Twitter revolutions and cyber crackdowns

User-generated content and social networking in the Arab spring and beyond

Alex Comninos

Association for Progressive Communications (APC)
June 2011

Table of Contents

Abstract

This issue paper, part of a series on the mobile internet, investigates the usage of user-generated content (UGC) and social networking websites (e.g. Facebook and Twitter) in the recent protests and uprisings in the Middle East and North Africa (MENA) region, collectively termed the Arab spring. The paper investigates the extent to which these protests and uprisings can be called "Twitter revolutions" or "Facebook revolutions" and investigates the role that UGC distributed over social networks has played in the Arab spring. 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 found to be areas of contestation between protesters and governments not necessarily balanced in favour of protesters. Social networking and UGC can serve as instruments of surveillance, and have been used to track and locate protesters and content creators.

Lessons learned from the Arab spring and related events in 2011 about social networking and user-generated content are extrapolated from the overview. These include issues of privacy and surveillance, issues regarding the reliability and veracity of UGC and the strengths and weaknesses of Twitter and Facebook for advocacy, as well as the implications of their terms of service and the increasingly worrying practices of sockpuppetry and astroturfing on content platforms. Suggestions on safe and informed use of social networking by protesters and activists facing repressive regimes are offered.

1. 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 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.

User-generated content (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 Twitter. UGC played an important role in the recent protests and uprisings in the Middle East and North Africa. And UGC created on mobile phones was particularly important as it allowed those involved in or witnessing the protests to upload content during the protests and report on events live. Mobile phones also allowed protesters to communicate with others and spread their message. Social networks like Facebook and the micro-blogging platform Twitter were the primary online tools used to disseminate this content.

UGC and social networking websites have been used and continue to be used in protests in other countries throughout the Middle East and North Africa (MENA) region. This paper investigates usage of UGC and social networking websites in the recent protests and uprisings in the MENA region, collectively referred to as the "Arab spring"[1] or "Arab awakening". Important issues regarding the use of UGC and social networking websites in struggles for human rights and democracy are also raised.

1.1. Twitter and Facebook revolutions?

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

It is not within the ambit of this paper to discuss whether the uprisings in MENA are political or social revolutions, or rather revolts and uprisings accompanied by military coups or other political developments. The word "revolution" will be used for convenience, as well as to be congruent with current popular discourse. Of concern is rather the role of UGC and social networking platforms in these events.

The usage of mobile phones, social networking websites and UGC in protests in MENA was not entirely unprecedented. Twitter has been used in protests in Moldova and Iran in 2009 and both these protests were also referred to by commentators as Twitter revolutions.[2] As far back as 2001,

[1]The term "Rabee3 el Arab" (Arab spring), is currently used in Arabic, but not extensively.

[2]The term was applied by Evgeny Morozov to the Moldovan protests in 2009. See Evgeny Morozov "Moldova's Twitter Revolution" (Net Effect, 7 April 2009) 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 2009) neteffect.foreignpolicy.com/posts/2009/04/07/more_analysis_of_twitters_role_in_moldova and "Moldova's Twitter revolution is NOT a myth" (Net Effect, 10 April 2009).

the popular ousting of President Joseph Estrada in the Philippines has been referred to as an "SMS revolution" due to the widespread use of text messages which mobilised protesters to congregate and demand the removal of Estrada. These events were described at the time by a programme officer at the United Nations University as "arguably the world's first 'e-revolution' - a change of government brought about by new forms of ICTs [Information and Communication Technologies]."[3]

Local creation and sharing of content on the ground in the Tunisian and Egyptian revolutions, combined with the size and ultimate effect of the protests involved, arguably have not been seen before on such a large scale.

Information and communication technologies (ICTs) such as mobile phones have played a significant role in struggles for democracy and human rights in MENA, however many feel that the role of ICTs should not be overstated.[4] ICTs were not the causes of the protests and uprisings in Tunisia or Egypt, or indeed in any other MENA country. The causes of the protests involve a combination of non-technological factors including: decades of repression, political and economic marginalisation, the long-term structural decay of the effectiveness and legitimacy of state institutions, and soaring food prices. This was combined with a long-felt yearning among the general population for political representation, and the recognition of their rights. On the streets, a variety of factors including popular sentiments, grass-roots organising, and the strength and allegiance of the security apparatuses of the state ultimately determined the outcomes of the protests.

