated and circulated. Wondering the same about the documentations of abuses at Abu Ghraib, the great United States (US) philosopher Susan Sontag wrote that, rather than being trophies, these images are "inspired by the vast repertory of pornographic imagery available on the internet" and are evidence of the "increasing acceptance of brutality in American life."⁵ Perhaps the same could be said of the mainstreaming of violence in Indonesian life – perhaps this acceptance is, sadly, universal. The mutilation of genitals in the cases of both Abu Ghraib and Kiwo's torture represents a violence that seems intertwined with the sexualisation of victims' bodies.⁶ Clearly, video evidence of torture presents ethical dilemmas, not only around how it is made and released, but how it is watched and how those who watch are implicated in the processes of social change.

Responding to the public attention around the torture video, video testimony was produced by human rights activists in Jayawijaya. The video testimony was an effort to provide more direct evidence for the case and also to respond to some of the dilemmas mentioned above by contextualising the event. It was passed along to the Papuan Customary Council – Dewan Adat Papua – and handed to Human Rights Watch. The interview was conducted in Lani (the language of the Jayawijaya region – Papua has over 200 languages), which was later translated into Indonesian by a Lani activist, and subtitled in both Indonesian and English. In November, EngageMedia released both videos of the testimony, one with English subtitles,⁷ one with Indonesian subtitles.⁸

Video testimony, as opposed to documentary, allows the victim to create his or her own narrative. But in order to be

effective, to be able to circulate in the wider world, these narratives require a great deal of context. Translation and subtitling take on renewed importance because they are part of the process of getting as close as possible to the victim's expression of events and making that expression the core of social change campaigns. For such cases, EngageMedia is currently teaming up with Universal Subtitles, an open source, online system that enables collaborative translation and subtitling of video. The system can be accessed on the Universal Subtitles website itself, and can also be used in concert with other video sites such as EngageMedia.org, tapping into already existing networks and communities.⁹

Being sensitive to local languages is just one of the practical challenges of using video in torture cases. "Given the previous cyber attacks," says Enrico Aditjondro, EngageMedia's Indonesia editor, "the decision to publish the testimony was a calculated risk that required careful preparation to ensure the safety of all organisations and individuals involved." As well as Universal Subtitles, EngageMedia teamed up with Human Rights Watch and others to urge the Indonesian government to mount a thorough, impartial and transparent investigation into the episode. This collaboration is important in tracing the way video can be used in concert with human rights campaigns in raising public awareness and bringing about social change.

The Indonesian government responded with a rapid trial of the soldiers involved. The AHRC says the trial only came about after heavy national and international pressure, and the result does not provide an adequate remedy for the gravity of the human rights violations. The perpetrators have not been charged with their actual crime and AHRC rejects this trial as a conclusion of the case. This is not surprising, considering the track record of the Indonesian government in coming to terms with human rights abuses, evident in other cases such as the poisoning of human rights activist Munir Said bin Thalib in September 2004, and the failure to convict any of the generals accused of war crimes in East Timor or Aceh.

Aditjondro says EngageMedia learns from each of these experiences, and continues to face similar dilemmas, most recently concerning the publication of what is known as the "Ahmadiyah Video". In February 2011, hundreds of villagers in Banten province, west of Jakarta, were filmed marching to a house where twenty Ahmadi¹⁰ had met. The video shows three bloody bodies of Ahmadi men who had been stripped, beaten and dragged from the house to the

5 Sontag, S. (2004) Regarding The Torture Of Others, *New York Times Magazine*, 23 May.

6 Carby, H. (2004) A strange and bitter crop: the spectacle of torture, *OpenDemocracy*, 10 October. www.opendemocracy.net/media-abu_ghraib/article_2149.jsp

7 www.engagemedia.org/Members/dewanadatpapua/videos/kiwotestimony_rev_en.mp4/view

8 www.engagemedia.org/Members/dewanadatpapua/videos/kiwotestimony_id/view

9 The aims for this collaboration are to broaden access to critical human rights and environmental stories from within Southeast Asia, increasing regional and international exposure; develop a Southeast Asia network of volunteer translators and subtitlers of citizen media, human rights and environmental video content; enhance the communication between video advocates, campaigners and citizens in the region to develop shared understandings of the common issues they face; and provide easy access to television stations and other websites to pick up and run non-native language content.

