

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

Alex Comminos

Doctoral candidate, Department of Geography, Justus Liebig University Giessen
www.comminos.org, www.uni-giessen.de/cms/faculties/f07/07/geography/depart-geo

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 revolutions.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.

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_twiters_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)

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.

Nonetheless, many protesters used UGC to express popular demands. Linkages were demonstrated between the mobilisation of demonstrators by social media as well as offline (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.

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

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

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 hashtags. The Twitter hashtags #SidiBouzid, #Jan25, #Jan30, #Feb14, #Feb17, #Mar11/#ksa/#tal3mrak,¹² #Yemen/#Yamen,

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

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, “[دي عن دلخ ان لاف] - 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 - ليربنا 6 بابش ظفرح”, 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

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

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

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 January 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

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/XKhikC and is.gd/jTWiIS

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*.

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

20 Somaiya, 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 (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.

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 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,

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, *Our Kingdom*, 29 April. www.opendemocracy.net/ourkingdom/guy-aitchison/political-purge-of-uk-facebook-underway

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.

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:

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 Neroulas, 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

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.upeace.org/innerpg.cfm?id_article=816