1.2. ICT access in MENA

Calling the uprisings in Tunisia and Egypt Twitter or Facebook revolutions overlooks 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. Furthermore, in Egypt only 7% of inhabitants are Facebook users, while 16% use the platform in Tunisia. Facebook use is highest in the United Arab Emirates (36%), Bahrain (29%), Qatar (24%) and Lebanon (23%). Of these countries, only one (Bahrain) experienced significant protests. From the ICT access and usage figures listed in Table 1 below it is clear that there is no necessary correlation between ICT access and unrest. Social networking users comprise a minority of the population. Thus, claims that UGC speaks for the demonstrators must be taken critically.

---

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 book, *The Net Delusion: The Dark Side of Internet Freedom* (New York: Public Affairs, 2011).

[3]Julius Cout "People Power II in the Philippines: The First E-Revolution?" (Background Paper, Overseas Development Institute, January 2001) www.odi.org.uk/resources/details.asp?id=3147&title=people-power-ii-philippines-first-e-revolution.

[4]The debate between techno-sceptics and techno-idealists with regards to the role of ICTs in Tunisia and Egypt is well outlined in Jose Antonio Vargas "Egypt, the Age of Disruption and the 'Me' in Media" (The Huffington Post, 7 February 2011) www.huffingtonpost.com/jose-antonio-vargas/egypt-age-of-disruption-me-in-media_b_819481.html. See also David Kravets "What's fueling Mideast protests? It's more than Twitter" *Wired Magazine*, 28 January 2011, 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 broad band subscriptions per 100 inhabitants	Facebook users	Facebook users per 100 inhabitants
Algeria	93,8	...	13,5	2,3	1.138.240	3,00
Azerbaijan	87.83	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*

Sources: International Telecommunication Union 2009[5] and Social Map[6]

The usage of the internet in developing countries is often disproportionately urban, thus there can be an urban bias in reporting on events. Throughout the Arab spring the world's attention was generally drawn to urban protests, for example Cairo and Alexandria in Egypt, and Tripoli and Benghazi in Libya. This may have been amplified by the intensive urban use of UGC. Also reflected in the use of UGC and social media are income and literacy biases, with smartphones and computers being used more often by literate individuals with higher incomes.

Nonetheless, many protesters did use UGC to represent popular demands, and there were clearly demonstrated linkages between mobilising demonstrators by social media and the mobilisation of demonstrators on the streets. Social media provided an initial momentum to the protests which then built up when protesters tried to get others to join them by engaging them on the streets.

It is also worth noting that there is no official data for Facebook usage in Iran, Sudan and Syria, which are under a comprehensive United States trade embargo. Although officially US websites are

[5]http://www.itu.int/ITU-D/ICTEYE/Indicators/Indicators.aspx

[6]http://geographics.cz/socialMap/

not supposed to be used in these countries, Facebook, Twitter and other US websites have been significantly used in these countries during the Arab Spring.

2. The use of UGC and social networking in MENA

While the terms "Twitter revolution" or "Facebook revolution" may not be accurate, the assertions that "the revolution will be tweeted," "the revolution will be live-blogged", and "the revolution will be streamed" do have credence in the cases of Egypt, Tunisia, Syria, Bahrain and Libya. These events involved masses of people protesting on the streets, many using mobile phones to organise the demonstrations and to spread their messages. UGC created during the protests and disseminated over social networking platforms played an important role in the MENA region, but not necessarily a decisive one.