10 Ahmadi, who practice the Ahmadiyah form of Islam, have been subject to various forms of persecution since the movement's inception in 1889. Ahmadiyah is a controversial religious minority in Indonesia that rose sharply in the 2000s with a rise of Islamic fundamentalism. As of 2011, the sect faces widespread calls for a total "ban" in Indonesia.

ground outside. Police officers appear in the video, making no attempt to stop the killing, and scores of young men looked on, recording it with their mobile phones.¹¹

EngageMedia and other independent media channels were immediately sent the footage by some of those who recorded the incident. While EngageMedia decided against posting the video on its site, journalist and human rights campaigner Andreas Harsono from Human Rights Watch used his own YouTube account to publish the video. Within minutes, he received numerous death threats. After receiving over 100,000 hits, the video was flagged and blocked. An anonymous uploader then re-posted the complete video on YouTube where it was still available at the time of writing, but viewers need to sign in to see it, due to the graphic nature.¹² Aditjondro says:

For credibility and integrity, taking responsibility for videos like this is important when they go out in public. But such actions can also endanger advocacy work and made people associated to him [Harsono] vulnerable as well. The story of Andreas Harsono helped activists realise the security implications of doing digital campaigning, particularly those activists working in more repressive environments such as West Papua.

Aditjondro also says that EngageMedia, knowing that the videos would be on YouTube, was more concerned with contextualising the event, and posted a news story with links to the footage.¹³ "Watching violence for the sake of it doesn't achieve anything," he says.

This incident, and the extrapolation of the torture video into Kiwo's testimony, also point out some of the responsibilities video makers and distributors have to their subjects and how people watch and interpret disturbing footage. While all activists have the same aim of exposing violations of human rights, not all campaigns take the same measures to make sure victims and their supporters have a voice and still remain secure.

In the case of the video of the torture itself, we cannot know how this video got into activist hands, whether it was intentionally or accidentally leaked. But, having the infrastructure in place for distribution, what we do with these opportunities in a way that is responsible and clear is a great challenge. This requires partnerships between technologists and human rights agencies. More than ever before, these networks must operate with an unprecedented level of security, speed and collaboration.

Concluding notes

Kiwo's story and the ways video has been generated from it tell us a great deal about the potential of information and communications technologies (ICTs) for human rights and social resistance. But they also relay the limitations of online video activism. Without an approach that also supports victims of human rights abuses in their day-to-day lives, in their own languages, what good is such evidence?

This report has focused on particular incidents because of the repercussions on activist security and because of the clear pressure they put on authorities. But this report concerned the impact of video in specific incidents. The story of human rights in Papua and other places is far more complex. Infant mortality, sexual health, land rights, access to basic human needs all indicate a grim situation for many indigenous people all over the world. Yet these stories are unlikely to receive many hits on YouTube. How can these issues also be integrated into a different type of activism, one that can move beyond the shock of violence shaming us into a real world response?

Perhaps more than any other medium, video has the power to reframe stories. Kiwo's story is much more than a file viewed in browsers and copied over servers. Taking responsibility for how videos effect change is about making them more than nameless images of violence.

Action steps

The immediate action to be taken around this incident is demanding the retrial of the soldiers who perpetrated the torture of Kiwo and his neighbour. This requires ongoing support for local activists in West Papua from regional and global networks.