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

2.1. Internet freedom in MENA

In November 2005 Reporters Without Borders (RSF) listed fifteen "enemies of the internet", four of which were in the MENA region: Libya, Saudi Arabia, Syria and Tunisia. In 2010, RSF listed twelve enemies of the internet, which included Saudi Arabia, Egypt, Syria and Tunisia. In March 2011, just Saudi Arabia and Syria were listed as "enemies of the internet", however Bahrain, Belarus, Egypt, Libya, Tunisia and the United Arab Emirates were listed as "under surveillance". In 2011 Saudi Arabia, Syria and Egypt are listed by RSF as having netizens in prison.[7]

Internet filtering is quite common in the MENA region, and software developed in the West is used to set up and manage these filters. The Open Net Initiative reports that Bahrain, UAE, Qatar, Oman, Saudi Arabia, Kuwait, Yemen, Sudan and Tunisia use Western technologies to block internet content, "such as websites that provide sceptical views of Islam, secular and atheist discourse, sex, GLBT, dating services, and proxy and anonymity tools."[8] Restrictions on internet freedom also happen in internet cafés. In Tunisia, internet cafés were required by law to monitor customers' access and to register their identity card numbers.

According to a 1997 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 or prevent activists from increasing their use of the technology to communicate and coordinate

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

[8]See Helmi Noman and Jillian C. York. *West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011* (OpenNet Initative, March 2008) opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

among themselves."[9] The study also points towards vibrantly growing use of UGC as well as internet activism throughout the region.

2.2 The use of UGC and social networking in the Arab spring – streaming the truth to power

In December 2010, in a small town in Tunisia called Sidi Bouzid, Mohammed Bouazizi, a poverty-stricken vegetable trader, set himself on fire in a public square outside a local government office. Bouazizi, who had been trying to support his single mother and siblings by peddling vegetables for years, was repeatedly harassed by the local police, who often asked for permits and bribes and confiscated his wares. His last encounter with the police, in which they had destroyed his goods and equipment as well as beaten him, was for him the last straw. After being denied an appointment with a local government official to discuss this harassment, he doused himself with fuel and set himself alight. He was to die in hospital weeks later.

News of Bouazizi's self-immolation inspired protests in Sidi Bouzid, Tunisia and the rest of the MENA region. However the global television and print media were slow to pick up on the story and often state media in MENA avoided reporting, or did not report accurately on the events. Significant amounts of internet content (like YouTube) were blocked by the Tunisian internet filter. Facebook, which was not blocked at the time, became an important platform for spreading news of Bouazizi and the revolt in Sidi Bouzid. Twitter, although used far less in Tunisia, was also instrumental in spreading the message of the protests.

Around the globe, many interested in the events were using Twitter and Facebook as a first port of call for information about Tunisia. News coming from Twitter about events in Tunisia served to inspire people throughout the region, like the Egyptian activist Gigi Ibrahim, who upon witnessing the downfall of the President of Tunisia, Zine al-Abidine Ben Ali, tweeted "The Tunisian revolution is being twitterised...history is being written by the people #sidibouzid #Tunisia."[10]

In Egypt social networking platforms like Facebook and Twitter were used to announce and publicise the initial protests of 25 January 2011. Facebook groups such as We are all Khaled Said[11] and the 6th of April Youth Movement[12] called for demonstrations on 25 January. The plans and message of the protest were also disseminated through conventional means like word of mouth, photocopied flyers, and email of a PDF file explaining the plans for the protests.

Facebook was also used to announce protests in many other countries in the MENA region, where it seems that virtually every call to protest in early 2011 was supported by some kind of Facebook page, event or group. UGC was used to communicate the messages of the protesters nationally,

[9]Albrecht Hofheinz "Arab Internet Use: Popular Trends and Public Impact" in Naomi Sklar (ed.) Arab Media and Political Renewal: Community, Legitimacy and Public Life (New York: IB Tauris, 2007), 60.

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

[11]See: Anonymous, " كلنا خالد سعيد - We are all Khaled Saeed." www.facebook.com/ElShaheeed. 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.elshaheeed.co.uk/ . The pages were created in response to the muder 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.

[12]See "6th of April Youth Movement - حركة شباب 6 إبريل.", www.facebook.com/shabab6april.

regionally and globally, and to provide live coverage, news and opinions. Information was often spread on Twitter, where the uprisings often had their own Twitter hash tags. The Twitter hash tags #SidiBouzid, #Jan25, #Jan30, #Feb14, #Feb17 #Mar11/#ksa, #Yemen/#Yamen, #Kuwait, and #Syria were used to refer to the protests in Tunisia, Egypt, Sudan, Bahrain, Libya, Saudi Arabia, Yemen, Kuwait and Syria respectively.

UGC helped to initially direct the world's attention to the uprisings in Tunisia and Egypt, and subsequently to other countries, influencing the democratic struggles of the region as a whole. UGC acted as a conduit for the provision of 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 the protest. The nexus of UGC and mobile phones presented an important tool for protesters to inform the outside world of their demands, the events surrounding the actual protests and the nature of police, military and civilian responses. UGC often offered views and perspectives that state-run and conventional media did not offer, as well as images that no other media was there to record. In Syria, where access by international journalists has been almost completely restricted, mobile phone videos became virtually the only way to report on protests. Throughout MENA, tools such as Twitter, Facebook and picture and video sharing platforms represented opportunities to stream the truth to power.

3. State responses to UGC and social networking

Many have commented on the awesome power of social media in the hands of protesters and activists, but 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 these protests?

3.1.Goliath and the mouse? Twitter revolutions and cyber crackdowns

An online campaign by the International Society for Human Rights (ISHR) has depicted challenged incumbent leaders gripped by fear of the revolutionary potential of ICTs. The presidents of Iran, Zimbabwe, Venezuela and Cuba, as well as Colonel Muammar Gaddafi and North Korea's Kim Jong Il, are portrayed in palatial abodes, cowering in near paralytic fear of a computer mouse, jumping on furniture, hanging from chandeliers and curtains, in an attempt to flee.[13] The ISHR campaign however does not accurately reflect the real balance of power in the electronic terrain, which is not necessarily in favour of the mouse. The real balance of power could have been better represented if balanced with other images: boots crushing mice, keyboards, and mobile phones after being identified as threats for spreading content seen as threatening to the regime. Or perhaps the regime's technicians unplugging the mice, thus terminating the ability of activists to communicate.

UGC can be a powerful tool in the hands of social movements campaigning for democracy and human rights. However, the infrastructures through which this content flows have proved to be

[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 on the blog post Duncan (no surname given), "ISHR Scared Dictators and The Mouse." (The Inspiration Room, 24 September 210) theinspirationroom.com/daily/2010/ishr-scared-dictators-and-the-mouse/.

areas of contestation between pro-democracy and pro-incumbent groups, not necessarily balanced in favour of those creating content in support of the protests. The next section investigates how regimes in the MENA region cracked down on dissent during the protests by inhibiting the flow of information, as well as by using UGC to track down protesters and arrest, detain and harass them.

Governments were able to take advantage of advanced internet filters to block content during the uprisings. In Tunisia, Egypt and Libya there were state crackdowns on UGC and the internet in general through internet blackouts, slowdowns and filtering. There were also arrests, detentions and harassment of those involved in the creation and dissemination of UGC.

Twitter and Facebook, as well as being possible instruments of protest, can also render users vulnerable to state surveillance. These platforms have been used by security and intelligence agencies to identify and locate activists and protesters.

In North Sudan, Facebook groups announced protests against the regime, as well as against President Omar el-Bashir. The North Sudanese government, following events in the region keenly, was actively monitoring social networking websites. When the protests did happen, many potential demonstrators found police waiting for them and were promptly arrested. There were reports that many of the people participating on Facebook pages were actually government agents or supporters of the regime, spreading propaganda on these groups, as well as spying on other Facebook users.[14]

In Azerbaijan, outside the region but influenced by events in Egypt, a number of Facebook pages and groups called for protests in early 2011. On 5 February, a 20-year-old activist, Jabbar Savalan from the opposition Popular Front, was arrested and charged with possession of narcotics – a charge denied by his supporters and lawyer, who claim that he was detained for comments he made on Facebook calling for Egypt-style protests.[15] 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."[16] Other detentions of people who made comments on Facebook groups also occurred.

In Saudi Arabia protests against the government and the monarchy, scheduled for 11 March 2011, were called for on Facebook and Twitter. Facebook activists were also swiftly arrested and proclamations were made about the dangers of activism by the regime.

The Tunisian Government's approach was far more advanced and involved the theft of user-names and passwords for Facebook, Twitter and online e-mail accounts like Gmail and Yahoo!. This was achieved through the injection of phishing scripts into the content of these pages before being sent to the end-user.