More broadly, activists need to:

- Be informed. Listen, watch and read stories from West Papua at www.engagemedia.org/taxonomy/countries/WP
- Follow the AHRC campaign to end violence in West Papua at www.humanrights.asia/countries/indonesia/end-violence-in-west-papua
- Sign the petition opposing US cooperation with Kopassus (the Indonesian Special Forces Command) at www.gopetition.com/petitions/dont-train-indonesias-deadly-kopassus.html
- Consider security implications to filmmakers and witnesses when conducting video documentation of human rights violations
- Download *Video for Change: A How-To Guide on Using Video in Advocacy and Activism* from www.witness.org
- Visit Tactical Tech Security-in-a-Box at www.tacticaltech.org/securityinbox ■

11 Dewan, A. (2011) Why We Should Support Indonesian Schools, *New Matilda*, 16 February. newmatilda.com/2011/02/16/why-we-should-support-indonesian-schools

12 www.youtube.com/verify_age?next_url=http%3A%2F%2Fwww.youtube.com%2Fwatch%3Fv%3DDWHzc8ZxRuQ%26feature%3Dplayer_embedded

13 EngageMedia (2011) Ahmadiyah bloodied video leads to calls for revoke of decree against religious minority, 14 February. www.engagemedia.org/Members/cikeusik/news/ahmadiyah-bloodied-video-leads-to-calls-for-revoke-of-decree-against-religious-minority

UNITED KINGDOM

Open Rights Group
Javier Ruiz
www.openrightsgroup.org



Introduction

The global crisis in the UK

The financial crisis of 2008 hit the United Kingdom (UK) particularly hard. Besides its own housing bubble, and the vulnerability to commodity prices due to the global character of its economy, Britain had to provide support to a disproportionately large financial sector around the City of London, which was estimated would add £1.5 trillion to the national debt.¹ Although the recession officially ended at the end of 2009, the economy has not recovered sustained growth, and unemployment is on the rise, with fears of a double-dip recession. However, the defining aspect of the crisis in the UK has not been foreclosures, price increases or youth unemployment, but the national debt.

Austerity...

The centre-right coalition government that took power in May 2010 made reducing the national debt its main priority, and quickly embarked on a major austerity programme that it claimed could lead to an irreversible reshaping of the welfare state. The necessity and severity of the cuts are widely debated,² and in particular their relationship to bailing out the banking sector.³ There is also a widespread popular perception of bankers as villains, particularly in relation to the payment of large bonuses, fuelled by the rapid recovery of the sector in contrast to the rest of the economy. There are also fears that these cuts will push the country further into recession.⁴

...and its discontents

Perhaps surprisingly, the government – particularly the Conservative majority in the coalition – has not suffered the expected level of political backlash seen in other countries under strict austerity measures, such as Spain. However, this does not mean that there is no opposition to these policies. The past year has seen an unprecedented intensity of social struggles by students, independent civic networks and trade unions, with the support of a large sector of the population. This past year has also witnessed a major escalation in innovative uses of the internet for social mobilisation, although it remains unclear whether this has reached its full potential for organisation and coordination.

UK Uncut

We have chosen the new phenomenon called UK Uncut as the central story for our report. Although it is not the largest or most sophisticated operation in terms of internet use, overall it is the most innovative.

UK Uncut came to prominence after 70 activists occupied and closed down mobile company Vodafone's flagship store in Central London on 27 October 2010.⁵ They had been mobilised on Twitter by the use of the hashtag #ukuncut, prompted by claims that Vodafone had been given an unfair amnesty on £6 billion of unpaid taxes, enough to cover some of the most severe cuts in social welfare. Within three days the protest had gone viral and 30 Vodafone stores had been occupied or picketed around the country.

There are now about 40 local Uncut groups in the UK, regularly organising fortnightly occupations and pickets of high street names associated with tax avoidance, including clothes retailer Topshop, the pharmacist Boots, and the banks HSBC and Barclays. Meanwhile, a spin-off called US Uncut has started across the Atlantic in the United States, with around 100 local participant nodes.

UK Uncut is characteristic of many current political phenomena in rejecting any form of incorporation or legal structure. In itself this is not new, UK Uncut being the latest incarnation of a particular political culture of creative non-violent direct action. Since the mid-1990s these networks have been very active in the UK on environmental issues, international solidarity, and the so-called anti-globalisation movement. These loose networks are generally composed of organising clusters based on personal acquaintance that coalesce around specific forms of action, rather than ideology. As a result we have seen clusters such as Reclaim the Streets, protest samba bands and a Climate Camp, among many others.