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

[15]Onnik Krikorian "Azerbaijan: Blowing Up in Their Facebook" (Global Voices Advocacy, 10 March 2010) advocacy.globalvoicesonline.org/2011/03/10/azerbaijan-blowing-up-in-their-facebook/.

[16]Cited in Ibid.

The Mubarak regime demonstrated its ultimate power over the internet by virtually shutting down all Egyptian access to the internet from midnight 27/28 April till 2 February 10:30 GMT.[17] In Libya, the internet was blocked to most Libyans since the beginnings of the protests and continues to be mostly blocked at the time of writing.[18]

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, such as Wael Ghonim, head of marketing of Google Middle East and North Africa, who was detained for seven days. Following these events, a popular view on Tahrir Square reflected in UGC was that many protesters were going to stay in the square until either they were defeated and arrested or Mubarak stepped down. For many, this was not only out of conviction, but also because they were content creators themselves or had created footprints on social networks. Many were afraid that in light of the arrests, detentions and alleged beatings of content creators, they had themselves become victims and they imagined being arrested if they returned home. This case demonstrates that crackdowns on ICT will not necessarily serve to quell revolutions and can in fact stoke them. It also demonstrates the amounts of danger and vulnerability that activists had exposed themselves to online.

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

4.1 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."[19] The capabilities of such a surveillance machine can be amplified by social networking platforms like Facebook that link an online identity to (most often) a user's real name, place of residence and work, interests, pictures, and network of friends .[20]

Information on Facebook made available to a user's friends or the general public may potentially be mined by third-party applications and advertisers. Facebook's API,[21] 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 particularly easy to obtain and analyse such information through the writing of basic query scripts which can then be imported into almost any

[17]Internet access during the Egyptian revolution can be graphed on Google Transparency (transparency.google.com). See: http://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.

[18]See Google Transparency for Libya from mid-February on at http://is.gd/XKhikC and http://is.gd/jTwIIS.

[19]The Hindu "World's greatest spying machine" *The Hindu*, April 2011 www.thehindu.com/opinion/editorial/article1602746.ece.

[20]Moderated, of course, by the user's privacy settings.

[21]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." Wikipedia (en.wikipedia.org/wiki/Application_programming_interface).

kind of database and then analysed with a variety of different software. Facebook "viruses" (they are operating system viruses or "malware", usually running on Windows) can be disseminated through UGC and spread to other users through links, while constantly mining for information from Facebook accounts and sending them to command and control centres. Mining of such information does not need advanced "hacking" skills, but can be done by "script-kiddies," running pre-assembled scripts and code.

4.2 Mobile phones and geolocation

Facebook and Twitter, as well as third-party mobile phone applications offer geolocation functionality, which may add location to a users' content (e.g. a tweet, Facebook update or a picture). In addition to this, all mobile phone users are constantly having their position triangulated (and often recorded) by their mobile operator. If there is an unregulated or corrupt relationship between the state and mobile operators, the usage of the mobile internet can actually enhance the surveillance capabilities of repressive regimes.

4.3. 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 played an important role in the cyber-arena of the 25 January revolution in Egypt, was opened in June 2010 but was shortly afterwards closed down by Facebook because the user who opened the account El Shaheed was using a moniker rather than a real name. Whilst this should come as no surprise –Facebook makes it explicitly clear that the use of fake names or monikers is not allowed on the platform and are a violation of the terms of service– many have questioned whether Facebook closures of certain pages have political motivations.

In the United Kingdom 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 12 hours Facebook had deleted over 50 Facebook profiles of activists in the UK.[22]

Guy Aitchison, a student at UCL and blogger for openDemocracy.net, made the following statement:

> Profiles are being deleted without warning or explanation... It may well be that these groups are technically in violation of Facebook's terms of agreement, which state that participants in social media must not make use of a 'fake name'. But the timing –on the royal wedding and May Day weekend– is deeply suspicious. We don't know for certain, but this purge of online organising groups could be linked to the wider crackdown on protest by authorities in Britain.

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

> Either way, it is a scandalous abuse of power by Facebook to arbitrarily destroy online communities built up over many months and years. These groups provide a vital means for activist groups to communicate with their supporters.[23]

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. As such, your account was disabled for violating these guidelines.
>
> If you would like to continue representing your organization on Facebook, we can convert your profile to a Page. During this process, all the friends of your profile will be converted to followers of your Page (i.e., people who like it). In addition, the account associated with your profile will be converted to a business account, from which you can administrate your Page and your ad campaigns.[24]

Of the many Facebook pages for protests and "days of rage" that were made to call for protests in the MENA region, there have been few reports of profiles, groups or pages being shut down - other than in Palestine, where the page calling for the Third Palestinian Intifada was shut down. The page was flagged as hate speech and reported to Facebook, which responded to what had been argued as a breach of their terms of service. Many Palestinians as well as sympathisers around the world wondered why all other Arab countries where allowed to have pages dedicated to a "day of rage" against their governments, but one was not allowed for a protest against Israeli occupation.

Facebook and Twitter have on the whole not interfered with the use of their platforms for protests in the MENA region. These examples however serve to remind activists that, at the end of the day, it is the social networking platforms or content platforms on which the content is hosted that has ultimate control over their online content.

4.4. Reliability and veracity of UGC

As well as for covering protests, UGC can also be used for misinformation and propaganda. The use of UGC to cover political crises raises important problems with regards to the reliability and veracity of information. Social networks can very quickly become mechanisms for spreading rumour and falsehood and, as there is usually no moderation of this content, it becomes the responsibility of the user to critically examine the veracity of claims made on these platforms.

[23]Guy Aitchison "Political purge of UK Facebook underway" (OurKingdom, 29 April 2011) www.opendemocracy.net/ourkingdom/guy-aitchison/political-purge-of-uk-facebook-underway

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

4.3 Sockpuppetry and astroturfing

More worrying is the use of UGC for disseminating propaganda. The increasing technological sophistication behind online propaganda is also a cause of concern. "Sockpuppets" are an important problem presented by the use of UGC. Wikipedia defines a sockpuppet as "an online identity used for purposes of deception within an online community. In its earliest usage, a sockpuppet was a false identity through which a member of an Internet community speaks with or about himself or herself, pretending to be a different person, like a ventriloquist manipulating a hand puppet." The *New York Times* refers to "sockpuppeting" as "the act of creating a fake online identity to praise, defend or create the illusion of support for one's self, allies or company."[25]

"Astroturfing" refers to sockpuppetry on a larger and more organised scale, designed to fake the appearance of grass-roots or "net-roots" movements (the word "astro-turf" in its conventional usage refers to synthetic grass). Sophisticated astroturfing could be used to disseminate views over UGC that appear to be the legitimate and spontaneous voices of a grass-roots movement, but are actually campaigns by individuals, corporations or governments. "The goal of such campaigns is to disguise the efforts of a political and/or commercial entity as an independent public reaction to some political entity -a politician, political group, product, service or event."[26]

The leaderless and largely faceless *hacktivist* collective Anonymous[27] claim to have discovered the existence of an advanced astroturfing software allegedly commissioned by the US Air Force and developed by the US security company HBGary and US defence contractor Booz Allen Hamilton. This software can create "armies of fake people", online identities with corresponding social networking profiles on multiple platforms, which can create UGC and comment on UGC with identities that appear contingent to previous posts, as well as according to culture, age or gender. In addition to providing a platform for astroturfing, this software is also a surveillance platform, as "fake friends" on social networks to monitor and surveil unsuspecting users.

Barrett Brown, a journalist previously involved with Anonymous, has mused that this software may have been employed in Azerbaijan to surveil and entrap activists, as well as to spread pro-invasion propaganda in Iraq.[28] The software has no official name, but has been given one by Anonymous for the purpose of reference: Metal Gear (named after the Japanese series of role-playing games). The possible existence of Metal Gear raises important concerns about the possible nexus of UGC, astroturfing and artificial intelligence. These are concerns that those seeking to analyse UGC in political crises should be particularly aware of.

[25]Cited in http://en.wikipedia.org/wiki/Sockpuppet_(Internet).