The focus on common action rather than political discourse can be very effective at cutting through complex arguments. Although most of the people in these networks would probably describe themselves as anti-capitalists, UK Uncut has focused on a very simple equation between cuts and tax avoidance. Also, closing down a store in a busy high street has a direct economic effect, albeit small.

Anyone can use the UK Uncut "brand" and call an action, and despite the potential for abuse, the core London organisers have only had to disown a very few fake calls to action.

UK Uncut core communications uses what has become the standard mobilisation toolkit of social media: Twitter, Facebook and a blog. They have large numbers of followers

1 www.thisismoney.co.uk/news/article.html?in_article_id=493025&in_page_id=2

2 www.thisismoney.co.uk/credit-crisis

3 www.guardian.co.uk/politics/2009/feb/20/public-debt-gordon-brown

4 www.guardian.co.uk/politics/2011/jun/04/george-osborne-plan-not-working

5 www.ukuncut.org.uk/about/ukuncut

on all platforms – almost 30,000 on Twitter – and take pride in being media savvy. This includes placing tactical articles in progressive newspapers, such as *The Guardian*, and use of short viral YouTube videos.

Despite the strong use of the internet for mobilisation for actions, aspects of the actual planning – secretive by necessity, such as choosing a target – tend to rely on face-to-face personal communication and trust, while organisational continuity is maintained typically in weekly or fortnightly evening meetings in public places.

Winter of discontent 2010-2011

UK Uncut are smart netizens, but they are not alone. These same online tools were also used by students in their ultimately unsuccessful protests against the trebling of university fees to £9,000 per year, in what nevertheless became some of the most challenging demonstrations for the authorities in years. This winter up to 50,000 students took to the streets on three occasions in disdain at their own National Union of Students, seen as weak and too close to the political establishment. Social media, with Twitter tags such as #dayx, brought out much larger numbers of students than expected by both organisers and police.

The opening salvo was the spontaneous mass occupation of the headquarters of the Conservative Party on 10 November 2010, which caused widespread shock and energised the students. This was followed by several increasingly assertive demonstrations accompanied by violent repression as authorities attempted to re-establish control of the situation. For the first time in recent memory, student protests included the more socially and ethnically diverse pupils from secondary education, who unlike their counterparts elsewhere in Europe, are generally not politicised. These protests were broadcasted around the world by satellite channels and weaved across social media. The UK has a disproportionate influence in global culture, as seen with the recent royal wedding of Prince William and Kate Middleton, and the student demos were followed live at homes in the Middle East,⁶ together with updates on WikiLeaks' release of US diplomatic cables.

The anti-fees days of action, together with a wave of dozens of high profile campus occupations,⁷ have been a significant political epiphany for a whole generation of students, largely outside unions and political parties. This also includes traditional left outfits that had dominated much of the resistance to the Iraq war. These new networks, some of them already active in campaigns against the Gaza war in January 2009, are finding their way into the wider anti-cuts movement, with many students taking part in UK Uncut actions.

At the same time, mainstream labour unions, completely tied up with the Labour Party and traditionally quite reluctant to mobilise, made some unprecedented moves this

winter. Several large unions have publicly supported the students and UK Uncut⁸ – including mobilising for actions – with some even calling for “non-violent resistance”⁹ and a “broad strike movement”¹⁰ against what they see as all-out war on the welfare state.

Part of this rapport was an attempt to harness the online world with a large conference in January 2011 called Netroots UK,¹¹ which brought together 500 trade unionists, activists and key digital players. This included influential blogs, such as Liberal Conspiracy,¹² and specialist online campaigning organisations 38 Degrees and Avaaz. The presence of US providers of campaigning services and tools, such as Blue State Digital, was a giveaway to its being inspired by the US initiatives¹³ that helped bring Barack Obama to the White House.

The event was broadly perceived in positive terms, but ultimately it did not lead to a progressive digital front in the UK. Clear divisions emerged on a range of issues such as support for the Labour Party, although in the long term more subtle cultural differences may have also played a role. The large mobilisation of trade unions against the cuts on 26 March 2011 saw over 250,000 people in Central London, but in every way it was a traditional left and unions march. On the day, UK Uncut organised a series of theatrical actions independent from the main march, culminating in a mass occupation of luxury retailer, popular tourist destination and alleged tax avoider Fortnum and Mason's, which led to the controversial arrest of 145 people.

The most innovative use of Twitter on the day came from the police, whose @CO11MetPolice account¹⁴ had been tested for the first time during the Climate Camp protests in 2009. Meanwhile, some technical activists have upped the ante and developed their own live mobile information system to enable demonstrators to evade police lines. The Sukey project¹⁵ is a technological breakthrough in a long cat-and-mouse information game between police and protesters in Europe that has seen the development of multiple SMS and web systems, including Indymedia's early experiments with Twitter,¹⁶ and had even led to eight activists being sentenced to long prison terms in Sweden in 2001.¹⁷ The project is still in early stages, but as in previous attempts the critical success factors will be adoption rates and trust by activists.

The anti-cuts demo #march26 was called and organised by unions, but many of the participants in the main

8 www.unitetheunion.org/news__events/latest_news/unite_backs_uk_uncut_s_banks_a.aspx

9 www.coalitionofresistance.org.uk/2011/06/rail-union-tssa-votes-to-participate-in-non-violent-resistance-activities

10 www.guardian.co.uk/commentisfree/2010/dec/19/unions-students-strike-fight-cuts

11 www.netrootsuk.org

12 liberalconspiracy.org

13 www.netrootsnation.org

14 twitter.com/#!/CO11MetPolice

15 sukey.org

16 www.indymedia.org.uk/en/2007/09/380691.html

17 en.wikipedia.org/wiki/Protests_during_the_EU_summit_in_Gothenburg_2001

6 See Solomon, C. and Palmieri, T. (eds) (2011) *Springtime: The New Student Rebellions*, Verso, London.

7 occupations.org.uk/occupations-2010

march came from other backgrounds. Many of these people travelled to London in trade union TUC¹⁸ buses or by independent means. There were also citizens with disabilities, who are doubly targeted by the cuts in services and reductions of benefits.¹⁹ Of course the students were there, together with lawyers and NGOs protesting cuts in legal aid,²⁰ and campaigners concerned about radical reforms to the National Health Service. Despite the large and diverse crowd, small side events organised by anarchist networks, punctuated by attacks on banks and luxury shops, grabbed the attention of mainstream media.

Since the cuts were announced in May 2010, innumerable local campaigns have been organised by communities trying to save specific services ranging from children's centres and public libraries to hospitals and parks.²¹

These networks are all organising regular actions and campaigns, including UK Uncut, which seems to have survived the mass arrest of its London core. Several large trade unions also planned a coordinated strike on 30 June 2011, which promised to become the next focal point for the anti-cuts networks.

Organisation

The #march26 demo showed that the current landscape of social struggle in the UK is very rich and diverse, composed of overlapping networks, campaigns and organisations, and UK Uncut is embedded in this mesh. Questions remain, however, on whether this movement will be successful in achieving its aims. Local campaigns, mostly organised around Facebook pages, have little influence on decisions taken by central government, while large demonstrations without continuity are occasional storms any government can cope with. Even some of the most successful national single-issue campaigns, such as those on legal aid and disability, taken in isolation will simply push the cuts elsewhere, notwithstanding the positive contagion effect they may have.

As we saw in relation to Netroots UK, attempts to bring together diverse groups are fraught with difficulties. The leftwing gathering²² around the union-led Coalition of Resistance²³ seemed to reproduce the model of past experiences, such as the unsuccessful Put People First mobilisation around the London G20 in 2009.²⁴ Nevertheless, in a departure from the past, they now support non-violent civil disobedience, and even help publicise UK Uncut actions. Proponents of a more grassroots approach believe that a union-led campaign will fail to engage the rest of society af-

ected by austerity policies,²⁵ but the alternatives have so far failed to materialise.