[26]en.wikipedia.org/wiki/Astroturfing

[27]Anonymous is known for their attacks in December 2010 on Mastercard, Visa and Paypal as well as for activism in support of protests in MENA. The software was discovered in leaked emails, acquired by a group of Anonymous hackers who hacked the Washington D.C. beltway security consulting company HBGary. This was in response to CEO of HB Gary Federal, Aron Barr, who proclaimed that he had found the identities of a large amount of Anonymous members, announced it to the media, and scheduled a talk about it at a security conference. Anonymous' pre-emptive attack resulted in acquiring and immediate leaking of over 4GB of emails from email accounts of the CEO of HB Gary, Greg Hoglund, as well as the CEO of Subsidiary HBGary Federal. The HBGary emails contain an in-depth view of the dealing of Beltway security companies.

[28]See Anonymous "Operation Metal Gear" (AnonNews, n.d.), http://anonnews.org/?p=press&a=item&i=752.

5. Conclusion

USG and mobile phones are not unequivocally tools for the benefit of protesters, but rather a contested terrain used by both the regimes and the protests movements in the societal conflicts around the uprisings in MENA. User content created on mobile phones and instantly disseminated on the internet was a powerful tool in the hands of the regime security and intelligence forces, as well as protesters, and USG could also be used to spread fear or disinformation. 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.

Concerns raised in this paper will not disappear in Egypt and Tunisia now that the incumbent presidents have been removed. 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 the internet, mobile phones, social media and social networking sites cease to be of relevance.

UGC created on mobile phones is being used actively in Egypt and Tunisia to expose violations of the security forces. In Egypt, the military recognised the power of Facebook, made a Facebook page after the fall of Mubarak to try to garner support and make peace with the protesters. The transition period in Egypt and Tunisia is still unfolding, elections need to be planned, political parties need to be organised, re-organised and new ones formed. These organisational processes cannot be conducted today without the internet and ICTs.

On 6 February 2011 Mahmoud Salem, aka Sandmonkey, a blogger, tweeter and activist who was detained and released during the Egyptian protests, offered in his blog post The Way Forward the following words of advice on organising to secure the revolution, build a political party to secure the aims of the revolution, run for office and implement a constitution:

> So here are my two cents: next time when you head to Tahrir, alongside blankets and food and medicine, please get some foldable tables, chairs, papers, pens, a laptop and a USB connection. Set up a bunch of tables and start registering the protesters. Get their names, ages, addresses & districts. Based on location, start organizing them into committees, and then have those committees elect leaders or representatives. Do the same in Alex[andria], In Mansoura, in Suez, in every major Egyptian city in which the Protesters braved police suppression and came out in the thousands. Protect the Data with your life. Get encryption programs to ensure the security of the data. Use web-based tools like Google documents to input the data in, thus ensuring that even if your laptops get confiscated by State Security Goons, they won't find anything on your hard drives. Have people outside of Egypt back-up your data daily on secure servers. Then, start building the structure.[29]

ICTs will have an important role in the transition period but must be approached in cognisance of the tough lessons learned about UGC and mobile phones in the Arab spring of 2011.

[29]Mahmoud Salem (Sandmonkey) "The Way Forward" (Rantings of a Sandmonkey, 6 February 2011) www.sandmonkey.org/2011/02/06/the-way-forward.

6. Recommendations on the safe use of UGC platforms

6.1 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 cannot be known. Nonetheless, in the context of regimes who repress and crack down on internet use, the protection afforded by anonymity does have its merits. Content creators should be informed about the possibilities of creating content anonymously and securely. Decisions need to be made about whether to use real names, or rather monikers in order to maintain anonymity. If anonymity, or a moniker is chosen, creators of content must be aware that using social networks over which to distribute UGC may expose their identity if not done correctly. Even if, for example, Facebook activism is conducted with an anonymous moniker something as simple as a network of real-life friends, one picture or an accidental use of geolocation could expose a user's identity.

6.2. Safe and informed use of social networking

Any platform for disseminating and sharing UGC raises the challenge of balancing activism with attention to privacy and online safety. Different platforms offer different strengths and weaknesses with regards to the often diverging goals of activism and privacy. For example, Facebook does not allow for anonymity, and the use of fake names are not permitted. Twitter does not allow for anonymous accounts but monikers are permitted.