There are profound differences on the type of organisation needed, with an important sector believing that these decentralised networks fuelled by the internet – UK Uncut, students, etc. – will be enough to generate a new movement with sufficient coordination to reverse the cuts.²⁶ The success of leaderless network movements in the Middle East and North Africa seemed for a while to vindicate this approach, although this is now tempered by events in several countries such as Syria.

A halfway point is provided by the website False Economy,²⁷ which provides a very polished portal of information on campaigns, also allowing the publication of new events. There are also several other projects using web tools to allow people to report and map specific cuts.²⁸ However, there are no spaces for the national coordination of campaign groups, and despite lots of ad hoc communications through backchannels, nobody is publicly discussing a real strategy.

UK Uncut activists claim they would like to have a national meeting of local campaigns, despite the difficulty of not knowing who exactly organises in each city. However, they fear the authorities would use it as an opportunity to clamp down on alleged ringleaders, in another step in the campaign of sustained repression against them.

Action – reaction

After being caught off guard by UK Uncut, the authorities slowly reacted. There had been some minor arrests around the country and isolated use of pepper spray against peaceful protestors in London. However, the mass arrest on 26 March of 145 activists seems to be a turning point designed, albeit unsuccessfully, to incapacitate the organisation. Bail conditions prevent the activists from entering the main shopping area in Central London and all their clothes were taken for forensic examination. In a new frontier for rights and technology, their smartphones were confiscated with all their digital social and political life inside. To achieve this with home computers would have required a special warrant.

The fact that there were almost no other arrests on the day other than for non-violent protests, despite the destruction of property by others, has generated criticisms of the Metropolitan Police's handling of the situation. Some lawyers have said that this is an attack on the fundamental democratic right to protest.²⁹ Large sectors of the media have falsely portrayed UK Uncut as responsible for the violence, no doubt helped by police Twitter messages such as:

18 righttework.org.uk/2011/01/transport-to-the-tuc-march-for-the-alternative-on-26th-march

19 www.dpac.uk.net/2011/02/light-up-a-map-of-the-uk-online-in-solidarity-with-the-protesters-on-the-streets-on-26-march

20 www.justice-for-all.org.uk/Who-we-are

21 stopthecutscoalition.org

22 www.guardian.co.uk/commentisfree/2010/aug/04/time-to-organise-resistance-now

23 www.coalitionofresistance.org.uk

24 www.putpeoplefirst.org.uk

25 www.guardian.co.uk/commentisfree/2010/aug/09/tony-benns-coalition-resistance-needs-strategic-approach

26 See the article on Open Sourcing of Political Activism by Guy Aitchison and Aaron Peters here: felixcohen.co.uk/FightBack

27 falseeconomy.org.uk

28 wherearethecuts.org and anticuts.org.uk

29 www.guardian.co.uk/uk/2011/mar/30/uk-uncut-arrests-protests?CMP=NECNETTX1766

@CO11MetPoliceMetropolitanPolice

Fortnum and Mason's is surrounded by police as this is a crime scene. Persons responsible will be arrested #ukuncut

The use of Twitter by police has been criticised by several of the people interviewed for this report. There is an impression of lack of accountability, which allows messages out that would be a lot more nuanced in a press conference.

Students have also been treated quite harshly. Prime Minister David Cameron threatened that the "full weight of the law" would fall on students who occupied the Conservative headquarters,³⁰ with sectors of the media collaborating in publishing "Wanted" photo galleries to help hunt for suspects.³¹

Police handling of further student protests and smaller marches that broke away from union-organised events has generated great controversy. This is particularly due to the widespread use of "kettling", which involves surrounding and corralling protesters for long periods of time without proper access to food, water or sanitation. Critics claim this is a punitive detention designed to put people off from going to demonstrations, rather than preventing breaches of public order. It is also claimed that this containment technique provokes more violence as protesters feel trapped and attempt to break through police lines. Besides kettling, police have been criticised for excessive baton charges and riding horses against groups of schoolchildren.

Separately, police have arrested suspected protest leaders in early morning raids, particularly around the time of the royal wedding³² – although it is unclear how police intelligence relates to internet surveillance. According to protester support group Green and Black, and lawyer Mike Schwartz from Bindmans, there are no known cases of people being arrested on the basis of evidence collected on social media. However, comments made on Facebook have apparently been brought up in court to support the case against those arrested for public disorder.

A very controversial incident involving Facebook was the closure of over 50 profile pages of protest groups on the eve of the royal wedding,³³ ostensibly for breaching the terms and conditions of Facebook, which make clear that organisations cannot use personal profiles. Facebook denies any active involvement, claiming that closures are automated if sites are reported. Attempts by Open Rights Group to find out the level of coordination behind the closures have been stonewalled by Facebook. Interestingly, Richard Allan, Facebook EU head of policy, claims that a similar situation happened in Egypt during the protests, which led to them

strengthening their processes for migrating from personal profiles to pages suited for organisations. Egyptian activists have partly confirmed this.

Without Facebook's collaboration we will probably never know who reported the offending protest sites, and whether this involved elements of the state. An early attempt by police to close down a website providing students with advice on destroying potential evidence to avoid arrest³⁴ backfired when it was mirrored WikiLeaks style. Since then the authorities have taken a more conciliatory tone, with, for example, Sukey being invited to friendly talks with police – although this could also be interpreted as letting the activists know they are known.

In an attempt to counter criticisms, the police took the unprecedented step of allowing human rights observers into their control room for the 26 March demo, but they were criticised³⁵ for the fact that the use of kettling was considered as first resort. In general, the ubiquity of multimedia recording devices and social media has had an effect on police, with several high-profile cases where they have been caught lying red handed.³⁶ A recent court ruling in April 2011 placed further restrictions on the use of kettling.³⁷

In general, the repression of the anti-cuts movement, while fairly harsh for UK standards, is quite targeted and has not reached large sectors of society. However, it shows that the movement has not yet managed to break into politically neutral spaces to dominate the national conversation, win the arguments and de-legitimise any criminalisation. This, for example, has happened in Spain with the build up of the broad and radical democracy and anti-austerity movement, organised around town square occupations. There are further protests and strikes on the horizon.

P.S. And then the riots – looking back at action steps already taken

As this report was being finalised, we witnessed the largest explosion of civil unrest in England in living memory, with five people killed in various incidents and widespread looting and arson. The disturbances started after police in North London shot a black suspect, but quickly spread, first across London and then major cities in England. Although there were no clear political demands, the demographics of those arrested show the majority to be very young and generally unemployed, with 41% living in the top 10% of the poorest areas of the UK.³⁸

The aftermath has seen a draconian crackdown that resembles an undeclared state of emergency, admittedly with widespread support from the majority of the population, who after the shock and fear are now in the mood for vengeance. Around 3,000 people have been arrested³⁹ as

30 www.opendemocracy.net/ourkingdom/guy-aitchison/significance-of-millbank-british-protest-begins

31 www.thisislondon.co.uk/standard-pictures/CCTV+images+of+student+riot+suspects+released+latest.do?id=23379553

32 news.sky.com/skynews/Home/Royal-Wedding/Royal-Wedding-Police-Have-Arrested-20-People-Amid-Fears-Of-A-Plot-To-Disrupt-The-Royal-Wedding/Article/201104415981406

33 wiki.openrightsgroup.org/wiki/FB_takedowns

34 www.fitwatch.org.uk

35 www.bbc.co.uk/news/uk-13109259

36 en.wikipedia.org/wiki/Death_of_Ian_Tomlinson

37 en.wikipedia.org/wiki/Kettling

38 www.alex-singleton.com/?p=507

39 www.guardian.co.uk/news/datablog/2011/aug/09/uk-riots-data-figures

police pore over 20,000 hours of closed circuit television (CCTV) footage. Some 100 people have been sent to prison every day since,⁴⁰ with courts instructed to “disregard normal sentencing guidelines.”⁴¹ As an example, a college student without a criminal record was jailed for six months for the opportunistic theft of a bottle of mineral water.⁴² The government is calling for those convicted to be “stripped of benefits,”⁴³ and the newly launched e-petitions site has seen 216,000 people in support of this measure.⁴⁴ Some families where one member has been arrested during the riots are already being evicted from social housing.⁴⁵