Facebook users need to be aware of the range of possible privacy settings, as well as of the implications of the various settings. The default Facebook privacy settings (which change very often) are not necessarily the best settings for privacy. With some settings, it is even possible to have Facebook statuses viewable even to those without a Facebook account. Minimal privacy settings in certain conditions may be useful for online activism insofar as they help build and coordinate communities, and help to spread content virally. In some contexts, these settings may not present the best choice of settings for activists.

Twitter aggregates less media and information on a user's profile. Tweets can be publicly viewable (the default option) and can thus potentially reach a much larger audience than most Facebook accounts. This audience can be reached without compromising anonymity as easily as with the use of a Facebook account. Furthermore, given the nature of Twitter, there is usually a lot less potentially identifiable personal information available.

Each platform for the creation and dissemination of UGC, as well as each social networking website, have conditions of use as well as a privacy policy 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. The relationships between governments and UGC platforms, or social networking websites such as Facebook and Twitter, must be considered as a possible risk factor. The example of the US Department of Justice´s subpoena of Twitter to provide information from the Twitter accounts of Wikileaks and its affiliates

and supporters (such as Icelandic MP, Birgita Jonsdottir) should be of relevance to informed activists.

6.3. Backup and mirroring of content

Facebook and Twitter have, on the whole, not interfered with the use of their platforms for protests in the MENA region and have, as outlined in the paper, provided valuable platforms for protest. However the examples of the We are all Khaled Said and the UGC Occupation Facebook pages serve to remind activists that, 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 planned for this by backing up and mirroring the content.

6.3. There *are* alternatives to Facebook

With all the raised concerns about social networking platforms, privacy management and the legal environment 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. It would offer a useful safety mechanism if social networking accounts could for example be switched off by the owner of the account, and appear as offline and untraceable at the will of the owner - turned instantly "off" or "on" at certain times, deemed to be safe or not safe.

Each social networking platform has its own strengths and weaknesses. There are alternatives to social networking platforms such as Twitter or Facebook. Pligg is an open-source software that allows one to create self-hosted social networks. The Diaspora project hopes to create multiple, overlapping social networks with a social networking platform called Diaspora which is self-hosted, 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. Status.net, developed by Canonical, offers a micro-blogging client that offers an alternative to Twitter which can be used to create open or closed micro-blogging networks.

6.4. UGC under surveillance

If the avoidance of state surveillance is required certain practices should be followed wherever possible when disseminating UGC and using mobile phones to disseminate 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 application should always be accessed through HTTPS encryption if it is available (by typing https://, instead of http:// before a web address).[30] Using HTTPS will help avoid the stealing of user names and passwords, as happened in Tunisia. Anonymising tools such as proxies, VPNs and TOR can also be used for protecting the identity of content creators, as well as for circumventing internet filtering and censorship systems.

[30]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.

Bibliography

Cout, Julius "People Power II in the Philippines: The First E-Revolution?", Background Paper, Overseas Development Institute, January 2001 http://www.odi.org.uk/resources/details.asp?id=3147&title=people-power-ii-philippines-first-e-revolution

Hofheinz, Albrecht "Arab Internet Use: Popular Trends and Public Impact" in Naomi Sklar (ed.) *Arab Media and Political Renewal: Community, Legitimacy and Public Life* New York: IB Tauris, 2007

Morozov, Evgeny *The Net Delusion: The Dark Side of Internet Freedom* New York: Public Affairs, 2011

Noman, Helmi and York, Jillian C. *West Censoring East: The Use of Western Technologies by Middle East Censors, 2010-2011* OpenNet Initative, March 2008 http://opennet.net/west-censoring-east-the-use-western-technologies-middle-east-censors-2010-2011

Nunns, Alex and Idle, Nadia *Tweets from Tahrir* New York: OR Books, 2011.

Reporters Without Borders *The 15 enemies of the Internet and other countries to watch* Reporters without Borders, 17 November 2005 http://en.rsf.org/the-15-enemies-of-the-internet-and-17-11-2005,15613.html

Reporters without Borders *Web 2.0 vs Control 2.0* Reporters Without Borders, 12 March 2010 http://en.rsf.org/IMG/pdf/Internet_enemies.pdf

Reporters Without Borders *Internet Enemies* Reporters without Borders, 12 March 2011 http://march12.rsf.org/i/Internet_Enemies.pdf