In this bonfire of liberal values and civil rights the internet and social media have received special attention. While North London was still in flames, a local parliamentarian unsuccessfully called for shutting down Blackberry Messenger (BBM) service, pointed out as the key tool rioters were using to coordinate.⁴⁶ Blackberrys are the most popular smartphone with UK youth, holding a 37% market share,⁴⁷ partly due to BBM, their free messaging service. BBM runs on Blackberry’s internal network and is scrambled with basic encryption,⁴⁸ which makes it more difficult to monitor than the fully transparent Twitter. This has been seen as a threat by several governments around the globe, such as India,⁴⁹ although in the UK Blackberry is fully cooperating with authorities.⁵⁰

The prime minister launched a widely condemned attack on social media as part of his speech to Parliament on 11

August.⁵¹ David Cameron initially called for police to be able to shut down social networks, and for rioters to be banned from using social media. In our experience of preferred modes of internet governance in the UK, the government will probably eschew new kill-switch powers for police, and probably propose some self-regulated scheme. Home Secretary Theresa May has announced a meeting with major social media firms Facebook, Twitter and RIM (the company behind Blackberry).⁵² It remains to be seen whether social media companies will risk their reputation by agreeing to self-censorship, or the UK government will press with new legislation. A seventeen-year-old has already been banned for twelve months from Facebook by a judge after posting a message saying “I think we should start rioting, it’s about time we stopped the authorities pushing us about and ruining this country.”⁵³ Separately, two young men have received four-year prison sentences for setting up calls on Facebook for “riots” in rural areas. In both cases only the police turned up and no violence took place.⁵⁴

Many of the critics of this attack on the internet and social communications point at the valuable role these served in providing timely information, fundraising for victims, and even the coordination of mass clean-up operations.⁵⁵ And, some argue, social websites have also been used by police, with their Flickr photo gallery of suspects generating hundreds of identification calls.⁵⁶ ■

40 www.bloomberg.com/news/2011-08-20/two-murders-among-crimes-in-uk-riots-police.html

41 www.guardian.co.uk/uk/2011/aug/15/riots-magistrates-sentencing

42 www.telegraph.co.uk/news/uknews/crime/8695988/London-riots-Lidl-water-thief-jailed-for-six-months.html

43 www.communitycare.co.uk/blogs/childrens-services-blog/2011/08/strip-convicted-rioters-of-their-benefits-says-ids.html

44 epetitions.direct.gov.uk/petitions/7337

45 www.guardian.co.uk/uk/2011/aug/12/london-riots-wandsworth-council-eviction

46 www.theregister.co.uk/2011/08/09/bbm_suspension

47 stakeholders.ofcom.org.uk/market-data-research/market-data/communications-market-reports/cm11/uk/1.39

48 www.berryreview.com/2010/08/06/faq-blackberry-messenger-pin-messages-are-not-encrypted

49 www.ft.com/cms/s/0/c73f4b10-bf47-11e0-898c-00144feabdc0.html

50 www.guardian.co.uk/technology/2011/aug/09/london-riots-blackberrys-police

51 www.apc.org/en/node/12807

52 socialmediaobservatory.com/social-media-news/facebook-rim-to-meet-with-uk-government-over-proposed-social-media-ban

53 www.bbc.co.uk/news/uk-england-suffolk-14556016

54 www.guardian.co.uk/uk/2011/aug/16/facebook-riot-calls-men-jailed

55 twitter.com/#!/riotcleanup

56 www.flickr.com/photos/metropolitanpolice/sets/72157627267892973